

# PRT-6302 (Series) Home Gateway

## User Manual



**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](mailto:INT-support@comtrend.com)

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

**Important Safety Instructions**

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

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- Never install telephone wiring during stormy weather conditions.

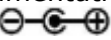
**CAUTION:**

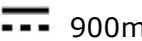
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.
- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
- Do not stack equipment or place 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.

**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
  
- 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

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 choisis 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 30 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 30 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 30 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 spécifications 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 )
  - TIA-968 / IC-CS03
  - UL 62368-1 / CSA 62368-1

### **Copyright**

Copyright©2021 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

<b>NOTE:</b> 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](mailto: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

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>10</b>
<b>CHAPTER 2 INSTALLATION.....</b>	<b>11</b>
2.1 HARDWARE SETUP.....	11
2.1.1 Back Panel.....	12
2.1.2 Front Panel.....	14
<b>CHAPTER 3 WEB USER INTERFACE.....</b>	<b>16</b>
3.1 DEFAULT SETTINGS .....	16
3.2 IP CONFIGURATION.....	17
3.3 LOGIN PROCEDURE.....	19
<b>CHAPTER 4 DEVICE INFORMATION.....</b>	<b>21</b>
4.1 WAN .....	23
4.2 STATISTICS.....	25
4.2.1 LAN Statistics .....	25
4.2.2 WAN Service .....	26
4.3 ROUTE.....	27
4.4 ARP.....	28
4.5 DHCP.....	29
4.6 NAT SESSION .....	30
4.7 IGMP INFO.....	31
4.8 CPU & MEMORY .....	32
4.9 NETWORK MAP .....	33
4.10 WIRELESS .....	34
4.10.1 Station Info .....	34
4.10.2 WiFi Insight .....	35
4.10.2.1 Site Survey.....	37
4.10.2.2 Channel Statistics .....	40
4.10.2.3 Metrics (Advanced Troubleshooting).....	44
4.10.2.4 Configure .....	46
4.11 TOPOLOGY .....	48
<b>CHAPTER 5 BASIC SETUP.....</b>	<b>49</b>
5.1 WAN SETUP .....	50
5.1.1 WAN Service Setup .....	51
5.2 NAT .....	53
5.2.1 Virtual Servers .....	53
5.2.2 Port Triggering.....	55
5.2.3 DMZ Host.....	57
5.2.4 ALG/Passthrough .....	57
5.3 LAN .....	58
5.3.1 Lan VLAN Setting.....	60
5.3.2 LAN IPv6 Autoconfig.....	61
5.3.3 UPnP .....	63
5.4 PARENTAL CONTROL.....	64
5.4.1 Time Restriction.....	64
5.4.2 URL Filter .....	65
5.5 HOME NETWORKING .....	67
5.5.1 Print Server .....	67
5.5.2 DLNA.....	67
5.5.3 Storage Service.....	68
5.5.4 USB Speed .....	70
5.6 WIRELESS .....	71
5.6.1 SSID.....	71
5.6.2 Security.....	72
5.7 WIFI XTEND 2.0 .....	75
5.8 AUTO XTEND.....	76



<b>CHAPTER 6 ADVANCED SETUP.....</b>	<b>77</b>
6.1 SECURITY .....	77
6.1.1 IP Filtering .....	77
6.1.2 MAC Filtering .....	81
6.2 QUALITY OF SERVICE (QoS).....	83
6.2.1 QoS Queue.....	84
6.2.1.1 QoS Queue Configuration .....	84
6.2.1.2 Wlan Queue .....	88
6.2.2 QoS Classification .....	89
6.2.3 QoS Port Shaping.....	92
6.3 ROUTING .....	93
6.3.1 Default Gateway.....	93
6.3.2 Static Route.....	94
6.3.3 Policy Routing .....	95
6.3.4 RIP .....	97
6.4 DNS .....	98
6.4.1 DNS Server.....	98
6.4.2 Dynamic DNS.....	99
6.4.3 DNS Entries.....	100
6.5 DNS PROXY .....	101
6.6 INTERFACE GROUPING.....	102
6.7 IPTUNNEL.....	105
6.7.1 IPv6inIPv4.....	105
6.7.2 IPv4inIPv6.....	107
6.7.3 MAP.....	108
6.8 IPSEC .....	110
6.8.1 IPSec Tunnel Mode Connections .....	110
6.9 CERTIFICATE.....	114
6.9.1 Local.....	114
6.9.2 Trusted CA.....	117
6.10 MULTICAST.....	118
6.11 WIRELESS .....	121
6.11.1 SSID.....	121
6.11.2 Security.....	122
6.11.3 WPS.....	125
6.11.4 MAC Filtering.....	127
6.11.5 WDS.....	128
6.11.6 Advanced.....	133
6.12 WIFIXTEND 2.0 .....	138
6.13 AUTOXTEND.....	139
<b>CHAPTER 7 DIAGNOSTICS.....</b>	<b>140</b>
7.1 DIAGNOSTICS – INDIVIDUAL TESTS .....	140
7.2 ETHERNET OAM .....	141
7.3 UPTIME STATUS .....	143
7.4 PING .....	144
7.5 TRACE ROUTE .....	145
<b>CHAPTER 8 MANAGEMENT .....</b>	<b>146</b>
8.1 SETTINGS.....	146
8.1.1 Backup Settings .....	146
8.1.2 Update Settings.....	147
8.1.3 Restore Default .....	147
8.2 SYSTEM LOG .....	149
8.3 SNMP AGENT .....	151
8.4 TR-069 CLIENT .....	152
8.5 STUN CLIENT .....	154
8.6 INTERNET TIME .....	155
8.7 ACCESS CONTROL .....	156
8.7.1 Accounts .....	156
8.7.2 Services.....	157

8.7.3 IP Address.....	158
8.8 UPDATE SOFTWARE .....	159
8.9 REBOOT.....	160
<b>CHAPTER 9 LOGOUT .....</b>	<b>161</b>
<b>APPENDIX A - FIREWALL .....</b>	<b>162</b>
<b>APPENDIX B - PIN ASSIGNMENTS .....</b>	<b>165</b>
<b>APPENDIX C – SPECIFICATIONS .....</b>	<b>166</b>
<b>APPENDIX D - SSH CLIENT .....</b>	<b>168</b>
<b>APPENDIX E - PRINTER SERVER.....</b>	<b>169</b>
<b>APPENDIX F - CONNECTION SETUP.....</b>	<b>176</b>

## Chapter 1 Introduction

PRT-6302 is a dual band WiFi 6 router with an updated silicon platform. It provides a 2.5 Giga Ethernet WAN port and four Giga Ethernet ports, supporting WiFi 6 (802.11ax) Wireless solution on frequency band of 2.4GHz (4T4R) & 5GHz (4T4R). PRT-6302 allows central management (ACS) by following TR-069. The core design concept of PRT-6302 is to enhance the user experience on high speed applications with its high power wireless design, so as to provide better coverage and stable WiFi services.

## Chapter 2 Installation

### 2.1 Hardware Setup



DO NOT STACK

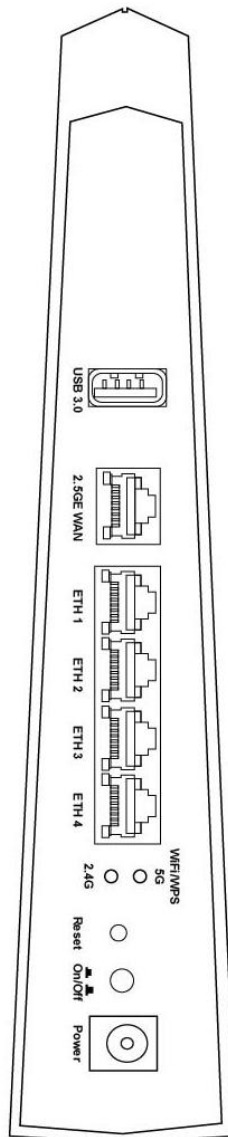
#### **Non-stackable**

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.



#### **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.

#### **GETH WAN PORT**

This port is designated to be used for 2.5 Gigabit Ethernet WAN functionality only. Use an Ethernet RJ-45 cable to connect to Gigabit WAN server for standard network usage.

#### **Ethernet (LAN) Ports**

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

**WiFi On/Off/ WPS Button 5G**

Press the 5G button for less than 5 seconds to enable WPS which will allow 2 minutes for WiFi connection.

Press and hold the 5G button > 5 seconds and less 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 > 5 seconds and less 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 PRT-6302 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**

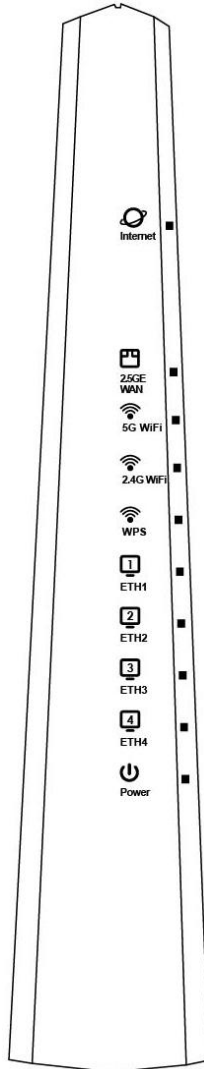
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section – LED Indicators).

**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.)

2.5GE WAN	Green	On	Ethernet WAN is connected.
		Off	Ethernet WAN is not connected.
		Blink	Ethernet WAN is transmitting/ receiving.
5G WiFi	Green	On	Wi-Fi enabled.
		Off	Wi-Fi disabled.
		Blink	Data transmitting or receiving over WLAN.
2.4G WiFi	Green	On	Wi-Fi enabled.
		Off	Wi-Fi disabled.
		Blink	Data transmitting or receiving over WLAN.
WPS	Green	On	WPS connection successful. The LED will stay on for 3 minutes.
		Off	No WPS association process ongoing.
		Blink	WPS connection in progress. WPS connection unsuccessful. The LED will keep blinking for 30 seconds.
ETH 1X-4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.

**Note:**

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



## 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 PRT-6302 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.

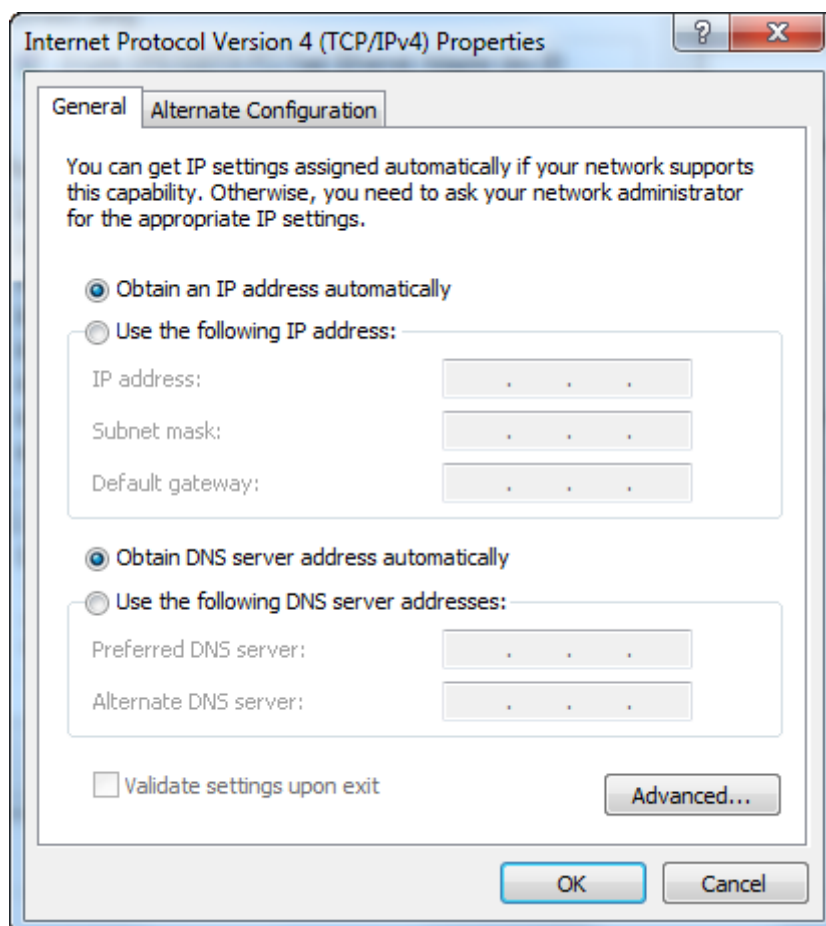
To obtain an IP address from the DHCP server, follow the steps provided below.

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

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

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

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



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

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

**STATIC IP MODE**

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

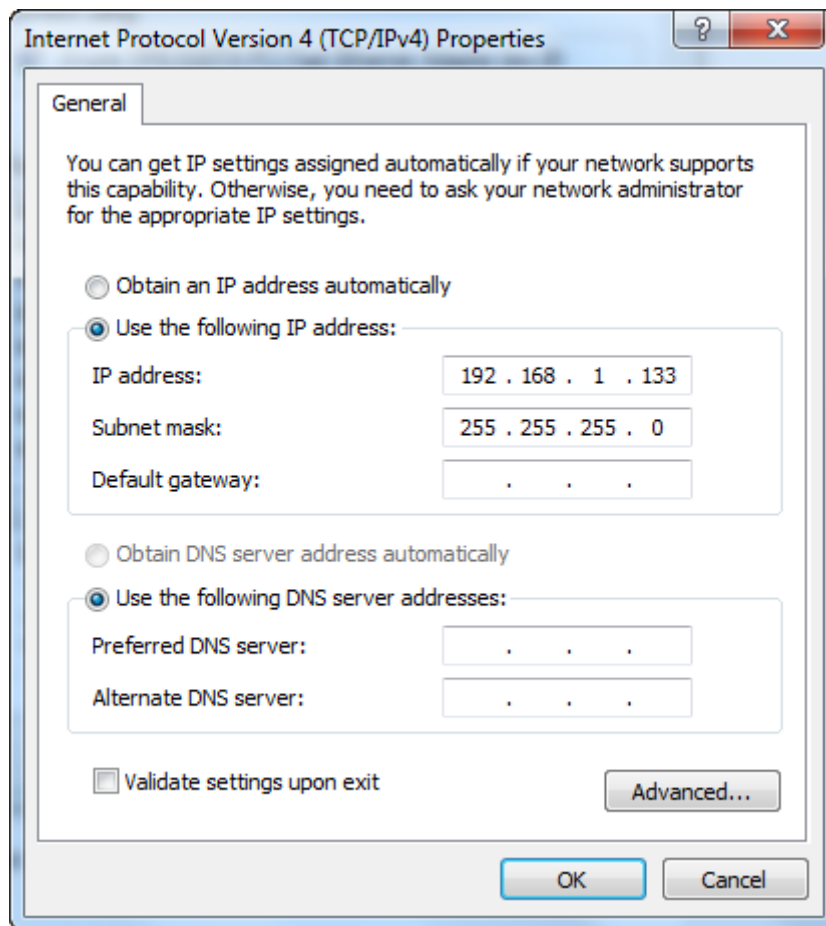
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



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

## 3.3 Login Procedure

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

**NOTE:** The default settings can be found in section [3.1 Default Settings](#).

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

**NOTE:** For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the [Device Information](#) screen and login with remote username and password.

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



Click **OK** to continue.

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

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

The screenshot displays the Comtrend web interface with the following sections:

- Navigation Tabs:** Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, Logout.
- Summary Menu:** Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, CPU & Memory, Network Map, Wireless, Topology.
- Device Section:**

Model	PRT-6302
Board ID	63158MR-187AX2
Serial Number	2095955UXXF-AA000000
Firmware Version	GT11-502CTU-C02_R02
Bootloader (CFE) Version	1.0.38-163.243-0
Up Time	38 secs
- Wireless Section:**
  - 2.4GHz Interface:**

Driver Version	17.10.99.27
Primary SSID	Comtrend5501_2.4GHz
Status	Enabled
Channel	1
Security	Secure
Primary Encryption	WPA2-PSK, AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>
  - 5GHz Interface:**

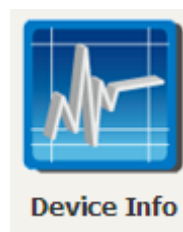
Driver Version	17.10.99.27
Primary SSID	Comtrend5501_5GHz
Status	Enabled
Channel	36
Security	Secure
Primary Encryption	WPA2-PSK, AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>
- LAN Section:**

eth1	Down
eth2	Down
eth3	100 FD
eth4	Down
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:59:55:01
DHCP Server	Enabled
- WAN Section:**

WAN Interface: ipoe\_eth0

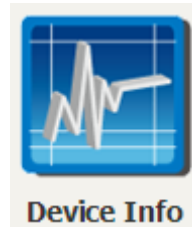
Link Type	Ethernet
Link Status	Up
Connection Type	Disconnected
Connection Type	IPoE
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

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.

**Summary**

**WAN**

**Statistics**

**Route**

**ARP**

**DHCP**

**NAT Session**

**IGMP Info**

**CPU & Memory**

**Network Map**

**Wireless**

**Topology**

**Device**

Model	PRT-6302
Board ID	63158MR-187AX2
Serial Number	2095955UXXF-AA000000
Firmware Version	GT11-502CTU-C02_R02
Bootloader (CFE) Version	1.0.38-163.243-0
Up Time	38 secs

**Wireless**

2.4GHz Interface	
Driver Version	17.10.99.27
Primary SSID	Comtrend5501_2.4GHz
Status	Enabled
Channel	1
Secure	
Primary Encryption	WPA2-PSK, AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>
5GHz Interface	
Driver Version	17.10.99.27
Primary SSID	Comtrend5501_5GHz
Status	Enabled
Channel	36
Secure	
Primary Encryption	WPA2-PSK, AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>

**LAN**

Down  
eth1

Down  
eth2

100 FD  
eth3

Down  
eth4

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:59:55:01
DHCP Server	Enabled

**WAN**

DOWN

WAN Interface	ipoe_eth0 ▾
Link Type	Ethernet
Link Status	Up
Disconnected	
Connection Type	IPvE
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

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.

Fixed MTU

MTU:

Enable PPP Manual Mode

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**IGMP Multicast**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

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

**COMTREND**

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	PPP connect/disconnect	IPv6 Status	IPv6 Address
ppp0.1	pppoe_eth0	PPPoE	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	LowerLayerDown		Connect	ServiceDown	

## 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.

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

**Summary**

**WAN**

**Statistics**

**LAN**

WAN Service

Route

ARP

DHCP

NAT Session

IGMP Info

CPU & Memory

Network Map

Statistics -- LAN

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
eth0	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	42020	357	0	0	0	89	211	57	255887	393	0	0	0	80	300	13
eth4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Item	Description
Interface	LAN interface(s)
Received/Transmitted:	<ul style="list-style-type: none"> <li>- Bytes</li> <li>- Pkts</li> <li>- Errs</li> <li>- Drops</li> </ul>
	<ul style="list-style-type: none"> <li>Number of Bytes</li> <li>Number of Packets</li> <li>Number of packets with errors</li> <li>Number of dropped packets</li> </ul>

25

Leading the **Communication Trend**

### 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	<ul style="list-style-type: none"> <li>- Bytes</li> <li>- Pkts</li> <li>- Errs</li> <li>- Drops</li> </ul>
	<ul style="list-style-type: none"> <li>Number of Bytes</li> <li>Number of Packets</li> <li>Number of packets with errors</li> <li>Number of dropped packets</li> </ul>

### 4.3 Route

Choose **Route** to display the routes that the PRT-6302 has found.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary  
WAN  
Statistics  
**Route**  
ARP  
DHCP

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	cpe-ipintf-1	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	cpe-ipintf-1	br0

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.

IP address	Flags	HW Address	Device
192.168.1.3	Complete	00:50:ba:24:29:bd	br0

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
Expires In	Shows how much remaining time is left for each DHCP Lease

## 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.

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

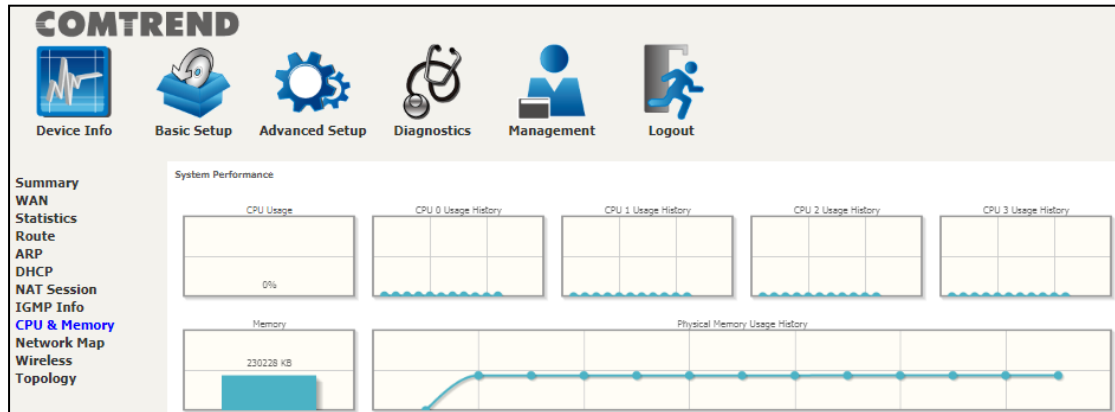
Click **IGMP Info** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.

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



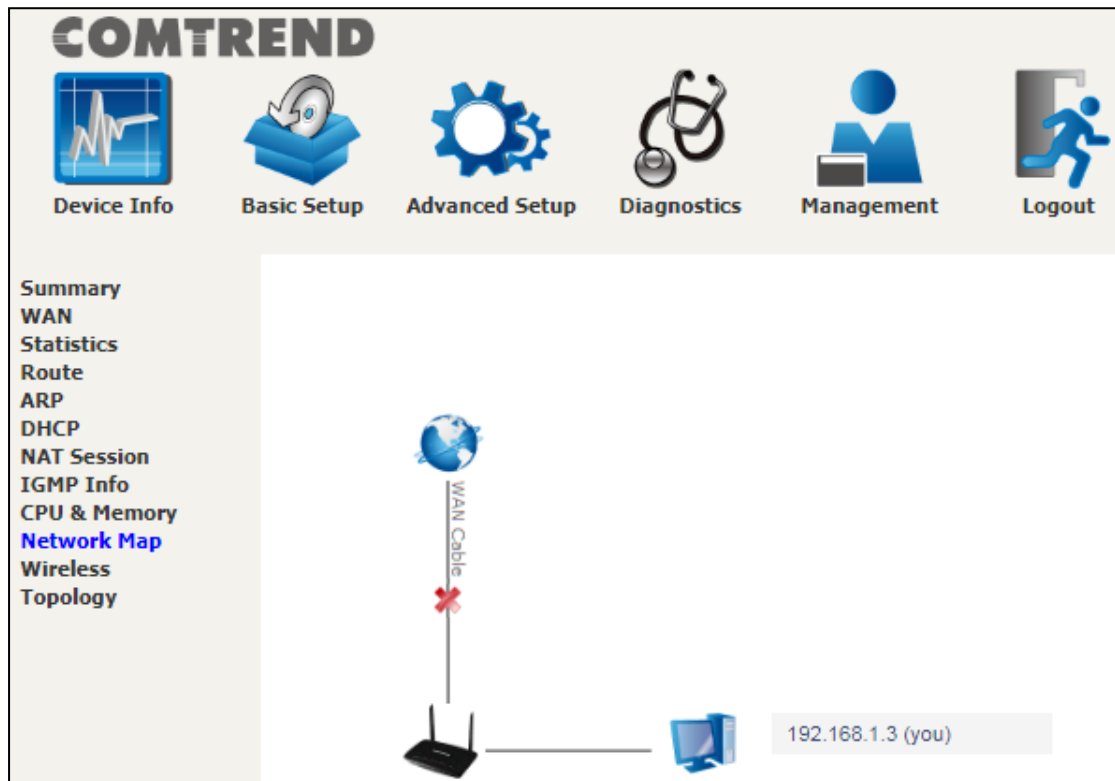
## 4.8 CPU & Memory

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.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Summary**  
**WAN**  
**Statistics**  
**Route**  
**ARP**  
**DHCP**  
**NAT Session**  
**IGMP Info**  
**CPU & Memory**  
**Network Map**  
**Wireless**  
[Station Info](#)  
[Wifi Insight](#)

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

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼  
 BSS-MAC (SSID): D8:B6:B7:59:55:02 (Comtrend5501\_2.4GHz enabled) ▼

Authenticated Stations:

MAC Address	Association Time	Authorized	WMM Link	Power Save	APSD Default
-------------	------------------	------------	----------	------------	--------------

Consult the table below for descriptions of each column heading.

Item	Description
Wireless Interface	Lists the 5GHz/2.4GHz interface that the station connects to
BSS-MAC (SSID)	Lists which SSID of the modem that the stations connect to
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 (WiFi MultiMedia)
Power Save	Lists those devices that utilize the Power Save Feature
APSD Default	Lists those devices that utilize the Automatic Power Save Delivery Feature

### 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 WiFi 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. Select the wireless interface, channel, bandwidth to check the different display if desired.

### 2.4GHz

The screenshot shows the Comtrend Site Survey interface. At the top, there are navigation icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. A sidebar on the left lists various system information sections. The main content area is titled 'Site Survey' and includes a sub-header 'In this page you will see all the AP's around.' Below this, there are three dropdown menus: '2.4 GHz - Comtrend5501\_2.4GHz', 'Select Channel', and 'Select Bandwidth', followed by a 'Scan' button. The central part of the interface features a graph titled 'AP's Around' with 'Signal Strength [dBm]' on the y-axis (ranging from -100 to 0) and 'Channels' on the x-axis (ranging from 1 to 13). A red curve shows a peak signal strength of 0 dBm at channel 3. Below the graph is a table with the following data:

Network Name	Network Address	Signal [dBm]	SNR [dB]	Bandwidth [MHz]	Center Channel	Control Channel	Max PHY Rate [Mbps]	802.11	Security
Comtrend5501_2.4GHz	D8:B6:B7:59:55:02	0	82	40	3	11	800	bgn	TKIP AES, WPA-PSK, WPA2-PSK

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
okSNR [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

**5GHz**

1. Select the wireless network (5GHz in above example) that you wish to monitor from the drop-down menu.
2. Select the channel that you wish to monitor from the drop-down menu.
3. Select a bandwidth of the wireless network from the drop-down menu.
4. 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]	SNR 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

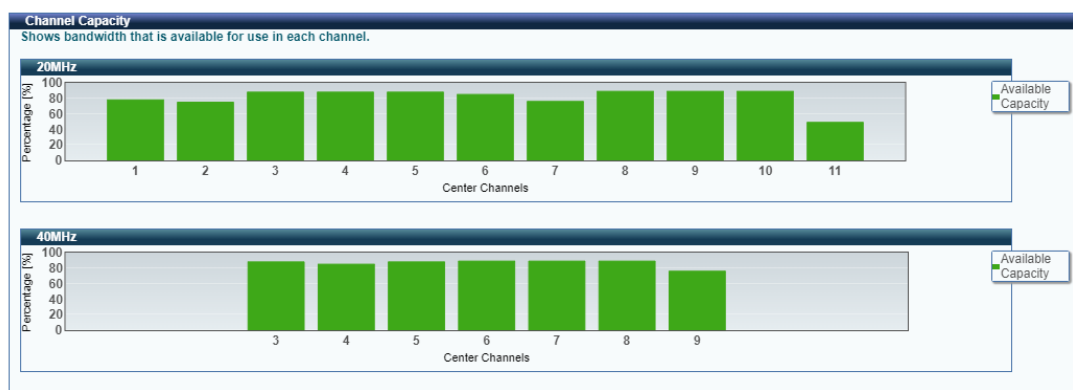
**4.10.2.2 Channel Statistics**

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

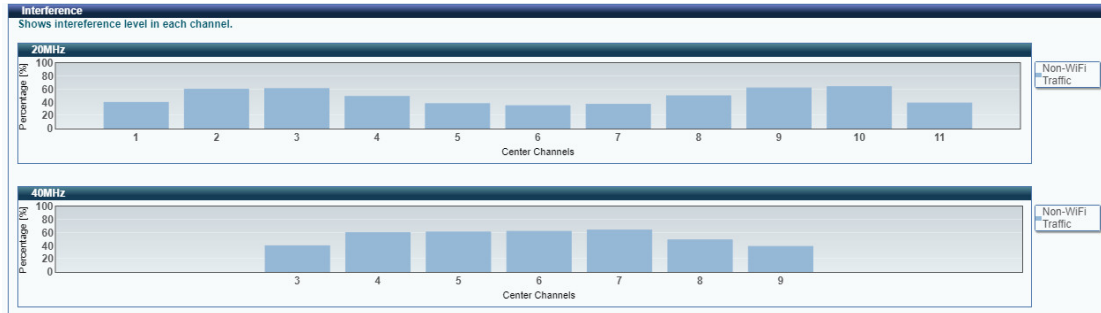
Click on the drop-down menu to select 2.4GHz or 5GHz interface.

**2.4 GHz**

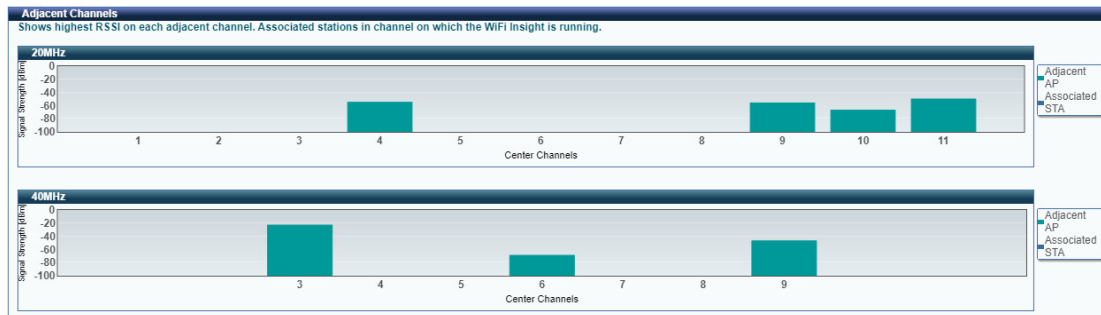
Shows the bandwidth that is available for use in each channel.



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**

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary  
WAN  
Statistics  
Route  
ARP  
DHCP  
NAT Session  
IGMP Info  
CPU & Memory  
Network Map  
Wireless  
Station Info  
Wifi Insight  
Site Survey  
**Channel Statistics**  
Metrics  
Configure  
Topology

**Channel Statistics**  
In this page you will see the Wi-Fi and Non Wi-Fi Interference also Available Capacity

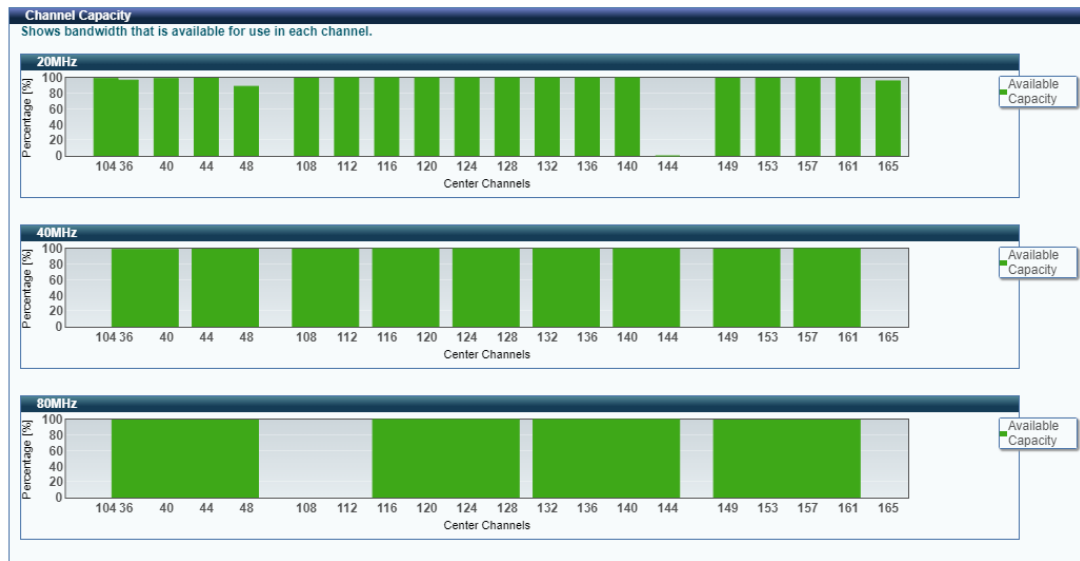
5 GHz - Comtrend5501\_5GHz

Current Channel :36/80  
Current Channel BandWidth:80 MHz  
Current Available Capacity :0%

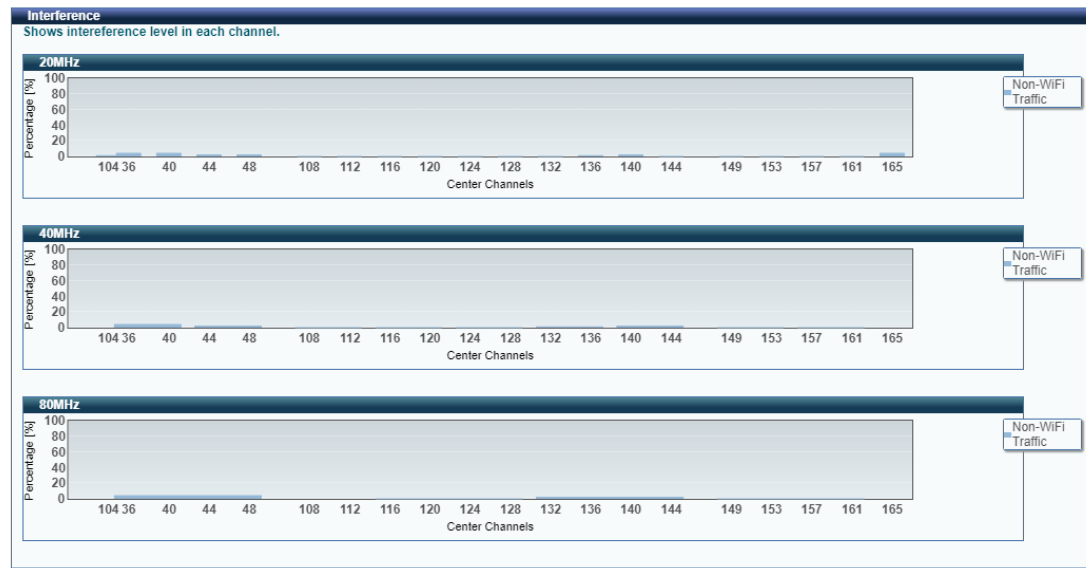
**Associated Station's**  
Shows stations associated with AP.

SSID : Comtrend5501\_5GHz  
BSSID : D8:B6:B7:59:55:03  
Channel : 36/80

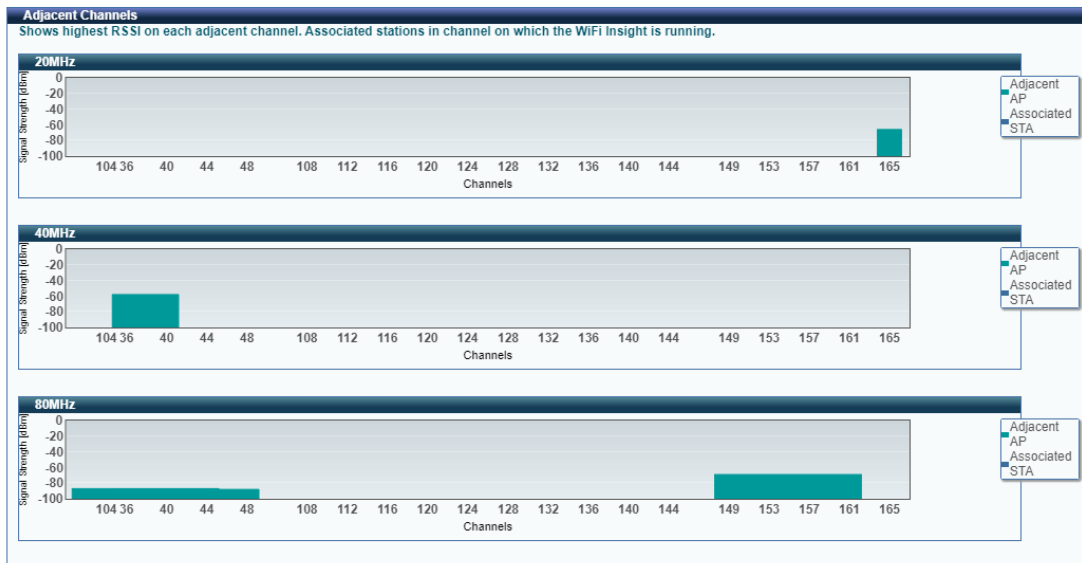
Shows the bandwidth that is available for use in each channel.



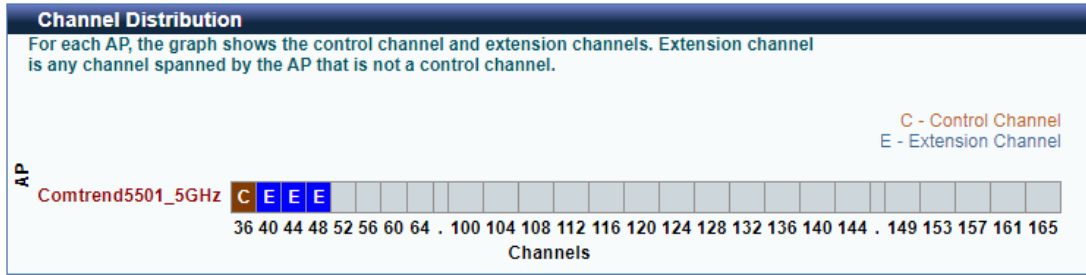
Shows interference level in each channel.



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), Glitch, Chanim and Packet Queue Statistics. This page is broken down into individual parts below.

**Advanced Troubleshooting**  
 In this page you will see most of the counters like AMPDU(if available), Glitch, Chanim and Packet Queue Statistics

5 GHz - Comtrend5501\_5GHz

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

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



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




Lists the associated station to the wireless interface.

**Associated Station's**

Click on station's to see the Packet Queue Statistics

SSID : Comtrend5501\_5GHz  
BSSID : D8:B6:B7:59:55:03  
Channel : 100



SR.	MAC	RSSI [dBm]	PHY Rate [Mbps]
-----	-----	------------	-----------------

### 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 WiFi 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.

Topology ID	Hostname	MAC Address	IP Address	Backhaul	RSSI	Device Connected	Ping
Master AP	PRT-6302	d8:b6:b7:59:55:01	192.168.1.1	NA	0	0	<input type="button" value="Ping"/>

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
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.

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

**WAN Setup**

NAT

LAN

Parental Control

Home Networking

Wireless

WifiXtend2.0

AutoXtend

**LAN**

Down eth1

Down eth2

100 FD eth3

Down eth4

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:59:55:01
DHCP Server	Enabled

**Wireless**

2.4GHz Interface	
Driver Version	17.10.99.27
Primary SSID	Comtrend5501_2.4GHz
Status	Enabled
Channel	1
	Secure
Primary Encryption	WPA2-PSK AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>
5GHz Interface	
Driver Version	17.10.99.27
Primary SSID	Comtrend5501_5GHz
Status	Enabled
Channel	36
	Secure
Primary Encryption	WPA2-PSK AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>

**WAN**

DOWN

WAN Interface	ipoe_eth0
Link Type	Ethernet
Link Status	Up
	Disconnected
Connection Type	IPoE
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

## 5.1 WAN Setup

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

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**WAN Setup**  
NAT  
LAN  
Parental Control  
Home Networking  
Wireless  
WifiXtend2.0  
AutoXtend

Step 1: Layer 2 Interface

Select new interface to add: **ETHERNET interface** Add

ETH WAN Interface Configuration

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

Step 2: Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Icmp Proxy	Icmp Source	NAT	Firewall	IPv6	Mid Proxy	Mid Source	Manual Mode	Remove	Edit
eth0.1	ipoe_eth0	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

Add Remove

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.

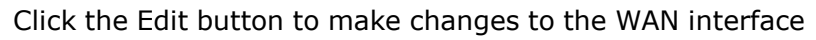
Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Manual Mode	Remove	Edit
eth0.1	ipoe_eth0	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Manual Mode	Remove	Edit
eth0.1	ipoe_eth0	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input checked="" type="checkbox"/>	Edit

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

A rectangular button with the text "Edit" inside.A rectangular text box containing the text "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 <b>Or</b> Custom Service	User should select the service from the list. <b>Or</b> User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	Select the protocol (TCP, TCP/UDP, or UDP) from the drop-down menu.
Internal Port Start	Enter the internal port starting number (when you select Custom Server) for the range you want to give access to the internal network. 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) for the range you want to give access to the internal network. 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.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**WAN Setup**  
**NAT**  
 Virtual Servers  
**Port Triggering**  
 DMZ Host  
 ALG/Pass-Through  
**LAN**  
 Parental Control  
 Home Networking  
 Wireless  
 WifiXtend2.0  
 AutoXtend

**NAT -- Port Triggering Setup**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the '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.

Add Remove

Application Name	Trigger				Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			

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

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**WAN Setup**  
**NAT**  
 Virtual Servers  
**Port Triggering**  
 DMZ Host  
 ALG/Pass-Through  
**LAN**  
 Parental Control  
 Home Networking  
 Wireless  
 WifiXtend2.0  
 AutoXtend

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. Remaining number of entries that can be configured: 32

Use Interface: eth0.1/eth0.1

Application Name:  
 Select an application: Select One  
 Custom application:

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

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

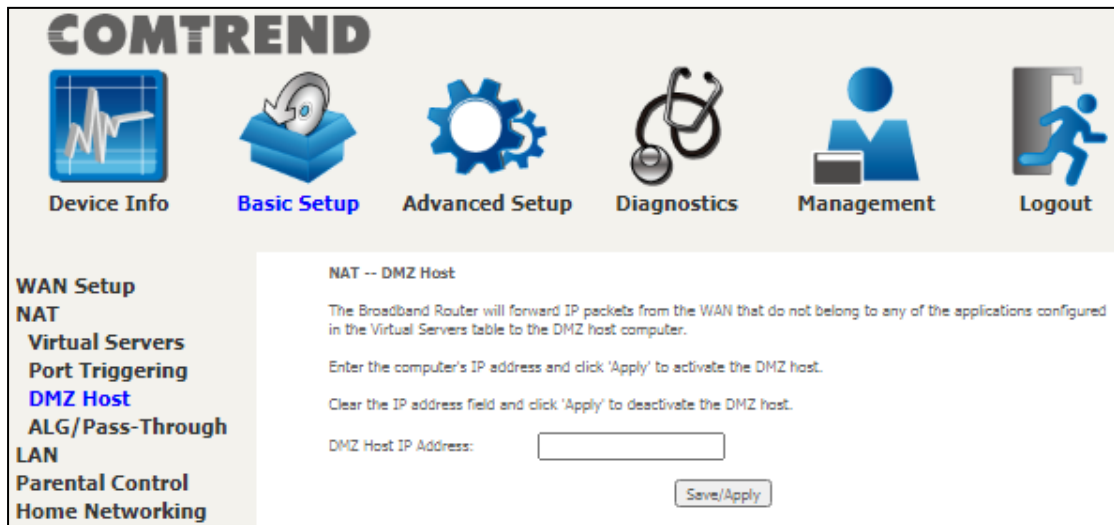


Consult the table below for item descriptions.

Item	Description
Use Interface	Select a WAN interface from the drop-down menu that you want the port triggering rules to apply to.
Select an Application <b>Or</b> Custom Application	User should select the application from the list. <b>Or</b> 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	Select the protocol (TCP, TCP/UDP, or UDP) from the drop-down menu.
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	Select the protocol (TCP, TCP/UDP, or UDP) from the drop-down menu.

### 5.2.3 DMZ Host

The 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.

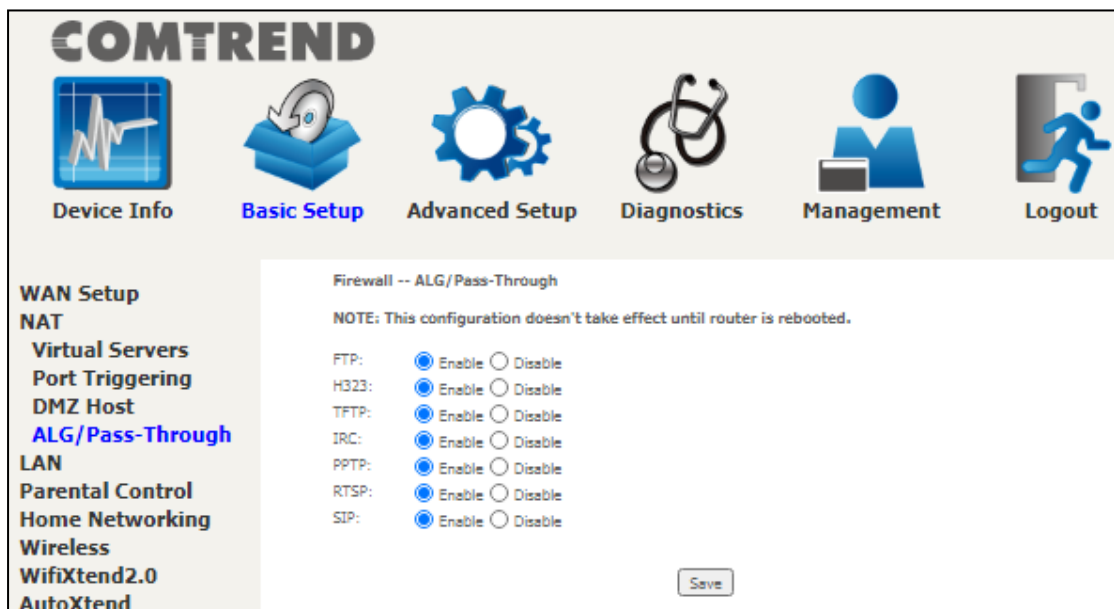


To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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

### 5.2.4 ALG/Passthrough

Supports 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 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.

### 1<sup>st</sup> 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 ticking the checkbox . This will improve bandwidth utilization.

**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 . This will drop all traffic except services which are set in the "Access Control" page.

**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**.

**DHCP Static IP Lease**

Enter the Mac address and Static IP address then click "Apply/Save".

MAC Address:

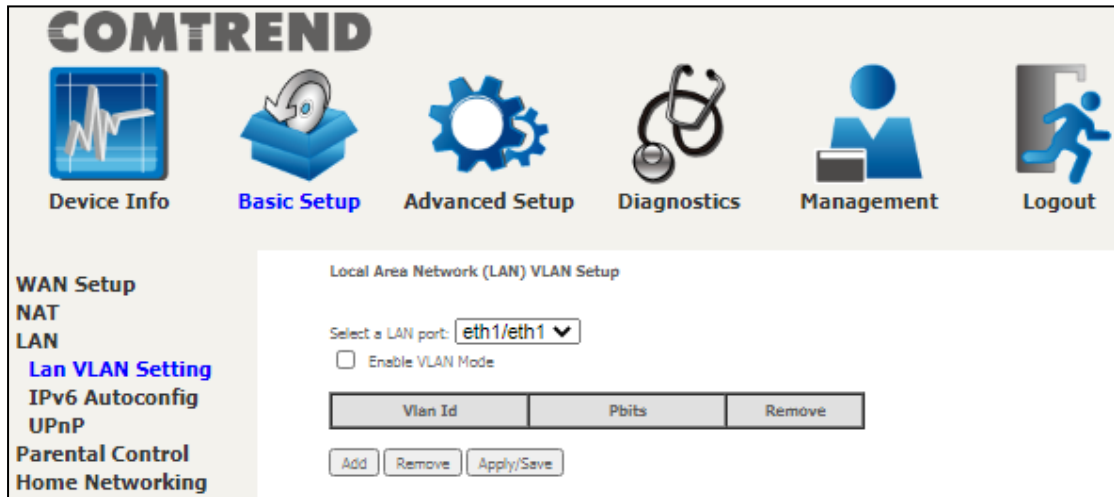
IP Address:

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.



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

Vlan Id	Pbits	Remove
<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>

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

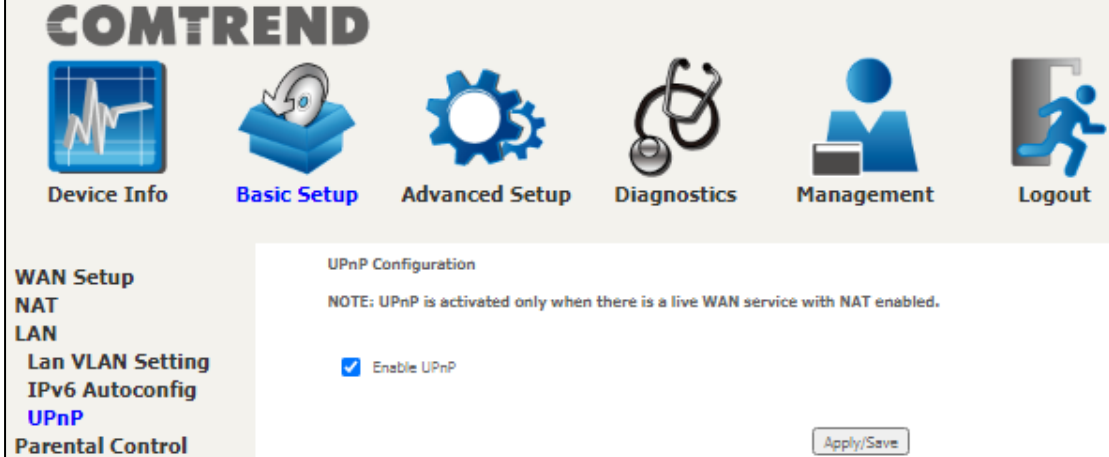
Item	Description
Enable RADVD	Enable use of router advertisement daemon
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Select to use a Randomly Generated Prefix
Statically Configure	Select to manually configure
Prefix	Specify the prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix. When the time threshold is reached, the unique local prefix is no longer valid (-1 means no limit).
Valid Life Time (hour)	The valid life time for this prefix (-1 means limitless)
Enable MLD Snooping	Enable by ticking the checkbox <input checked="" type="checkbox"/> . This will improve bandwidth utilization
Standard 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
Blocking Mode	In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group

Enable MLD LAN  
To LAN Multicast

Enable/disable IPv6 multicast between LAN ports

### 5.3.3 UPnP

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



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. Below this is a sidebar menu with options: WAN Setup, NAT, LAN, Lan VLAN Setting, IPv6 Autoconfig (highlighted), UPnP, and Parental Control. The main content area is titled 'UPnP Configuration' and contains a note: 'NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.' Below the note, there is a checkbox labeled 'Enable UPnP' which is checked. At the bottom right of the configuration area, there is an 'Apply/Save' button.



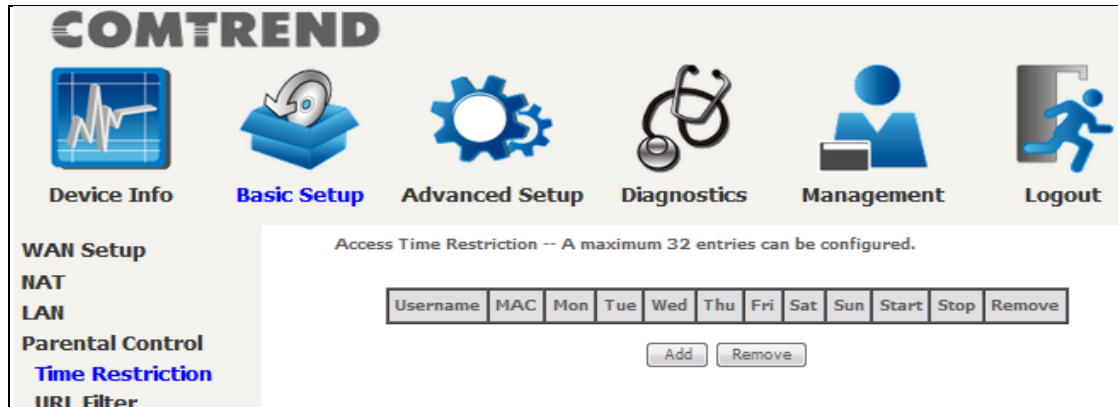
## 5.4 Parental Control

This selection provides WAN access control functionality.

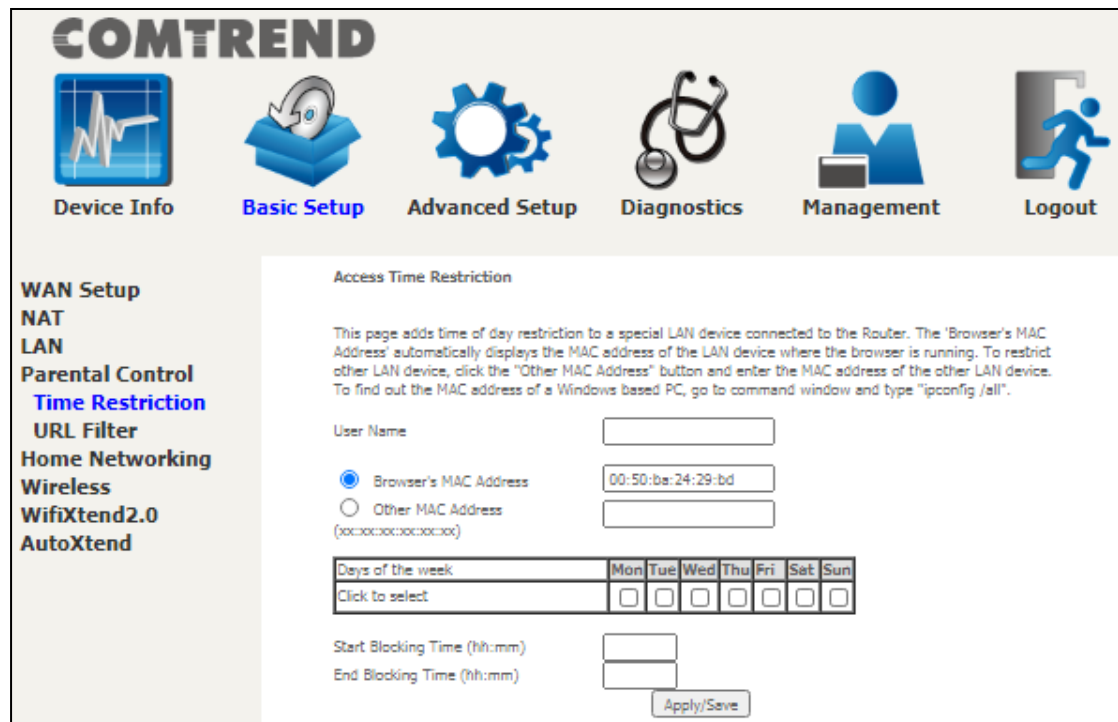
### 5.4.1 Time Restriction

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.

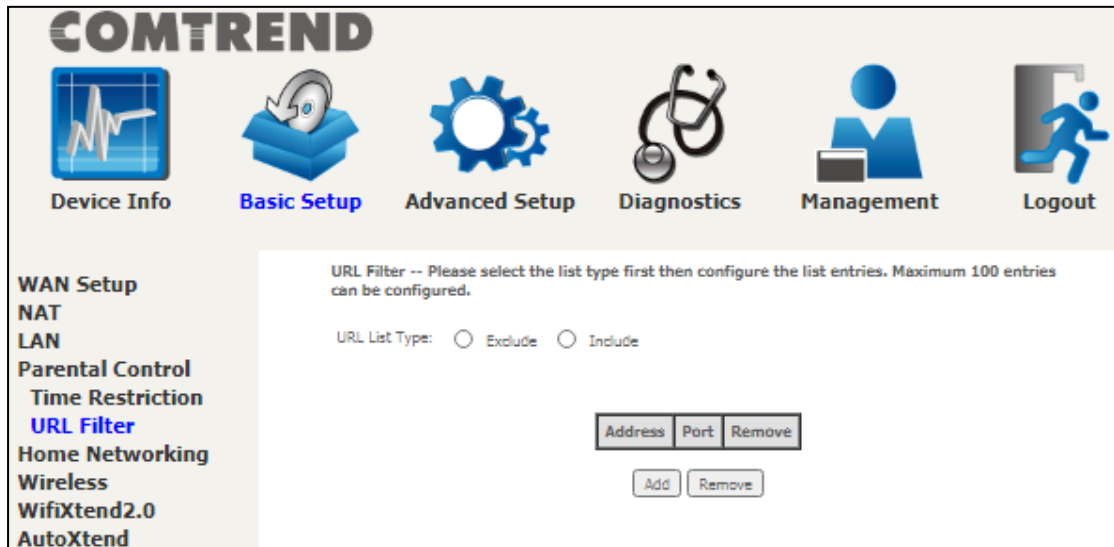


See below for item descriptions. Click **Apply/Save** to add a time restriction.

- 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.

### 5.4.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL (Uniform Resource Locator) 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.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type:  Exclude  Include

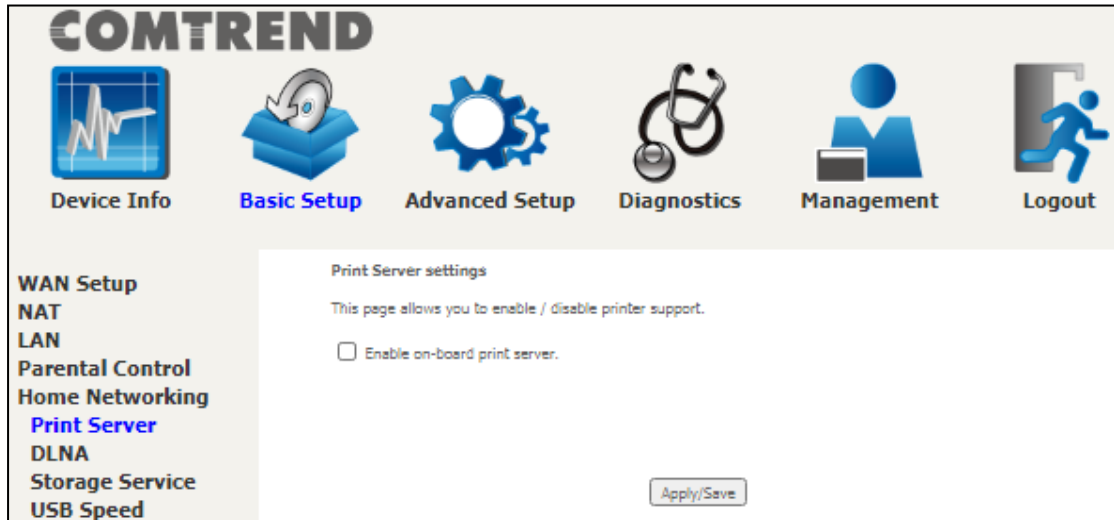
Address	Port	Remove
www.yahoo.com	80	<input type="checkbox"/>

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

## 5.5 Home Networking

### 5.5.1 Print Server

This page allows you to enable or disable printer support.

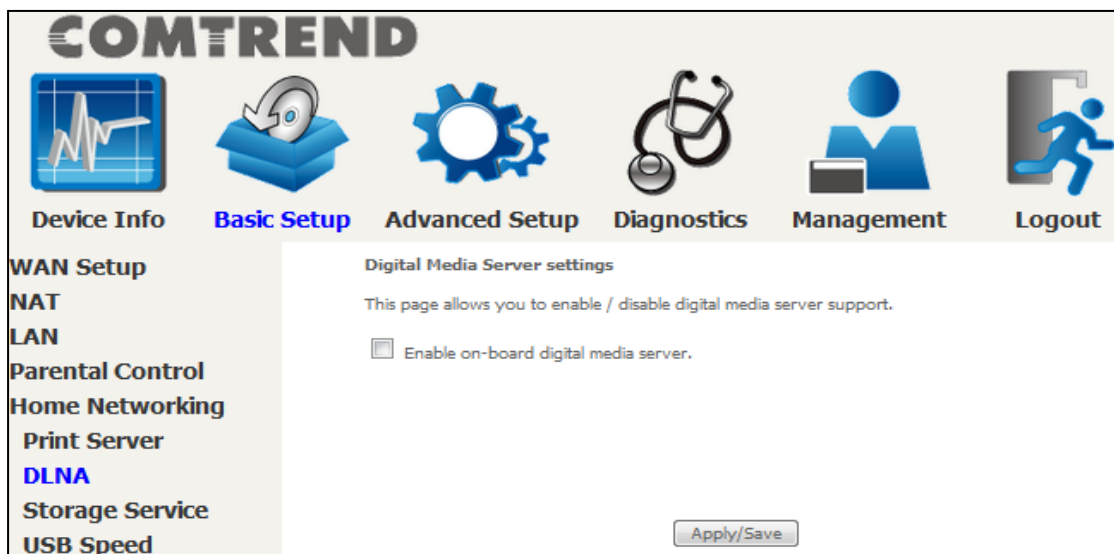


Please reference [Appendix E](#) to see the procedure for enabling the Printer Server.

### 5.5.2 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.



### 5.5.3 Storage Service

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

#### 5.5.3.1 Storage Device Info

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

**COMTREND**

Device Info   **Basic Setup**   Advanced Setup   Diagnostics   Management   Logout

WAN Setup  
NAT  
LAN  
Parental Control  
Home Networking  
Print Server  
DLNA  
Storage Service  
**Storage Device Info**  
User Accounts

**Storage Service**

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

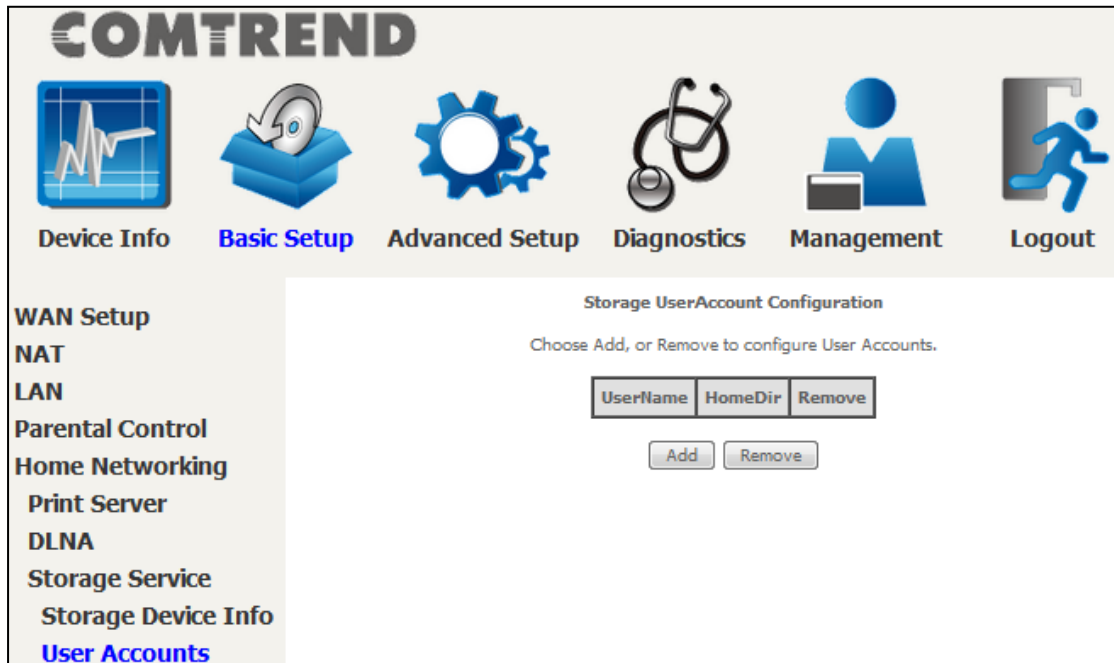
Volumename	FileSystem	Total Space	Used Space
disk1_1	fat	962	6

Display after storage device attached (for your reference).

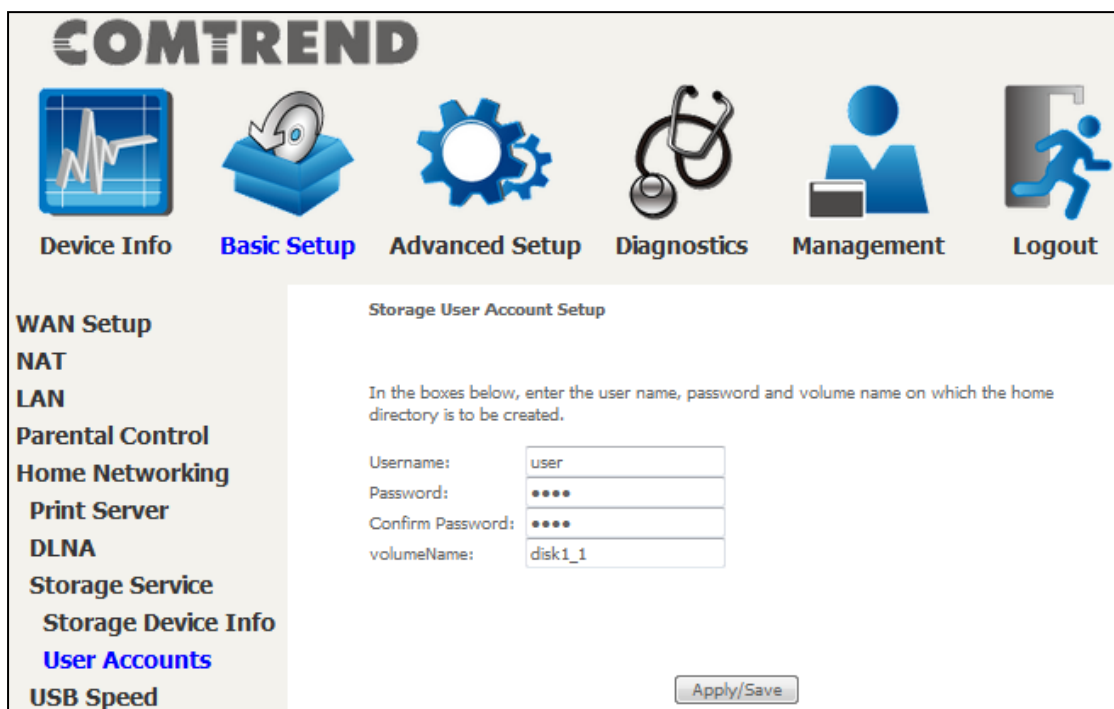
Volumename	FileSystem	Total Space	Used Space
disk1_1	fat	962	6

### 5.5.3.2 Storage User Accounts

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

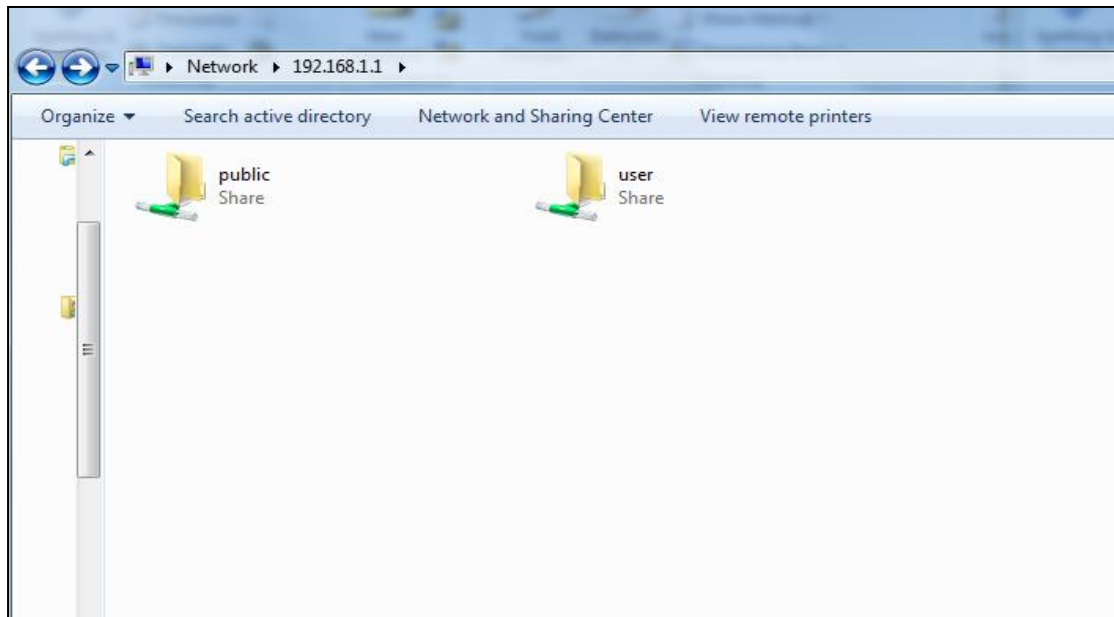


Click the **Add** button to display the following. volumeName would be disk1\_1 if only 1 USB has been plugged into the device.



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.



### 5.5.4 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



## 5.6 Wireless

### 5.6.1 SSID

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

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup  
NAT  
LAN  
Parental Control  
Home Networking  
Wireless  
SSID  
Security  
WifiXtend2.0  
AutoXtend

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

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

BSS-MAC (SSID): D8:B6:B7:59:55:02 (Comtrend5501\_2.4GHz enabled) ▼

BSS Enabled: Enabled ▼

Network Name (SSID): Comtrend5501\_2.4GHz

Network Type: Open ▼

AP Isolation: Off ▼

BSS Max Associations Limit: 64

WMM Advertise: Advertise ▼

WMF: On ▼

Apply Cancel

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 <b>Closed</b> hides the network from active scans. Selecting <b>Open</b> reveals the network from active scans.
AP Isolation	Selecting <b>On</b> enables AP Isolation mode. When enabled, STAs associated with the AP will not be able to communicate with each other.
BSS Max Associations Limit	Sets the maximum associations for this BSS



WMM Advertise	When WMM (Wireless MultiMedia) is enabled for the radio, selecting <b>On</b> allows WMM to be advertised in beacons and probes for this BSS. <b>Off</b> disables advertisement of WMM in beacons and probes.
WMF	Choose <b>On</b> to enable Wireless Multicast Forwarding on this BSS. <b>Off</b> disables this feature.

### 5.6.2 Security

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

The screenshot shows the Comtrend web interface with a navigation menu at the top: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left sidebar, the 'Wireless' section is expanded to show 'Security'. The main content area is titled 'SECURITY' and contains the following configuration options:

- Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) [Select]
- 802.11 Authentication: Open
- 802.1X Authentication: Disabled
- WPA: Disabled
- WPA-PSK: Disabled
- WPA2: Disabled
- WPA2-PSK: Enabled
- WPA3-SAE: Disabled
- WPA Encryption: AES
- RADIUS Server: 0.0.0.0
- RADIUS Port: 1812
- RADIUS Key: [Masked]
- WPA passphrase: [Masked] [Click here to display](#)
- Protected Management Frames: Capable
- Network Key Rotation Interval: 0
- Pairwise Key Rotation Interval: 0
- Network Re-auth Interval: 36000

Buttons for 'Apply' and 'Cancel' are located at the bottom of the configuration area.

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).

This close-up shows the '802.11 Authentication:' dropdown menu with a mouse cursor hovering over it. A tooltip box is displayed over the dropdown, containing the text: 'Selects 802.11 authentication method. Open or Shared. OSEN:'. The dropdown menu is currently set to 'Open'.

The descriptions are also shown below.

Item	Description
Wireless Interface	Select which wireless interface to configure
802.11 Authentication	Select 802.11 authentication method. Open or Shared.
802.1X Authentication	Select Network authentication type
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
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.

## 5.7 WifiXtend 2.0

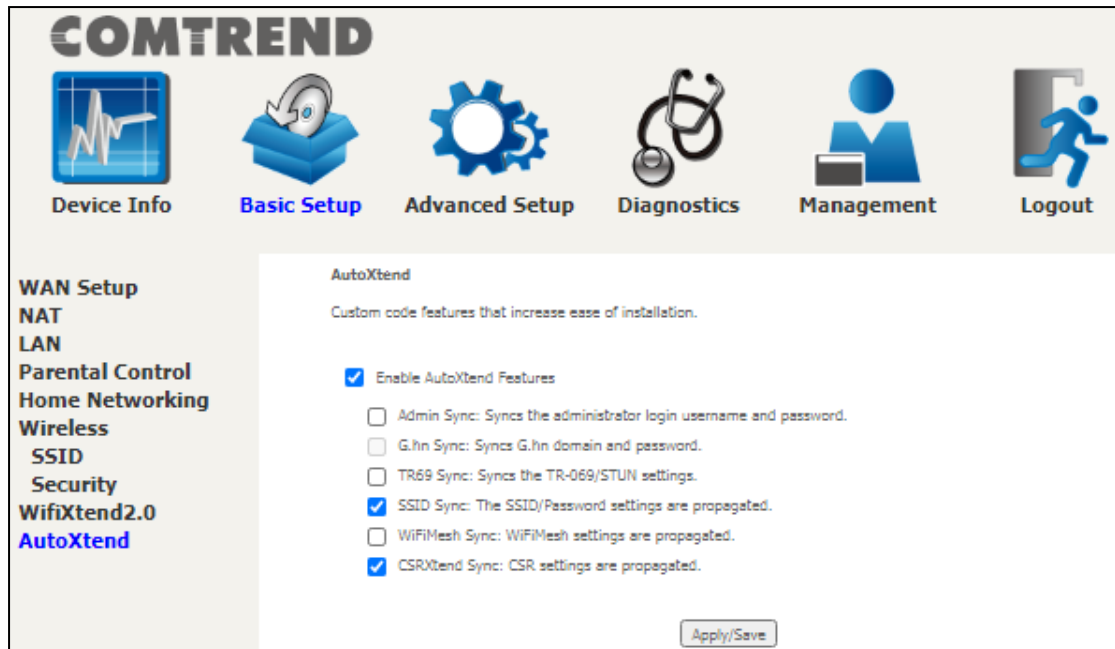
**WifiXtend** is a function to construct and optimize a mesh-network. Check the checkbox and click the **Apply/Save** button to enable **WifiXtend**.



To enable the end-user WiFi optimization via mesh-enhanced technology, check the checkbox and click the **Apply/Save** button.

## 5.8 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.

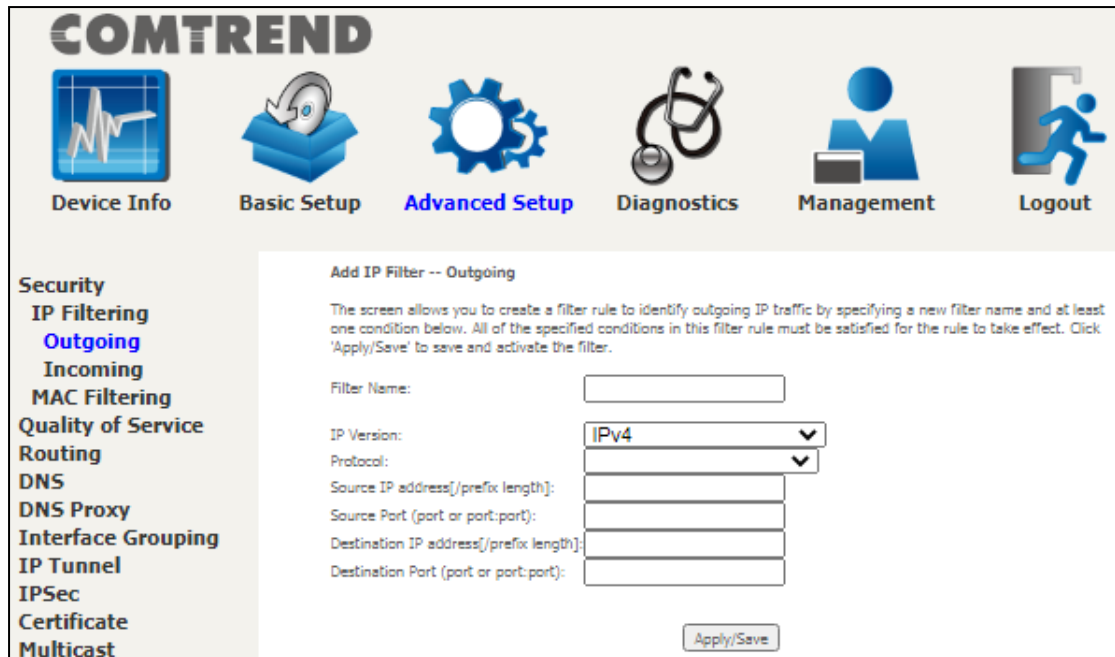
#### OUTGOING IP FILTER

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. Below this, a sidebar on the left lists 'Security' options: IP Filtering (with 'Outgoing' selected), Incoming, MAC Filtering, and Quality of Service. The main content area is titled 'Outgoing IP Filtering Setup' and contains the following text: 'By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters.' Below the text is a table with the following columns: Filter Name, IP Version, Protocol, SrcIP/ PrefixLength, SrcPort, DstIP/ PrefixLength, DstPort, and Remove. At the bottom of the table are 'Add' and 'Remove' buttons.

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.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

**Security**  
 IP Filtering  
**MAC Filtering**  
 Quality of Service  
 Routing  
 DNS  
 DNS Proxy  
 Interface Grouping  
 IP Tunnel  
 IPSec  
 Certificate  
 Multicast  
 Wireless  
 WifiXtend2.0  
 AutoXtend

**MAC Filtering Setup**

MAC Filtering is only effective on WAN services configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:  
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
eth0.1	<b>FORWARD</b>	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

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.

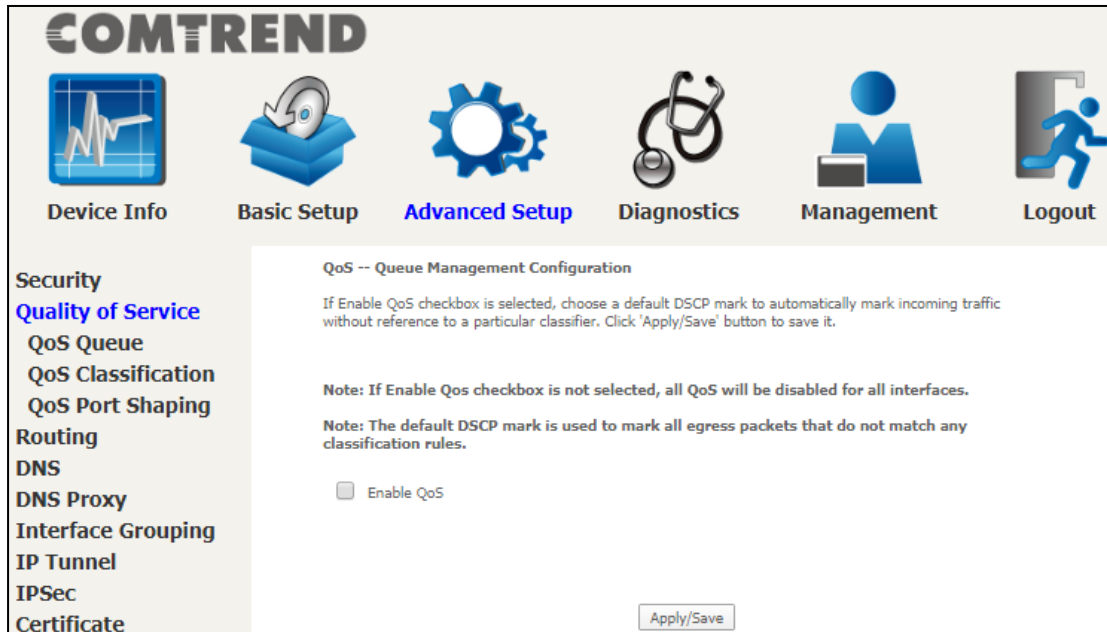
Item	Description
Protocol Type	Select from the drop down menu the protocol (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP) that will apply to this rule.
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing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

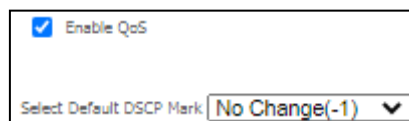
To Enable QoS tick the checkbox  and select a Default DSCP Mark.

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).

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

**Security**

**Quality of Service**

**QoS Queue**

Queue Configuration

Wlan Queue

QoS Classification

QoS Port Shaping

**Routing**

DNS

DNS Proxy

Interface Grouping

IP Tunnel

IPSec

Certificate

Multicast

Wireless

WifiXtend2.0

AutoXtend

**QoS Queue Setup**

For each Ethernet interface, maximum 8 queues can be configured.  
 For each Ethernet WAN interface, maximum 8 queues can be configured.  
 To add a queue, click the Add button.  
 To remove queues, check their remove-checkboxes, then click the Remove button.  
 The Enable button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.  
 The enable-checkbox also shows status of the queue after page reload.

Note: Ethernet LAN queue configuration only takes effect when all the queues of the interface have been configured.  
 The QoS function has been disabled. Queues would not take effects.

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

Add
Enable
Remove

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

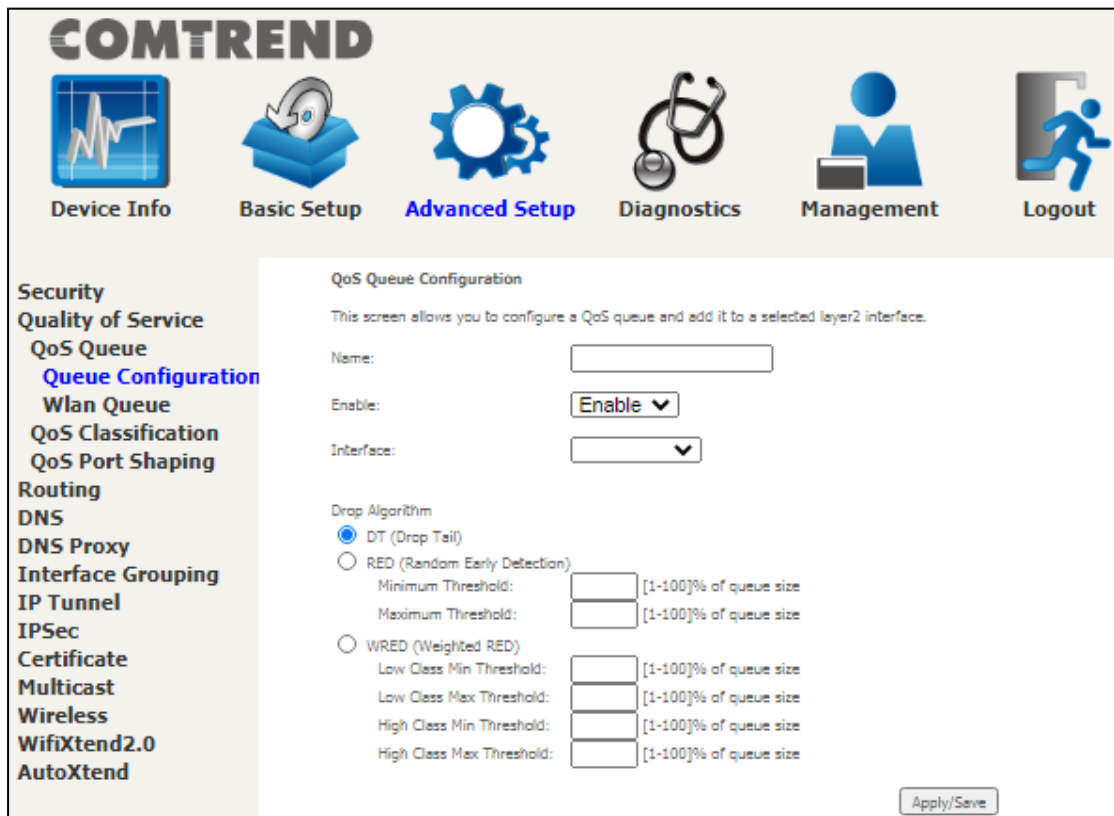
The **Enable** button will scan through every queue in the table. Queues with the enable-checkbox checked will be enabled. Queues with the enable-checkbox un-checked will be disabled.

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).

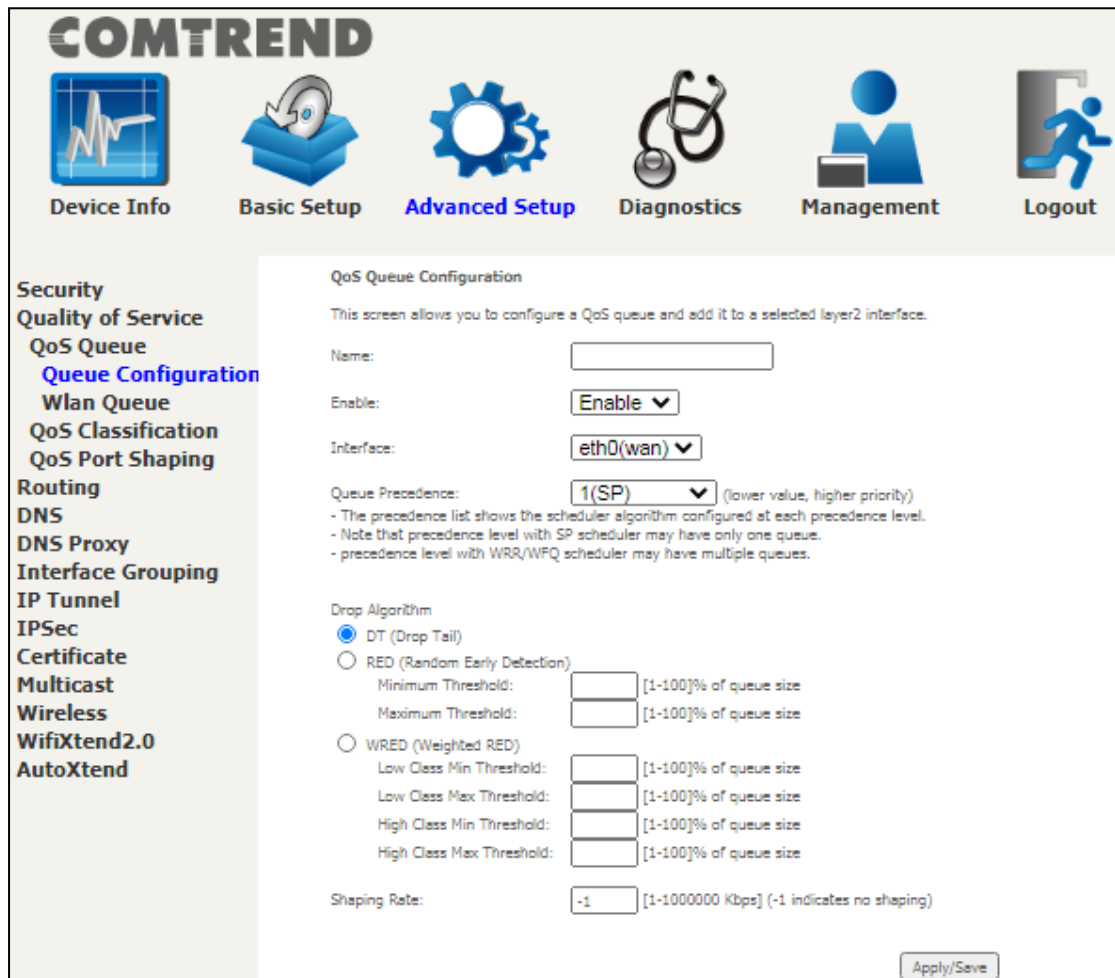
**Drop Algorithm:** Select the algorithm to be used to ensure that the QoS rule is enforced if the traffic exceeds the configured limit.

**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.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
QoS Queue  
Queue Configuration  
**Wlan Queue**  
QoS Classification  
QoS Port Shaping  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
WifiXtend2.0  
AutoXtend

**QoS Wlan Queue Setup**

Note: If WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

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.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.  
 To remove rules, check their remove-checkboxes, then click the **Remove** button.  
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.  
 The enable-checkbox also shows status of the rule after page reload.  
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS						
Class Name	Order	Class	Ether Intf	SrcMAC/Mask	DstMAC/Mask	SrcIP/PrefixLength	DstIP/PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

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.

**Add Network Traffic Class Rule**

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.  
 Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:  ▾

Rule Status:  ▾

**Specify Classification Criteria** (A blank criterion indicates it is not used for classification.)

Ingress Interface:  ▾

Ether Type:  ▾

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

**Specify Classification Results** (A blank value indicates no operation.)

Specify Egress Interface (Required):  ▾

Specify Egress Queue (Required):  ▾

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):  ▾

Mark 802.1p priority:  ▾

- 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:  [Kbits/s]

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.
<b>Classification Criteria</b>	
Ingress Interface	Select an interface: (i.e. LAN, WAN, local, ETH1, ETH2, ETH3, w10)
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.
<b>Classification Results</b>	
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.

	<ul style="list-style-type: none"><li>- 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.</li><li>- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.</li><li>- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.</li></ul>
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.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
QoS Queue  
QoS Classification  
**QoS Port Shaping**  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
WifiXtend2.0  
AutoXtend

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.  
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate (Mbps)	Burst Size (bytes)	Enable
eth0	WAN	-1	0	<input type="checkbox"/>
eth1	LAN	-1	0	<input type="checkbox"/>
eth2	LAN	-1	0	<input type="checkbox"/>
eth3	LAN	-1	0	<input type="checkbox"/>
eth4	LAN	-1	0	<input type="checkbox"/>
eth5	LAN	-1	0	<input type="checkbox"/>

Apply/Save

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

## 6.3 Routing

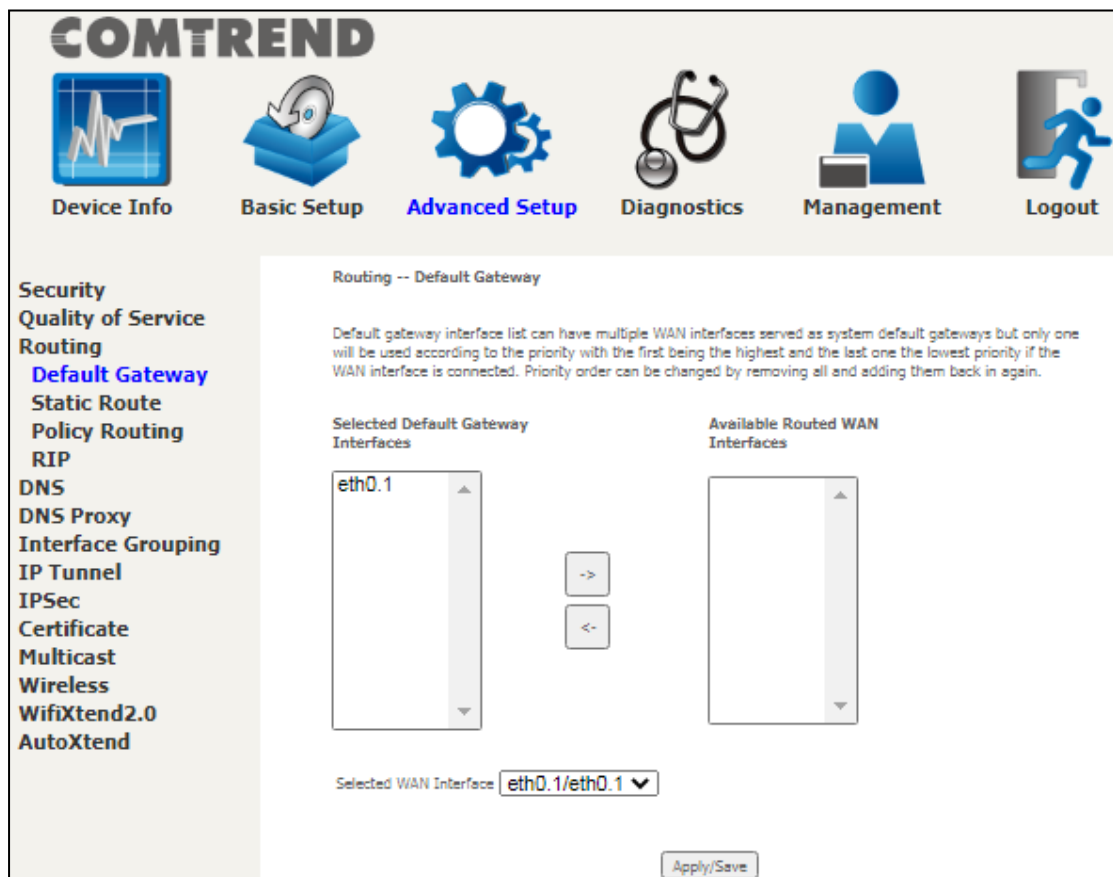
The following routing functions are accessed from this menu:

**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

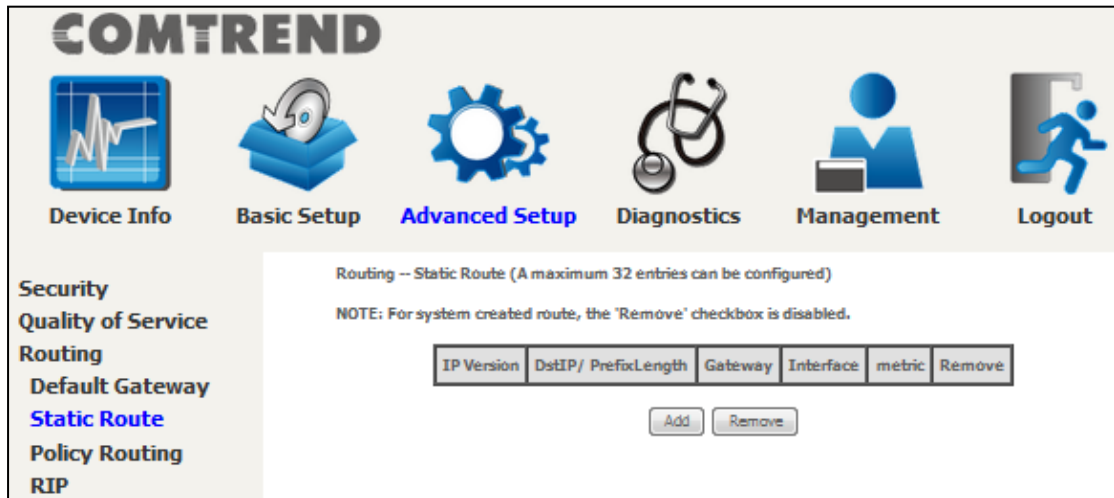
The default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing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



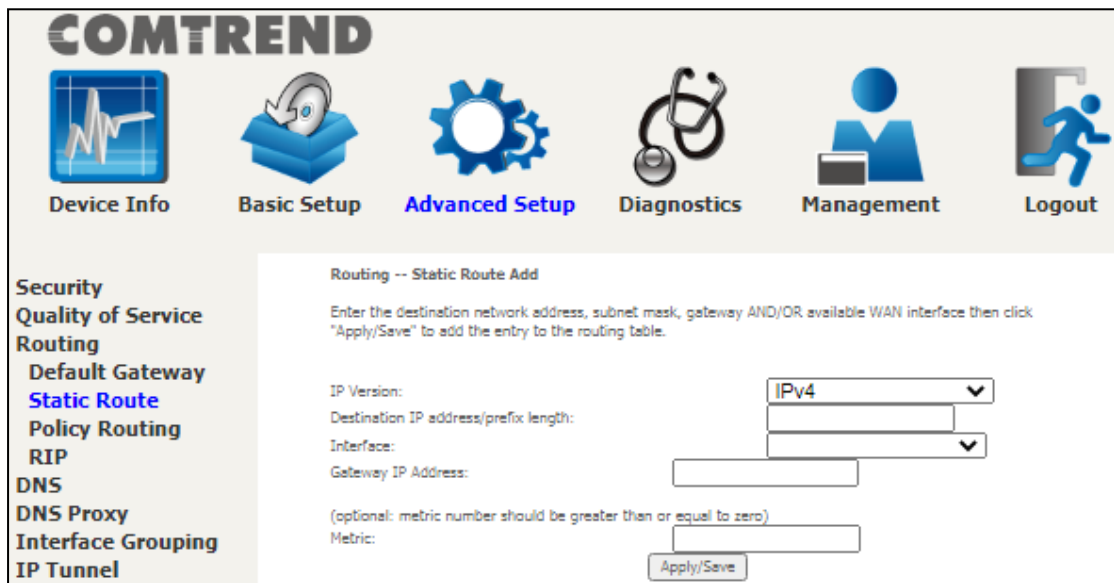
Click **Apply/Save** to apply and save the settings.

### 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.



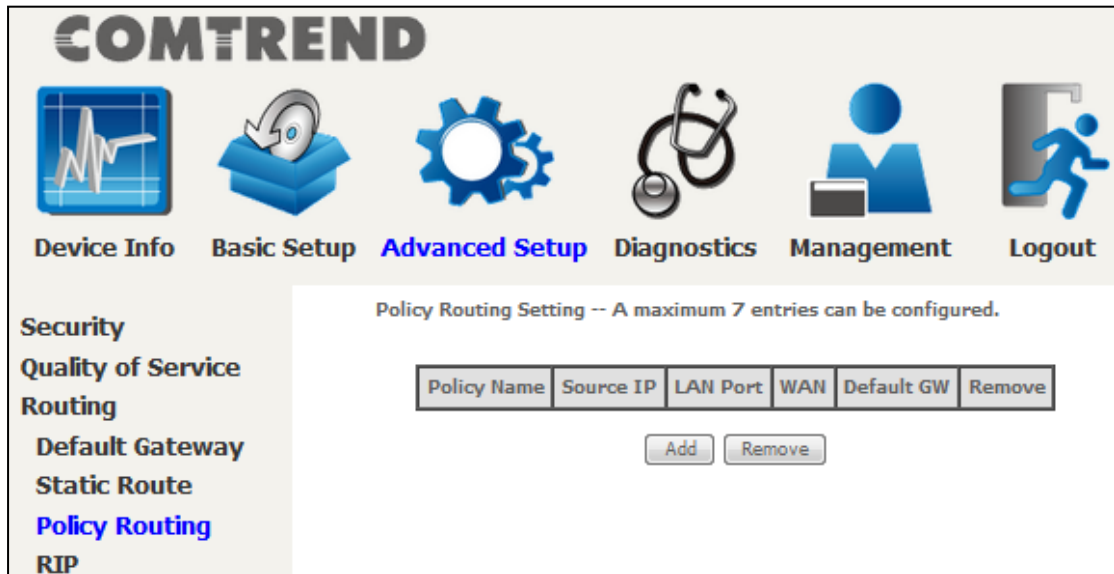
- **IP Version:** Select the IP version to be IPv4 or IPv6.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** Select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing. . Enter a number greater than or equal to 0.

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

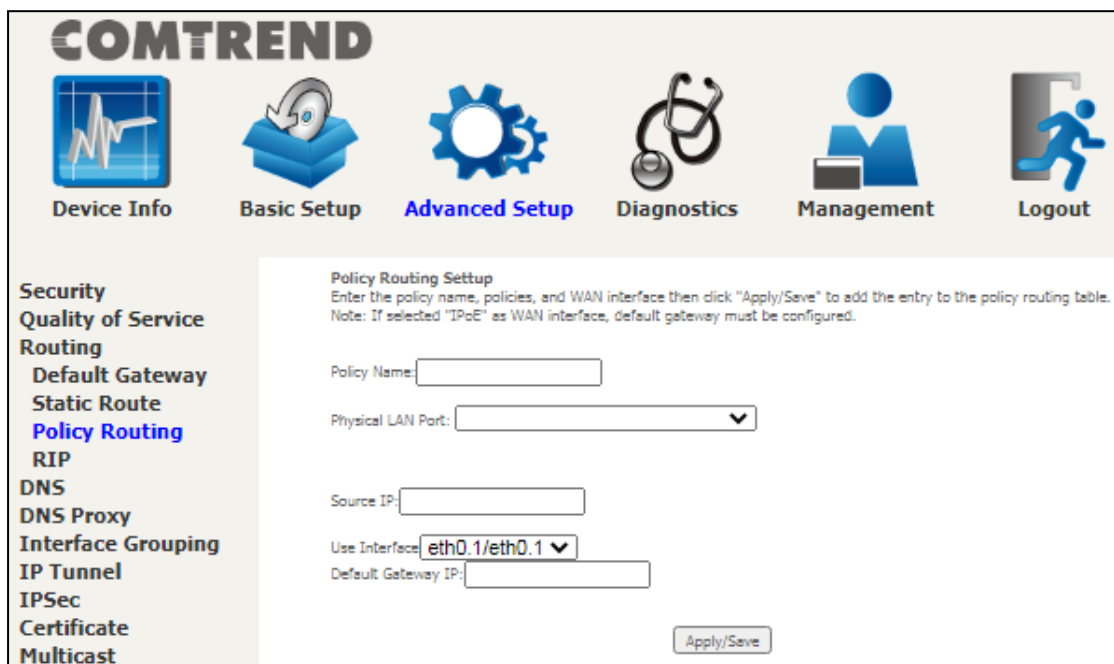
### 6.3.3 Policy Routing

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.



<b>Item</b>	<b>Description</b>
Policy Name	Name of the route policy rule
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Select the interface that traffic will be directed to
Default Gateway IP	Enter the 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**.

**COMTREND**

Device Info    Basic Setup    **Advanced Setup**    Diagnostics    Management    Logout

Security  
Quality of Service  
Routing  
Default Gateway  
Static Route  
Policy Routing  
**RIP**  
DNS  
DNS Proxy  
Interface Grouping

Routing -- RIP Configuration

NOTE: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
eth0.1	2	Passive	<input type="checkbox"/>

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.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
 DNS Server  
 Dynamic DNS  
 DNS Entries  
 DNS Proxy  
 Interface Grouping  
 IP Tunnel  
 IPsec  
 Certificate  
 Multicast  
 Wireless  
 WifiXtend2.0  
 AutoXtend

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN with 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

eth0.1

Use the following Static DNS IP address:  
 Primary DNS server:   
 Secondary DNS server:

Obtain IPv6 DNS info from a WAN interface:  
 WAN Interface selected:

Use the following Static IPv6 DNS address:  
 Primary IPv6 DNS server:   
 Secondary IPv6 DNS server:

Apply/Save

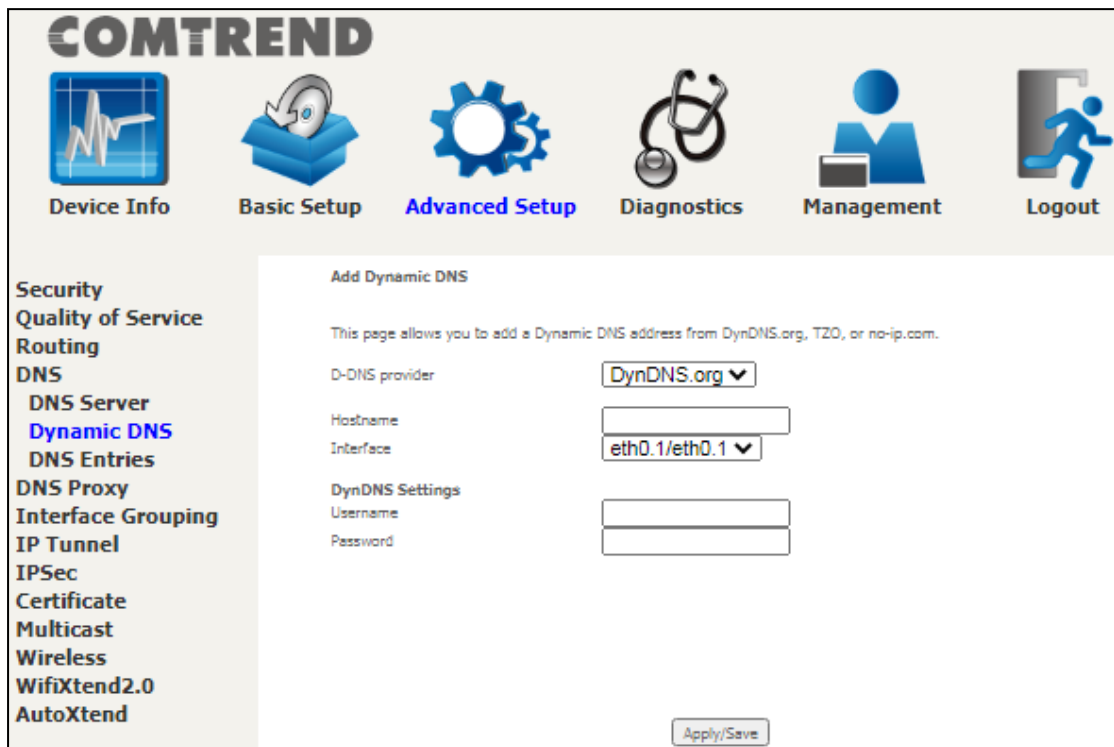
Click **Apply/Save** to save the new configuration.

### 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.



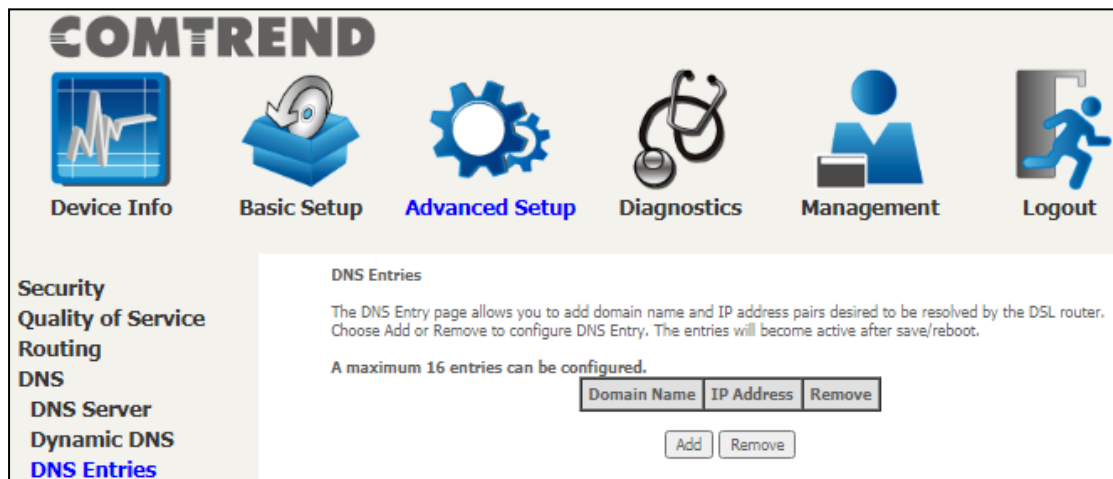
Click **Apply/Save** to save your settings.

Consult the table below for item descriptions.

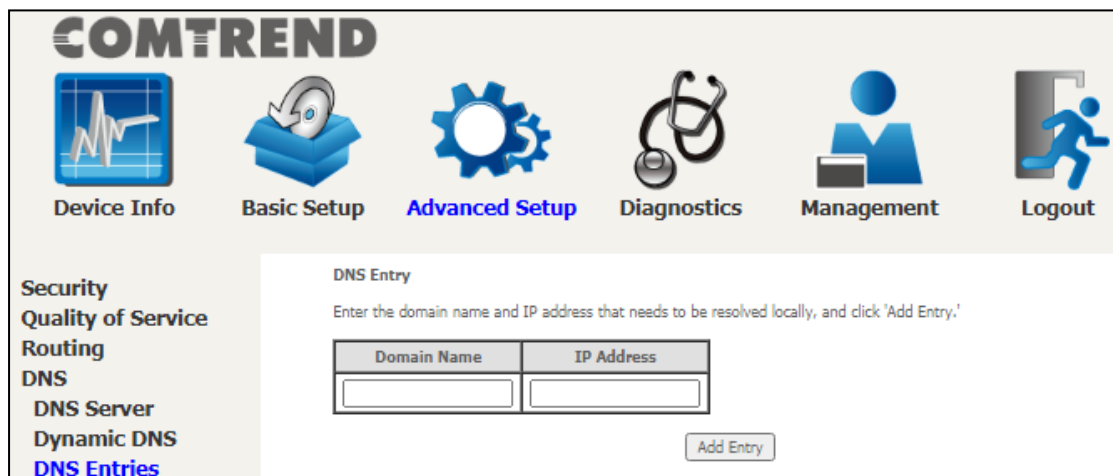
Item	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the drop-down menu
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

### 6.4.3 DNS Entries

The DNS Entry page allows you to add domain names and IP address pairs desired to be resolved by the 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 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".

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
**DNS Proxy**  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless

DNS Proxy Configuration

Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

DNS Relay Configuration  
This controls the DHCP Server to assign public DNS.

Enable DNS Relay

Apply/Save

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

## 6.6 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.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
**DNS Proxy**  
**Interface Grouping**  
**IP Tunnel**  
**IPSec**  
**Certificate**  
**Multicast**  
**Wireless**  
**WifiXtend2.0**  
**AutoXtend**

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to WAN and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs	MAC Address
Default		eth0.1	eth1.0		
			eth2.0		
			eth3.0		
			eth4.0		
			eth5.0		
			Comtrend5501_2.4GHz		
			Comtrend5501_5GHz		

Add Remove

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.



Device Info



Basic Setup



Advanced Setup



Diagnostics



Management



Logout

- Security
- Quality of Service
- Routing
- DNS
- DNS Proxy
- Interface Grouping
- IP Tunnel
- IPSec
- Certificate
- Multicast
- Wireless
- WifiXtend2.0
- AutoXtend

Interface grouping Configuration

This feature allows you to set ports or devices connected to either LAN or WLAN to use a specific WAN interface. This feature can be either a static or dynamic approach. Using the Vendor ID or Any Port, Any WAN option is an option for a dynamic configuration.

Here are the steps to create an Interface Group feature:

**Step 1.** Enter the Group Name. Each group name must be unique when creating multiple groups.

**Step 2.** Select WAN Interface that the group will associate to. Click on the WAN interface from the Available WAN Interfaces column, then move it to the Grouped WAN Interfaces column. Use the Arrow button to move the interfaces between columns.

**Step 3.** Choose from the 3 options that best suit your needs: [a.] Grouped LAN interface, [b.] Vendor ID OR [c.] MAC address for Any port, Any WAN.

[a.] The Grouped LAN interfaces option designates a port(s) to that specified WAN Interfaces group. Click on the LAN and WLAN interfaces you choose to associate. Use the Arrow button to toggle the LAN/WLAN interfaces to the other column.

[b.] The Vendor ID option will automatically add LAN or WLAN clients port(s) or WLAN SSID to the Grouped LAN Interfaces based on the Vendor ID in the DHCP Discover from the connected LAN client. Add the DHCP Vendor ID string from the LAN Client. If you do not know the Vendor ID, either you can check with the manufacturer or take a packet capture to identify the Vendor ID in the DHCP Discover packet.

[c.] The MAC Address Match List for Any Port, Any WAN option automatically adds LAN or WLAN clients port(s) or WLAN SSID to the Grouped LAN Interfaces based on the MAC Address. Add the MAC address for those devices that need to be associated to the specific WAN Interface. Using the MAC OUI (first 6 characters of the MAC address) is acceptable but you will need to fill in the rest of the MAC address using the "xx" as a wild card. For example, d8:b6:b7:a1:87:6d will have a MAC OUI of d8:b6:b7. To use the wild card you will enter d8:b6:b7:xx:xx:xx.

**Step 4.** Click Apply/Save button to make the changes effective immediately.

**IMPORTANT:** If a Vendor ID or MAC address is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to request an IP address and associate the port to the appropriate Group.

Group Name:

Grouped WAN Interfaces

->
<-

Available WAN Interfaces

eth0.1/eth0.1

Grouped LAN Interfaces

Available LAN Interfaces

Comtrend5501\_2.4GHz  
 Comtrend5501\_5GHz  
 eth1.0  
 eth2.0  
 eth3.0  
 eth4.0  
 eth5.0

Automatically Add Clients With the following DHCP Vendor IDs


MAC Address Match List for Any Port Any Wan


Apply/Save



**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.

## 6.7 IP Tunnel

### 6.7.1 IPv6inIPv4

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

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
**IPv6inIPv4**  
IPv4inIPv6  
MAP

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

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

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
**IPv6inIPv4**  
IPv4inIPv6  
MAP  
IPSec  
Certificate  
Multicast  
Wireless

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism: 6RD

Associated WAN Interface:

Associated LAN Interface: LAN/br0

Manual  Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

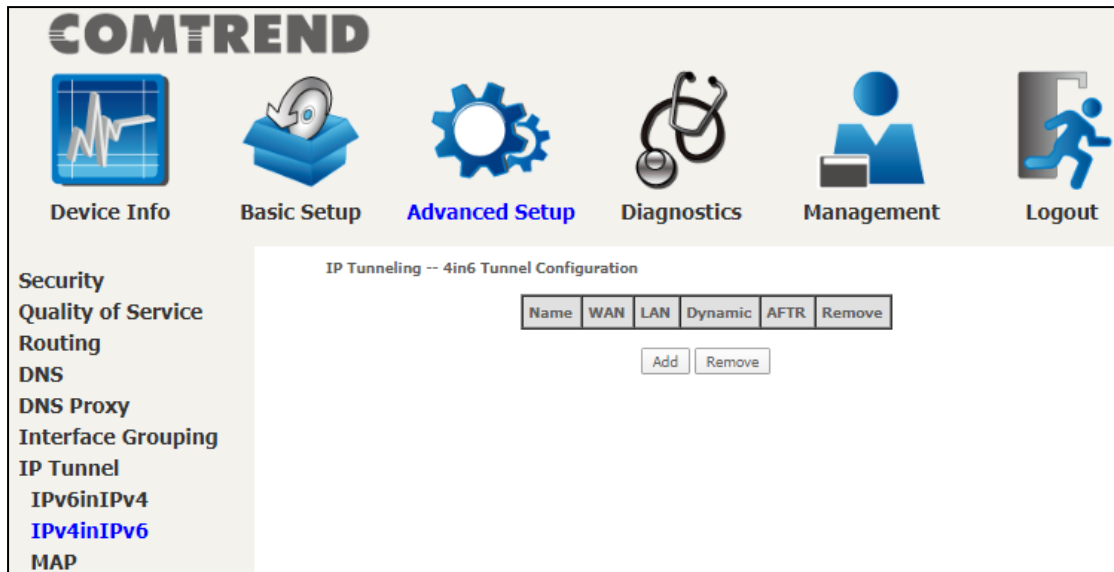
Click **Apply/Save** to apply and save the settings.

Item	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment

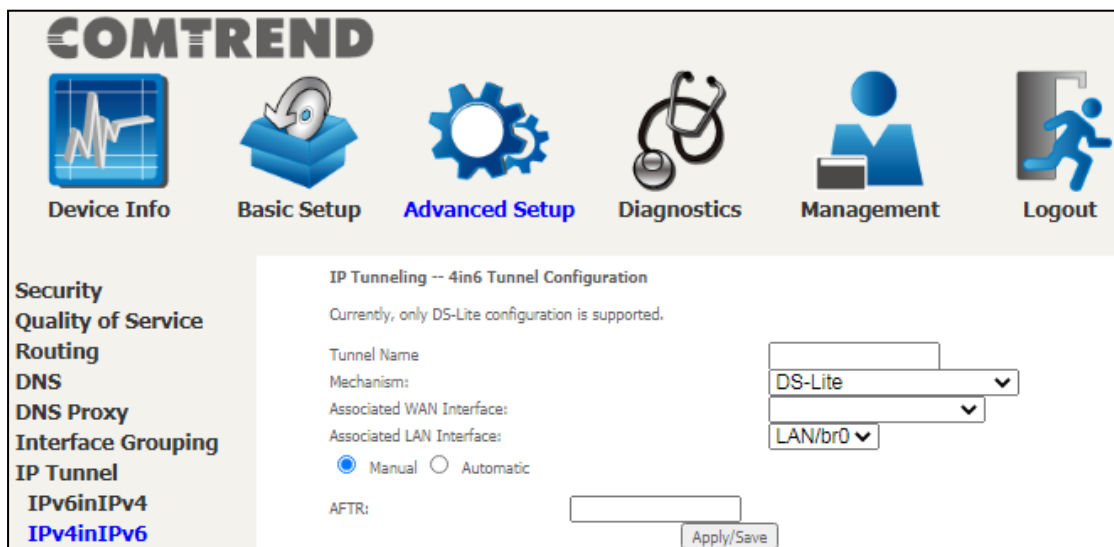
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used 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

### 6.7.2 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

### 6.7.3 MAP

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

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPv6inIPv4  
IPv4inIPv6  
**MAP**

MAP -- MAP-T/MAP-E Configuration

Mechanism	WAN	Dynamic	BR Prefix	BMR IPv6 Prefix	BMR IPv4 Prefix	PSID Offset	PSID Length	PSID	Remove

Add Remove

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

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPv6inIPv4  
IPv4inIPv6  
**MAP**  
IPSec  
Certificate  
Multicast  
Wireless  
WifiXtend2.0

MAP -- MAP-T/MAP-E Configuration

Mechanism: MAP-T

Associated WAN Interface: [ ]

Associated LAN Interface: LAN/br0

Manual  Automatic

BR IPv6 Prefix: [ ]

BMR IPv6 Prefix: [ ]

BMR IPv4 Prefix: [ ]

PSID Offset: [ ]

PSID Length: [ ]

PSID Value: [ ]

Apply/Save

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

## 6.8 IPSec

### 6.8.1 IPSec Tunnel Mode Connections

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

**COMTREND**

Device Info    Basic Setup    **Advanced Setup**    Diagnostics    Management    Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
  IPv6inIPv4  
  IPv4inIPv6  
  MAP  
**IPSec**

**IPSec Tunnel Mode Connections**  
Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	IP Version	Tunnel Mode	Key Exchange Method	Local Gateway Interface	Remote Gateway	Local Addresses	Remote Addresses	Remove
<input type="button" value="Add New Connection"/> <input type="button" value="Remove"/>								

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

The following screen will display.

The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below this is a sidebar menu with the following items: Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPv6inIPv4, IPv4inIPv6, MAP, IPsec, Certificate, Multicast, Wireless, WifiXtend2.0, and AutoXtend. The main content area is titled 'IPSec Settings' and contains the following configuration fields:

- IPSec Connection Name: new connection
- IP Version: IPv4
- Tunnel Mode: ESP
- Local Gateway Interface: Select interface
- Remote IPsec Gateway Address: 0.0.0.0
- Tunnel access from local IP addresses: Subnet
- IP Address for VPN: 0.0.0.0
- Mask or Prefix Length: 255.255.255.0
- Tunnel access from remote IP addresses: Subnet
- IP Address for VPN: 0.0.0.0
- Mask or Prefix Length: 255.255.255.0
- Key Exchange Method: Auto(IKEv1)
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: key
- Perfect Forward Secrecy: Disable
- Advanced IKE Settings: Show Advanced Settings

At the bottom right of the configuration area, there is an 'Apply/Save' button.

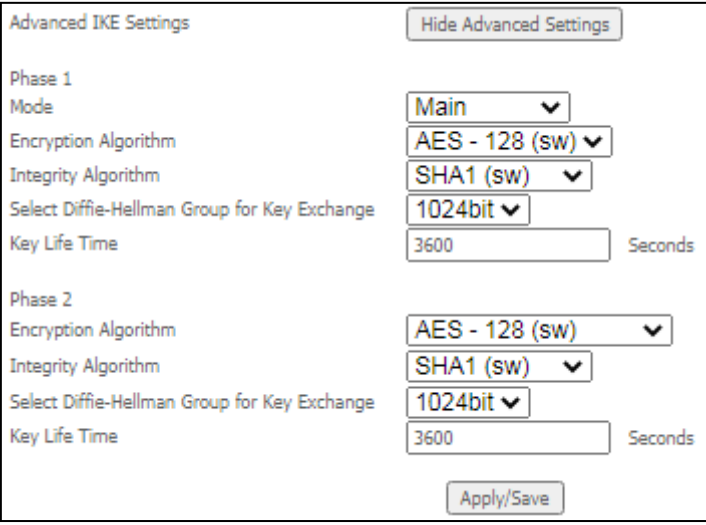
Heading	Description
IPSec Connection Name	User-defined label
IP Version	Select the corresponding IPv4 / IPv6 version for the IPSEC connection
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Local Gateway Interface	Select from the 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 <b>Single</b> or <b>Subnet</b> .



IP Address/Subnet Mask for VPN	If you chose <b>Single</b> , please enter the host IP address for VPN. If you chose <b>Subnet</b> , please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose <b>Single</b> or <b>Subnet</b> .
IP Address/Subnet Mask for VPN	If you chose <b>Single</b> , please enter the host IP address for VPN. If you chose <b>Subnet</b> , 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 <b>Show Advanced Settings</b> to reveal the advanced settings options shown below.
	
Advanced IKE Settings	Select <b>Hide Advanced Settings</b> 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**

Key Exchange Method	Manual ▼
Encryption Algorithm	AES ▼
Encryption Key	<input style="width: 100%;" type="text"/> <small>Hex value: DES - 16 digit, 3DES - 48, AES 32, 48, 64 digit</small>
Authentication Algorithm	SHA1 ▼
Authentication Key	<input style="width: 100%;" type="text"/> <small>Hex value: MD5 - 32 digit, SHA1 - 40 digit</small>
SPI	<input style="width: 100%;" type="text" value="101"/> <small>Hex value: 100-FFFFFFFF</small>
<input type="button" value="Apply/Save"/>	

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

## 6.9 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.

### 6.9.1 Local

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. Below this is a sidebar menu with categories: Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPSec, Certificate, **Local**, and Trusted CA. The main content area is titled 'Local Certificates' and contains the following text: 'Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.' Below the text is a table with the following header: 

Name	In Use	Subject	Type	Action
------	--------	---------	------	--------

. At the bottom of the main content area, there are two buttons: 'Create Certificate Request' and 'Import Certificate'.

**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.

The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with icons and labels for: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below this, a left-hand navigation menu lists various system settings: Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPSec, Certificate (with 'Local' selected), Trusted CA, Multicast, Wireless, WifiXtend2.0, and AutoXtend. The main content area is titled 'Import certificate' and contains the following elements:

- Instruction: Enter certificate name, paste certificate content and private key.
- Field: Certificate Name: [input box]
- Field: Certificate: [text area containing: -----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----]
- Field: Private Key: [text area containing: -----BEGIN RSA PRIVATE KEY-----<br><insert private key here><br>-----END RSA PRIVATE KEY-----]
- Button: Apply

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

### 6.9.2 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.

## 6.10 Multicast

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

The screenshot shows the COMTREND web interface with a navigation menu on the left and a main configuration area. The navigation menu includes: Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPsec, Certificate, **Multicast**, Wireless, WifiXtend2.0, and AutoXtend. The main configuration area is titled 'COMTREND' and contains several sections:

- Multicast Precedence:** A dropdown menu set to 'Disable' with a note 'lower value, higher priority'.
- Multicast Strict Grouping Enforcement:** A dropdown menu set to 'Disable'.
- IGMP Configuration:** A section with the instruction 'Enter IGMP protocol configuration fields if you want modify default values shown below.' It includes input fields for:
  - Default Version: 3
  - Query Interval: 125
  - Query Response Interval: 10
  - Last Member Query Interval: 10
  - Robustness Value: 2
  - Maximum Multicast Groups: 25
  - Maximum Multicast Data Sources (for IGMPv3): 10
  - Maximum Multicast Group Members: 25
  - Fast Leave Enable:
- IGMP Group Exception List:** A table with columns 'Group Address', 'Mask/Mask bits', and 'Remove'. It contains three entries:
 

Group Address	Mask/Mask bits	Remove
224.0.0.0	255.255.255.0	<input checked="" type="checkbox"/>
239.255.255.250	255.255.255.255	<input type="checkbox"/>
224.0.255.135	255.255.255.255	<input type="checkbox"/>

 Below the table are input fields for adding new entries and a 'Remove Checked Entries' button.
- MLD Configuration:** A section with the instruction 'Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.' It includes input fields for:
  - Default Version: 2
  - Query Interval: 125
  - Query Response Interval: 10
  - Last Member Query Interval: 10
  - Robustness Value: 2
  - Maximum Multicast Groups: 10
  - Maximum Multicast Data Sources (for mldv2): 10
  - Maximum Multicast Group Members: 10
  - Fast Leave Enable:
- MLD Group Exception List:** A table with columns 'Group Address', 'Mask/Mask bits', and 'Remove'. It contains three entries:
 

Group Address	Mask/Mask bits	Remove
ff01::0000	ffff::0000	<input checked="" type="checkbox"/>
ff02::0000	ffff::0000	<input checked="" type="checkbox"/>
ff05::0001:0003	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	<input type="checkbox"/>

 Below the table are input fields for adding new entries and a 'Remove Checked Entries' button.

At the bottom right of the configuration area is an 'Apply/Save' button.

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

**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**

<b>Item</b>	<b>Description</b>
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.

## 6.11 Wireless

### 6.11.1 SSID

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

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

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

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

BSS-MAC (SSID): D8:B6:B7:59:55:02 (Comtrend5501\_2.4GHz enabled) ▼

BSS Enabled: Enabled ▼

Network Name (SSID): Comtrend5501\_2.4GHz

Network Type: Open ▼

AP Isolation: Off ▼

BSS Max Associations Limit: 64

WMM Advertise: Advertise ▼

WMF: On ▼

Apply Cancel

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 <b>Closed</b> hides the network from active scans. Selecting <b>Open</b> reveals the network from active scans.
AP Isolation	Selecting <b>On</b> enables AP Isolation mode. When enabled, STAs associated with the AP will not be able to communicate with each other.
BSS Max Associations Limit	Sets the maximum associations for this BSS

WMM Advertise	When WMM is enabled for the radio, selecting <b>On</b> allows WMM to be advertised in beacons and probes for this BSS. <b>Off</b> disables advertisement of WMM in beacons and probes.
WMF	Choose <b>On</b> to enable Wireless Multicast Forwarding on this BSS. <b>Off</b> disables this feature.

### 6.11.2 Security

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

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Security**

Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
SSID  
**Security**  
WPS  
MAC Filtering  
WDS  
Advanced  
WifiXtend2.0  
AutoXtend

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

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) Select

802.11 Authentication: Open

802.1X Authentication: Disabled

WPA: Disabled

WPA-PSK: Disabled

WPA2: Disabled

WPA2-PSK: Enabled

WPA3-SAE: Disabled

WPA Encryption: AES

RADIUS Server: 0.0.0.0

RADIUS Port: 1812

RADIUS Key: \*\*\*\*

WPA passphrase: \*\*\*\*\* [Click here to display](#)

Protected Management Frames: Capable

Network Key Rotation Interval: 0

Pairwise Key Rotation Interval: 0

Network Re-auth Interval: 36000

Apply Cancel

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).

802.11 Authentication: Selects 802.11 authentication method. Open or Shared. OSEN:

Open

Disabled

Disabled

The descriptions are also shown below.

Item	Description
Wireless Interface	Select which wireless interface to configure
802.11 Authentication	Select 802.11 authentication method. Open or Shared.
802.1X Authentication	Select Network authentication type
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
WPA Encryption	Select the WPA encryption algorithm
RADIUS Server	Set the IP of the RADIUS 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.

### 6.11.3 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 WiFi simple config mode
Device WPS UUID	Displays the WPS UUID number of this device
Device PIN	Displays the PIN number for this device
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 <a href="#">Click here to display</a>
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
Station PIN	Input the station PIN to verify expected station. Note: Empty for PBC method.
Authorized Station MAC	Input the authorized station MAC
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.

### 6.11.4 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).

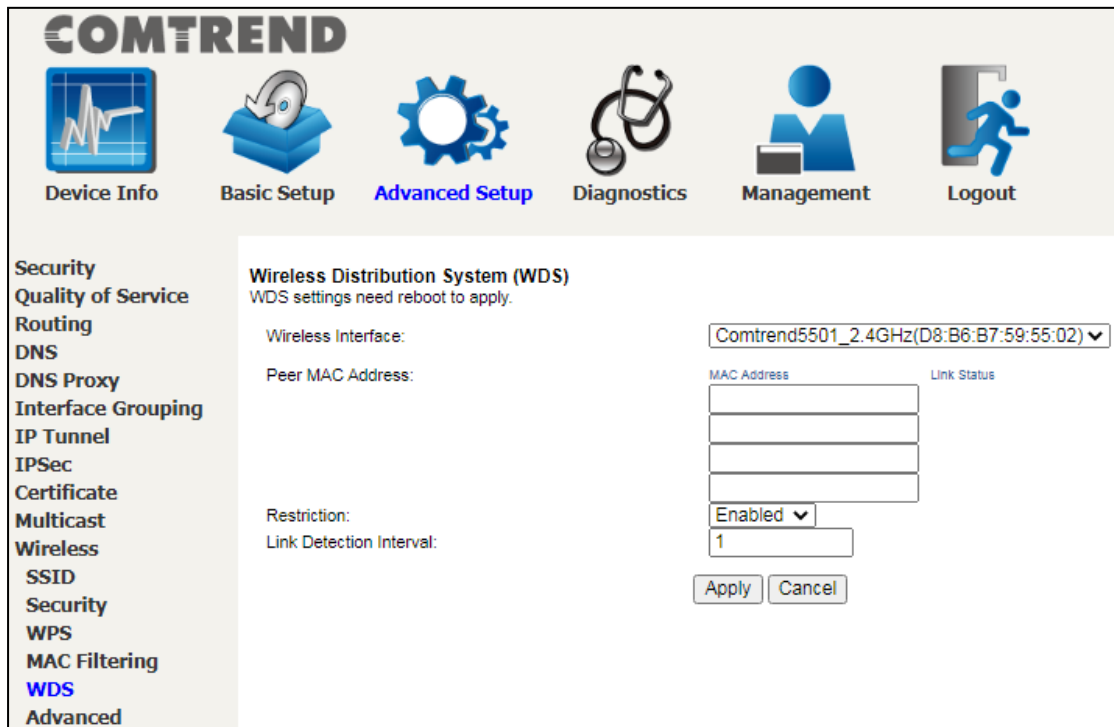
The descriptions are also shown below.

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.



### 6.11.5 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.

<p>Link Direction Interval</p>	<p>Set the WDS link detection interval in seconds. Leave blank or set to zero to disable the detection.</p>
--------------------------------	---

**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 LAN](#), for details on how to change the IP address.

**COMTREND**

Device Info    **Basic Setup**    Advanced Setup    Diagnostics    Management    Logout

**WAN Setup**  
**NAT**  
**LAN**  
 Lan VLAN Setting  
 IPv6 Autoconfig  
 UPnP  
 Parental Control  
 Home Networking  
 Wireless

**Local Area Network (LAN) Setup**

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName **Default** ▾

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode  
 Blocking Mode

Enable IGMP LAN to LAN Multicast: **Disable** ▾  
LAN2LAN multicast setting takes effect only when WAN service is up.  
 LAN2LAN multicast is always enabled when WAN service is down regardless of this setting.

Enable LAN side firewall

Disable DHCP Server  
 Enable DHCP Server

Start IP Address:   
 End IP Address:   
 Leased Time (hour):

Setting TFTP Server

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

- Both devices need to have the same fixed channel. See section [6.11.6 Advanced](#) for details.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

**Security**  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
SSID  
Security  
WPS  
MAC Filtering  
WDS  
**Advanced**  
WifiXtend2.0  
AutoXtend

**Radio**  
This page allows you to configure the Physical Wireless interfaces.

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

Interface: Enabled ▼

802.11 Band: 2.4 GHz ▼ Current: 2.4 GHz

**Channel Specification: 11 ▼ Current: 11\*\*\*Interference Level: Acceptable**

Bandwidth: 40 MHz ▼ Current: 40MHz

VLAN Priority Support: Off ▼

OBSS Coexistence: Off ▼

Transmit Power: 100% ▼

Max Associations Limit: 32

XPress™ Technology: On ▼

Beamforming transmission (BFR): Disabled ▼

Beamforming reception (BFE): Disabled ▼

MU-MIMO TX: Disabled ▼

RIFS Mode Advertisement: Auto ▼

WMM Support: On ▼

No-Acknowledgement: Off ▼

APSD Support: Off ▼

Enable IGMP Proxy: Disable ▼

BandSteering Daemon : Disable ▼

Airtime Fairness: Disable ▼

Enable 802.11ax: On ▼

Apply Cancel

- Both devices need to have a (different) fixed access SSID (Network Name). See section [6.11.1 SSID](#) for details.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

**Security**  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
SSID  
Security

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

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

BSS-MAC (SSID): D8:B6:B7:59:55:02 (Comtrend5501\_2.4GHz enabled) ▼

BSS Enabled: Enabled ▼

**Network Name (SSID): Comtrend5501\_2.4GHz**

Network Type: Open ▼

AP Isolation: Off ▼

BSS Max Associations Limit: 64

WMM Advertise: Advertise ▼

WMF: On ▼

Apply Cancel

Both devices need to have 802.11 Authentication Open and WPA2-PSK/WPA3-SAE disabled. See section 6.11.2 Security for details.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

**Security**  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
SSID  
**Security**  
WPS  
MAC Filtering  
WDS  
Advanced

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

Wireless Interface: Comtrend80D1\_2.4GHz(1C:64:99:32:80:D2) Select

802.11 Authentication: Open

802.1X Authentication: Disabled

WPA: Disabled

WPA-PSK: Disabled

WPA2: Disabled

WPA2-PSK: Enabled

WPA3-SAE: Disabled

WPA Encryption: AES

RADIUS Server: 0.0.0.0

RADIUS Port: 1812

RADIUS Key: \*\*\*\*

WPA passphrase: \*\*\*\*\* [Click here to display](#)

Protected Management Frames: Capable

Network Key Rotation Interval: 0

Pairwise Key Rotation Interval: 0

Network Re-auth Interval: 36000

Apply Cancel

- Both devices (A & B) need to have each other's MAC address. See section 6.11.5 WDS for details.

**COMTREND**

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Security  
Quality of Service  
Routing  
DNS  
DNS Proxy  
Interface Grouping  
IP Tunnel  
IPSec  
Certificate  
Multicast  
Wireless  
SSID  
Security  
WPS  
MAC Filtering  
**WDS**  
Advanced

**Wireless Distribution System (WDS)**  
WDS settings need reboot to apply.

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

Peer MAC Address:  Link Status

Restriction: Enabled ▼

Link Detection Interval: 1

Apply Cancel

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

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics **Management** Logout

Settings  
System Log  
SNMP Agent  
TR-069 Client  
STUN Client  
Internet Time  
Access Control  
Update Software  
**Reboot**

Click the button below to reboot the router.

Reboot

### 6.11.6 Advanced

This page allows you to configure the Physical Wireless interfaces.

#### 2.4GHz

**COMTREND**

Device Info    Basic Setup    **Advanced Setup**    Diagnostics    Management    Logout

**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
**DNS Proxy**  
**Interface Grouping**  
**IP Tunnel**  
**IPSec**  
**Certificate**  
**Multicast**  
**Wireless**  
**SSID**  
**Security**  
**WPS**  
**MAC Filtering**  
**WDS**  
**Advanced**  
**WifiXtend2.0**  
**AutoXtend**

**Radio**  
 This page allows you to configure the Physical Wireless interfaces.

Wireless Interface: Comtrend5501\_2.4GHz(D8:B6:B7:59:55:02) ▼

Interface: Enabled ▼

802.11 Band: 2.4 GHz ▼    Current: 2.4 GHz

Channel Specification: 11 ▼    Current: 11 \*\*\*Interference Level: Acceptable

Bandwidth: 40 MHz ▼    Current: 40MHz

VLAN Priority Support: Off ▼

OBSS Coexistence: Off ▼

Transmit Power: 100% ▼

Max Associations Limit: 32

XPress™ Technology: On ▼

Beamforming transmission (BFR): Disabled ▼

Beamforming reception (BFE): Disabled ▼

MU-MIMO TX: Disabled ▼

RIFS Mode Advertisement: Auto ▼

WMM Support: On ▼

No-Acknowledgement: Off ▼

APSD Support: Off ▼

Enable IGMP Proxy: Disable ▼

BandSteering Daemon: Disable ▼

Airtime Fairness: Disable ▼

Enable 802.11ax: On ▼

Apply    Cancel

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
Bandwidth	Select channel bandwidth
VLAN Priority Support	Advertise packet priority using VLAN tag

OBSS Coexistence	Enable/Disable overlapping BSS coexistence aka 20/40 coex.
Transmit Power	Select the transmit power percentage
Max Associations Limit	Set the number of associations the driver should accept
Xpress Technology	Enable/Disable Xpress mode
Beamforming transmission (BFR)	Enable/Disable beamforming transmission
Beamforming reception (BFE)	Enable/Disable beamforming reception
MU-MIMO TX	Enable/Disable MU-MIMO transmission
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
Enable IGMP Proxy	Enable/Disable IGMP Proxy
BandSteering Daemon	Select standalone for dual band traffic control (i.e will switch between 2.4 & 5GHz connections automatically)  Select Disable to close this feature
Airtime Fairness	Enable/Disable airtime fairness between multiple links
Enable 802.11ax	Disable (Off) to make those not-support-802.11ax NIC/STA see this AP

**5GHz**

**COMTREND**

Device Info    Basic Setup    **Advanced Setup**    Diagnostics    Management    Logout

**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
**DNS Proxy**  
**Interface Grouping**  
**IP Tunnel**  
**IPSec**  
**Certificate**  
**Multicast**  
**Wireless**  
**SSID**  
**Security**  
**WPS**  
**MAC Filtering**  
**WDS**  
**Advanced**  
**WifiXtend2.0**  
**AutoXtend**

**Radio**  
 This page allows you to configure the Physical Wireless interfaces.

Wireless Interface: Comtrend5501\_5GHz(D8:B6:B7:59:55:03) ▼

Interface: Enabled ▼

802.11 Band: 5 GHz ▼    Current: 5 GHz

Channel Specification: 36/80 ▼    Current: 36/80 \*\*\*Interference Level: Acceptable

Bandwidth: 80 MHz ▼    Current: 80MHz

VLAN Priority Support: Off ▼

OBSS Coexistence: Off ▼

Transmit Power: 100% ▼

DFS Channel Selection: Disable ▼

Max Associations Limit: 32

XPress™ Technology: On ▼

Beamforming transmission (BFR): Disabled ▼

Beamforming reception (BFE): Disabled ▼

MU-MIMO TX: Disabled ▼

RIFS Mode Advertisement: Auto ▼

WMM Support: On ▼

No-Acknowledgement: Off ▼

APSD Support: Off ▼

Enable IGMP Proxy: Disable ▼

BandSteering Daemon : Disable ▼

Airtime Fairness: Disable ▼

Enable 802.11ax: On ▼

Apply    Cancel

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).

Interface: Enabled ▼

802.11 Band: 5 GHz ▼    Current: 5 GHz

802.11ax: Auto ▼    Current: 56/80 \*\*\*Interference Level: Acceptable

Selects 802.11 Band to use.

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
Bandwidth	Select channel bandwidth
VLAN Priority Support	Advertise packet priority using VLAN tag
OBSS Coexistence	Enable/Disable overlapping BSS coexistence aka 20/40 coex.
Transmit Power	Select the transmit power percentage
DFS Channel Selection	<p>DFS (Dynamic Frequency Selection) is a channel selection scheme specifically for 5GHz Wi-Fi to prevent collision with other usages, such as military/satellite communications and weather radar</p> <p>The DFS Reentry feature if selected, will try re-entering to a DFS channel to avoid service interruption for the user</p>
Max Associations Limit	Set the number of associations the driver should accept
Xpress Technology	Enable/Disable Xpress mode
Beamforming transmission (BFR)	Enable/Disable beamforming transmission
Beamforming reception (BFE)	Enable/Disable beamforming reception
MU-MIMO TX	Enable/Disable MU-MIMO transmission
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
Enable IGMP Proxy	Enable/Disable IGMP Proxy
BandSteering Daemon	Select standalone for dual band traffic control (i.e will switch between 2.4 & 5GHz connections automatically)  Select Disable to close this feature
Airtime Fairness	Enable/Disable airtime fairness between multiple links
Enable 802.11ax	Disable (Off) to make those not-support-802.11ax NIC/STA see this AP

## 6.12 WifiXtend 2.0

**WifiXtend** is a function to construct and optimize a mesh-network. Check the checkbox and click the **Apply/Save** button to enable **WifiXtend**.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPSec, Certificate, Multicast, Wireless, SSID, Security, WPS, MAC Filtering, WDS, Advanced, **WifiXtend2.0**, and AutoXtend. The main content area displays the **WiFiXTEND™ 2.0** logo and the text "WiFiXtend2.0: End-User WiFi Optimization via Mesh-Enhanced Technology". Below this, there is a checkbox labeled "Enable WiFi Mesh" which is checked. To the right of the checkbox is an "Apply/Save" button. Below a horizontal line, the **WifiXtend™** logo is displayed, followed by the text "WiFiXtend1.0: Historical reference only. This now exists under AutoXtend as SSID Sync."

To enable the end-user WiFi optimization via mesh-enhanced technology, check the checkbox and click the **Apply/Save** button.

## 6.13 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.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. Below this is a sidebar menu with categories like Security, Quality of Service, Routing, DNS, DNS Proxy, Interface Grouping, IP Tunnel, IPSec, Certificate, Multicast, Wireless, SSID, Security, WPS, MAC Filtering, WDS, Advanced, WifiXtend2.0, and **AutoXtend**.

The main content area is titled "AutoXtend" and contains the following text and options:

AutoXtend  
Custom code features that increase ease of installation.

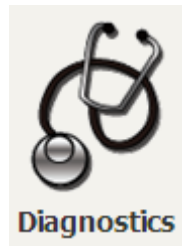
- Enable AutoXtend Features
  - Admin Sync: Syncs the administrator login username and password.
  - G.hn Sync: Syncs G.hn domain and password.
  - TR69 Sync: Syncs the TR-069/STUN settings.
  - SSID Sync: The SSID/Password settings are propagated.
  - WiFi Mesh Sync: WiFi Mesh settings are propagated.
  - CSRXtend Sync: CSR settings are propagated.

An "Apply/Save" button is located at the bottom right of the configuration area.

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.

The screenshot shows the COMTREND interface with the Diagnostics menu item highlighted. The dashboard displays LAN status for four ports (eth1, eth2, eth3, eth4) and a table of device information.

LAN	
Down eth1	Down eth2
100 FD eth3	Down eth4
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:59:55:01
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254

Device	
Model	PRT-6302
Serial Number	2095955UXKF-AA000000
Firmware Version	GT11-502CTU-C02_R02
Bootloader (CFE) Version	1.0.38-163.243-0
Up Time	8 mins:52 secs
System Log	<input type="button" value="Show"/>

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

The screenshot shows the COMTREND interface with the Diagnostics menu item selected. The screen displays a table of connection test results and a 'Rerun Diagnostic Tests' button.

**Diagnostics**

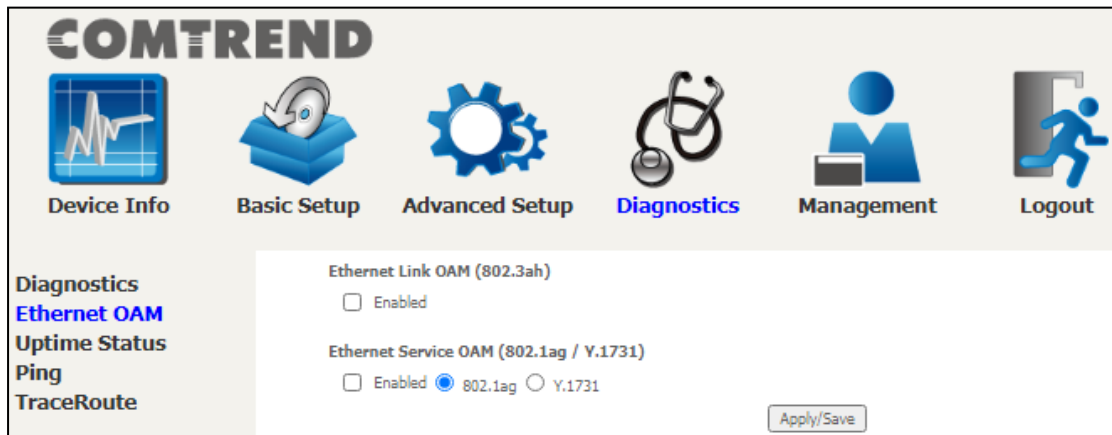
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your eth1 Connection:	<b>FAIL</b>	<a href="#">Help</a>
Test your eth2 Connection:	<b>PASS</b>	<a href="#">Help</a>
Test your eth3 Connection:	<b>FAIL</b>	<a href="#">Help</a>
Test your eth4 Connection:	<b>FAIL</b>	<a href="#">Help</a>
Test your Wireless Connection:	<b>PASS,PASS</b>	<a href="#">Help</a>

## 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.

**Ethernet Link OAM (802.3ah)**

Enabled

WAN Interface:

OAM ID:  (positive integer)

Auto Event

Variable Retrieval

Link Events

Remote Loopback

Active Mode

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.

**Ethernet Service OAM (802.1ag / Y.1731)**

Enabled  802.1ag  Y.1731

WAN Interface:

MD Level:  [0-7]

MD Name:  [e.g. Broadcom]

MA ID:  [e.g. BRCM]

Local MEP ID:  [1-8191]

Local MEP VLAN ID:  [1-4094] (-1 means no VLAN tag)

CCM Transmission

Remote MEP ID:  [1-8191] (-1 means no Remote MEP)

**Loopback and Linktrace Test**

Target MAC:  [e.g. 02:10:18:aa:bb:cc]

Linktrace TTL:  [1-255] (-1 means no max hop limit)

Loopback Result:	N/A			
Linktrace Result:	N/A			

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.

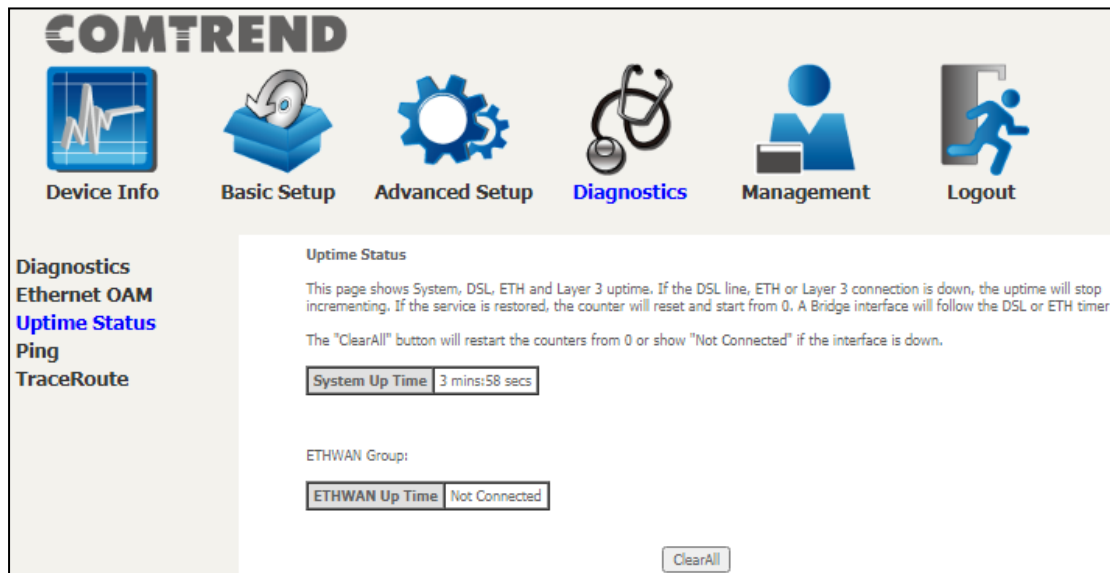
Remote MEP ID	Maintenance association End Point Identifier for the remote receiver
---------------	--

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.

**COMTREND**

Device Info    Basic Setup    Advanced Setup    **Diagnostics**    Management    Logout

**Diagnostics**  
 Ethernet OAM  
 Uptime Status  
**Ping**  
 TraceRoute

**Ping**

Send ICMP ECHO\_REQUEST packets to network hosts. Please make sure ICMP is set to be accessible from WAN in Access Control configuration.

Ping IP Address / Hostname:

```

PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.277 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.168 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.138 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.238 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.205/0.277 ms
  
```

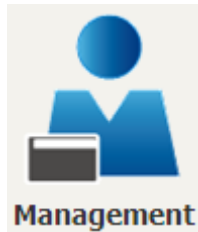
## 7.5 Trace Route

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.

The screenshot displays the COMTREND web interface. At the top, the COMTREND logo is visible. Below it, a navigation menu contains six icons with corresponding labels: Device Info (line graph), Basic Setup (CD/DVD), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). The Diagnostics menu item is highlighted in blue. On the left side, a sidebar lists several diagnostic tools: Diagnostics, Ethernet OAM, Uptime Status, Ping, and TraceRoute (which is highlighted in blue). The main content area is titled 'TraceRoute' and contains the following text: 'Trace the route ip packets follow going to "host". Please make sure ICMP is set to be accessible from WAN in Access Control configuration.' Below this is a form with the label 'TraceRoute IP Address / Hostname:' followed by an empty text input field and a 'TraceRoute' button. At the bottom of the main area, the results of a test are shown: 'traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets' and '1 Comtrend.Home (192.168.1.1) 0.040 ms'.

## Chapter 8 Management

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



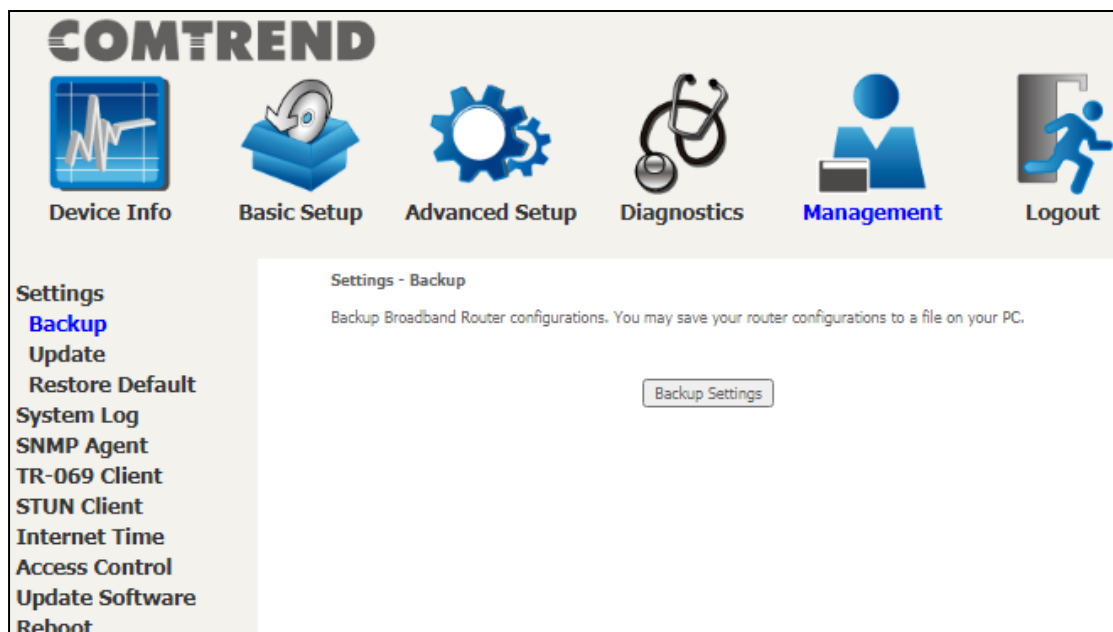
The Management menu has the following maintenance functions and processes:

### 8.1 Settings

This includes [Backup Settings](#), [Update Settings](#), and [Restore Default](#) screens.

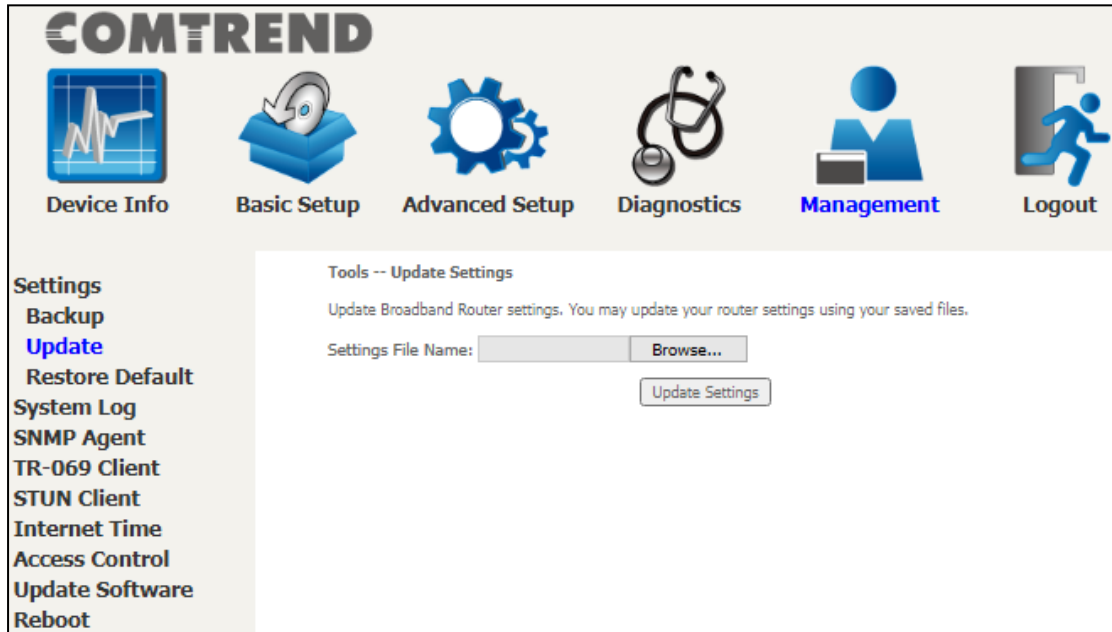
#### 8.1.1 Backup Settings

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.



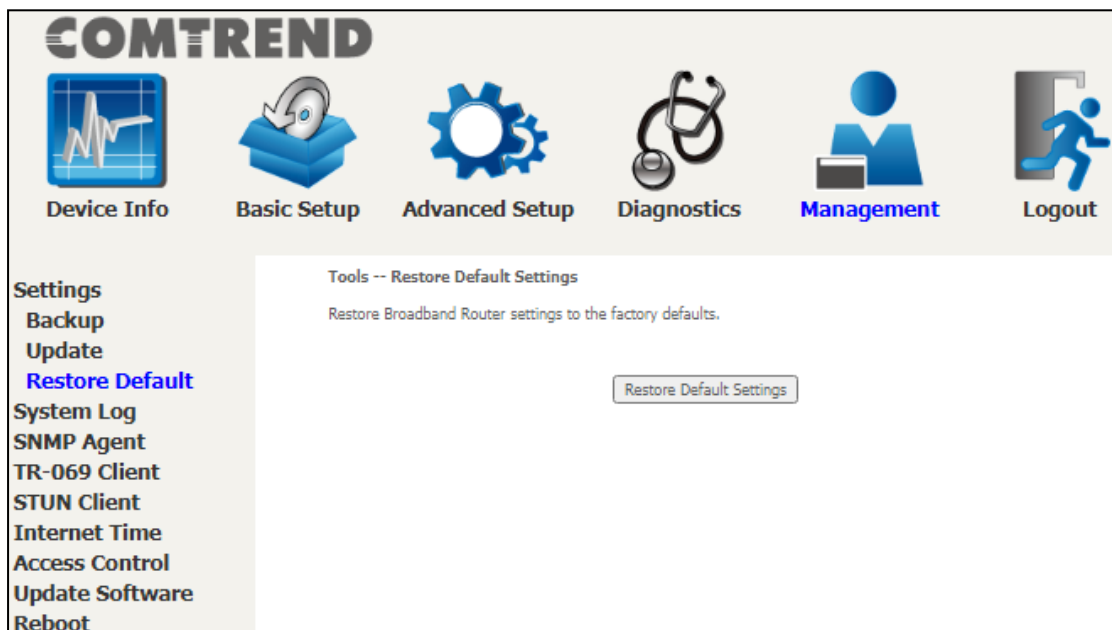
### 8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Press **Browse...** to search for the file, or enter the file name (including folder path) in the **File Name** box, and 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.

**Broadband Router Restore**

The Broadband Router configuration has been restored to default settings and the router is rebooting.

Close the Broadband Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

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.

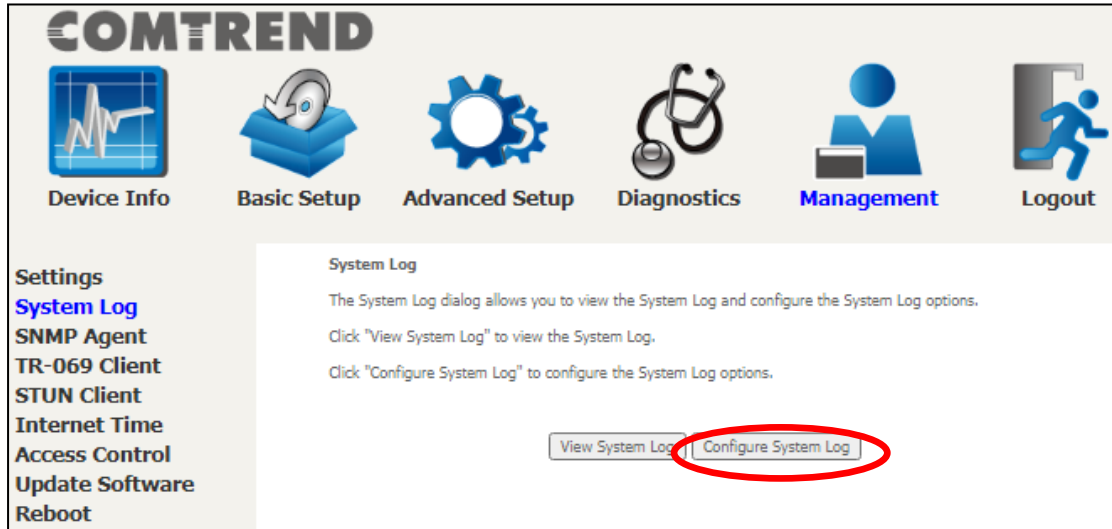
**NOTE:** This entry has the same effect as the **Reset** button. The PRT-6302 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously 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

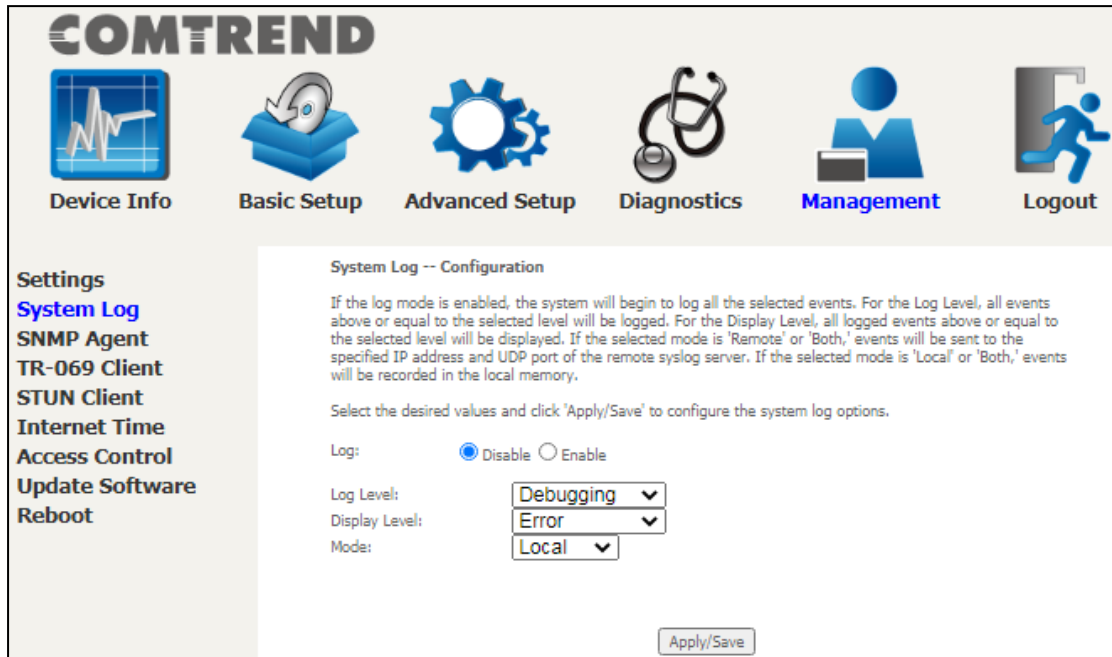
This function allows a system log to be kept and viewed upon request.

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 <b>Enable</b> radio button and then click <b>Apply/Save</b> .

<p>Log Level</p>	<p>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 PRT-6302 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.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> <li>• Emergency = system is unusable</li> <li>• Alert = action must be taken immediately</li> <li>• Critical = critical conditions</li> <li>• Error = Error conditions</li> <li>• Warning = normal but significant condition</li> <li>• Notice= normal but insignificant condition</li> <li>• Informational= provides information for reference</li> <li>• Debugging = debug-level messages</li> </ul> <p>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.</p>
<p>Display Level</p>	<p>Allows the user to select the logged events and displays on the <b>View System Log</b> window for events of this level and above to the highest Emergency level.</p>
<p>Mode</p>	<p>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.</p>

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

System Log			
Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.

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.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Settings**  
 System Log  
 SNMP Agent  
**TR-069 Client**  
 STUN Client  
 Internet Time  
 Access Control  
 Update Software  
 Reboot

**TR-069 client - Configuration**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Enable TR-069

OUI-serial  MAC  Serialnumber  
 Inform  Disable  Enable  
 DHCP Option 43  Disable  Enable

Inform Interval:   
 ACS URL:   
 ACS User Name:   
 ACS Password:   
 WAN Interface used by TR-069 client:

Connection Request Authentication

Connection Request User Name:   
 Connection Request Password:   
 Connection Request URL:

The table below is provided for ease of reference.

Item	Description
Enable TR-069	Tick the checkbox <input checked="" type="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.
<b>Connection Request</b>	
Authentication	Tick the checkbox <input checked="" type="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.

**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Settings**  
 System Log  
 SNMP Agent  
 TR-069 Client  
**STUN Client**  
 Internet Time  
 Access Control  
 Update Software  
 Reboot

**STUN client - Configuration**

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 "Apply/Save" to configure the STUN client options.

Disable  Enable

STUN Server Address:

STUN Server Port:

STUN User Name:

STUN Password:

Max KeepAlive Period:

Min KeepAlive Period:

Apply/Save

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**.

**COMTREND**

Device Info    Basic Setup    Advanced Setup    Diagnostics    Management    Logout

Settings  
System Log  
SNMP Agent  
TR-069 Client  
STUN Client  
**Internet Time**  
Access Control  
Update Software  
Reboot

**Time settings**  
This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:    
 Second NTP time server:    
 Third NTP time server:    
 Fourth NTP time server:    
 Fifth NTP time server:

Time zone offset:

**NOTE:** Internet Time must be activated to use. See [5.4 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 PRT-6302 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.

**COMTREND**

Device Info    Basic Setup    Advanced Setup    Diagnostics    **Management**    Logout

**Settings**  
 System Log  
 SNMP Agent  
 TR-069 Client  
 STUN Client  
 Internet Time  
**Access Control**  
 Accounts  
 Services  
 IP Address  
 Update Software  
 Reboot

**Access Control -- Accounts/Passwords**  
 By default, access to your Broadband router is controlled through three user accounts: root,support,and user.  
 The root account has unrestricted access to view and change the configuration of your Broadband router.  
 The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.  
 The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.  
 Use the fields below to update passwords for the accounts, add/remove accounts (max of 5 accounts). Note: Passwords may be as long as 16 characters but must not contain a space.

Select an account:   
 Create an account:

Old Password:   
 New Password:   
 Confirm Password:

---

Use the fields below to enable/disable accounts as well as adjust their specific privileges.

Feature	root
Account access	Both
Add/Remove WAN	Enabled
Wireless - Basic	Enabled
Wireless - Advanced	Enabled
LAN Settings	Enabled
Interface Grouping	Enabled
NAT Settings	Enabled
Update Software	Enabled
Security	Enabled
Quality of Service	Enabled
Management Settings	Enabled
Advanced Setup	Enabled

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.

**COMTREND**

Device Info    Basic Setup    Advanced Setup    Diagnostics    Management    Logout

Settings  
System Log  
SNMP Agent  
TR-069 Client  
STUN Client  
Internet Time  
Access Control  
Accounts  
**Services**  
IP Address  
Update Software  
Reboot

**Service Access Control Configuration**  
Select each listbox and click save/apply to configure your Setting.

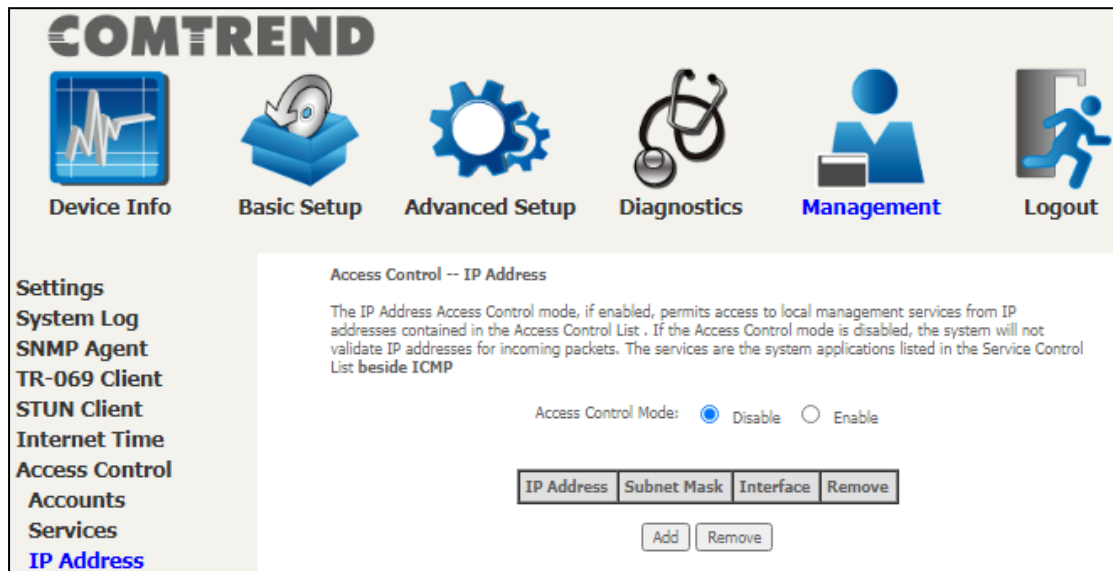
Service	Current	New	Port
HTTP	Lan	LAN	80
SSH	Lan	LAN	22
TELNET	Lan	LAN	23
SNMP	Disable	Disable	161
HTTPS	Lan	LAN	443
FTP	Lan	LAN	21
ICMP	Lan	LAN	0

Apply/Save

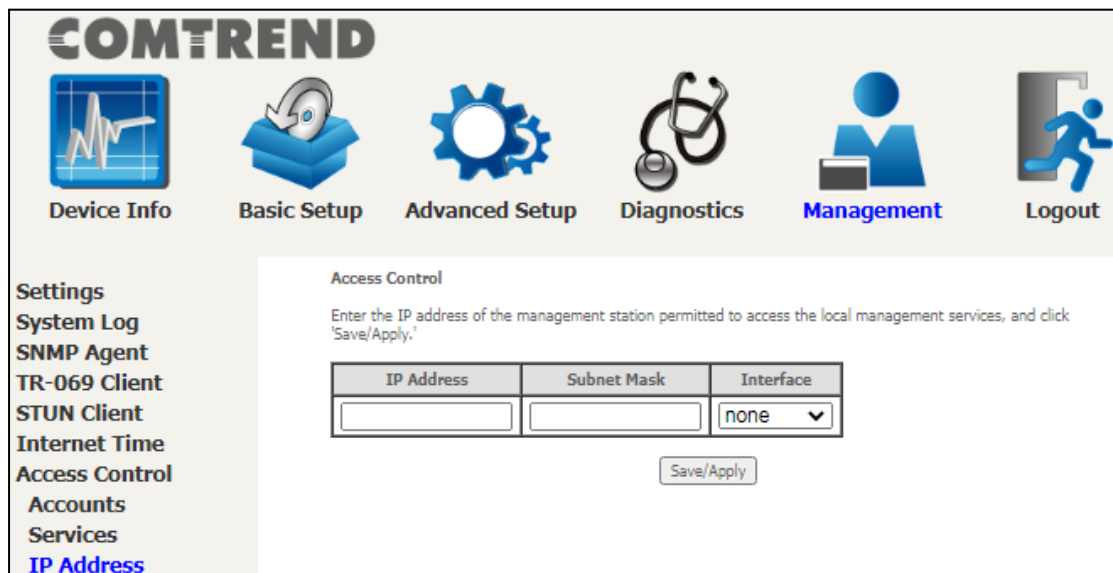
Please note that any Comtrend firmware upgrade will not modify any WiFi parameters (including the WiFi power setting). Comtrend’s products follow the market’s standard requirements.

### 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.

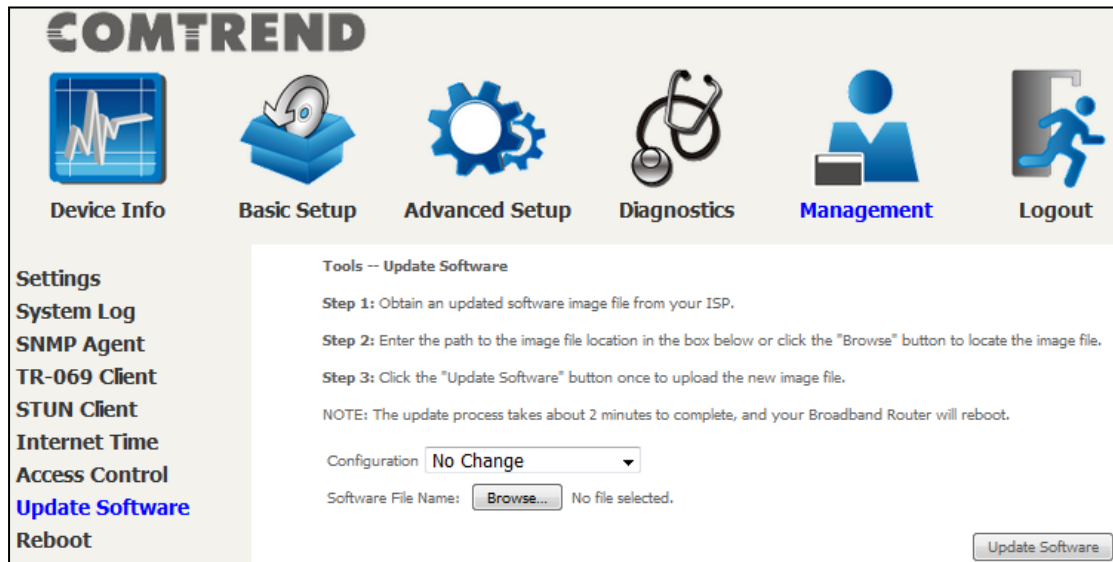
**Subnet Mask** – Subnet address for the management station.

**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 WiFi power setting). Comtrend's products follow the market's standard requirements.



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

**STEP 2:** Select the configuration from the drop-down menu.

### 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.

**STEP 3:** Enter the path and filename of the firmware image file in the **Software File Name** field or click the **Browse** button to locate the image file.

**STEP 4:** Click the **Update Software** button once to upload and install the file.

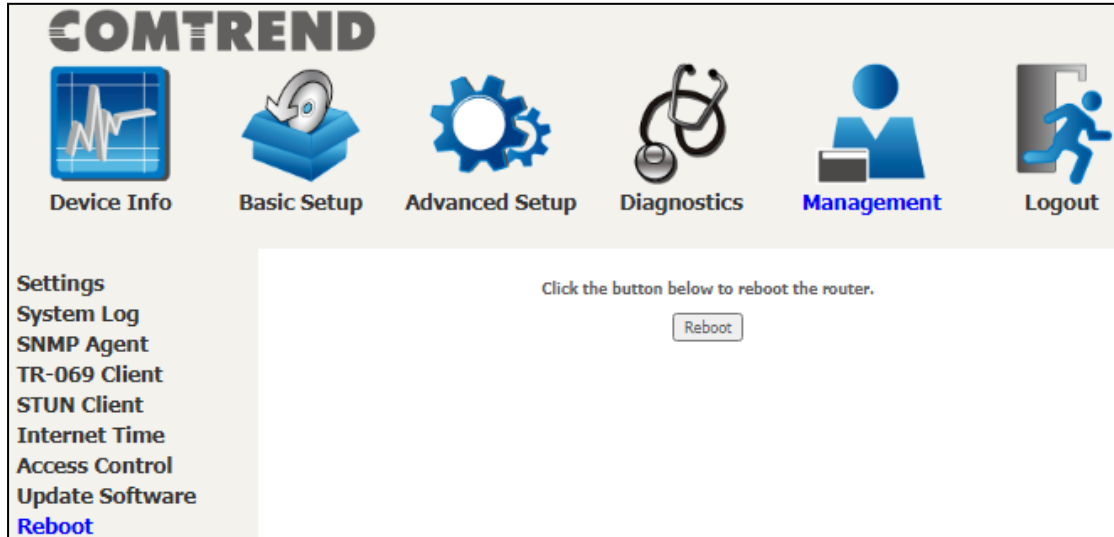
**NOTE1:** The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Information](#) screen with the firmware version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

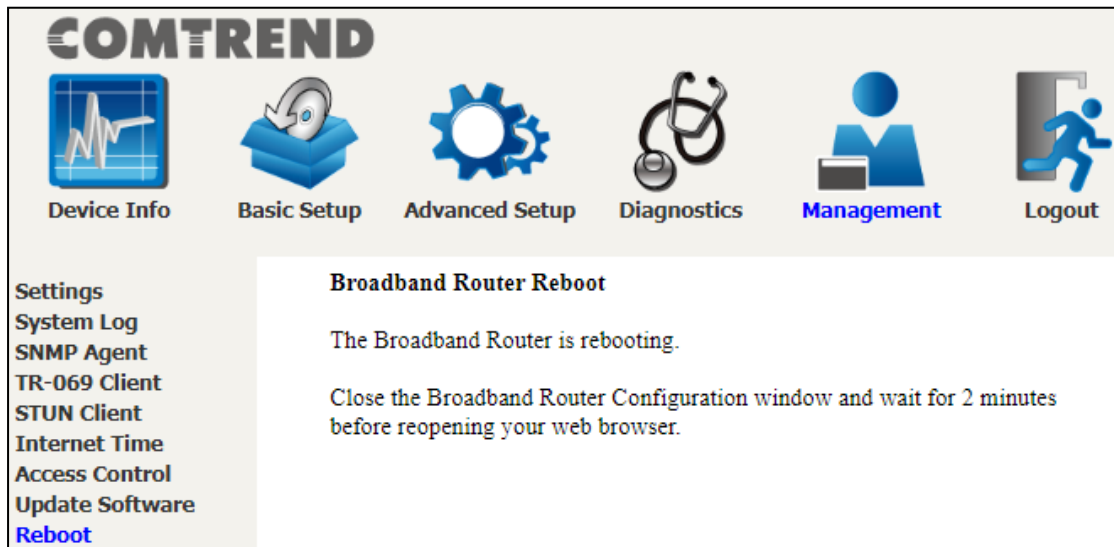


## 8.9 Reboot

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

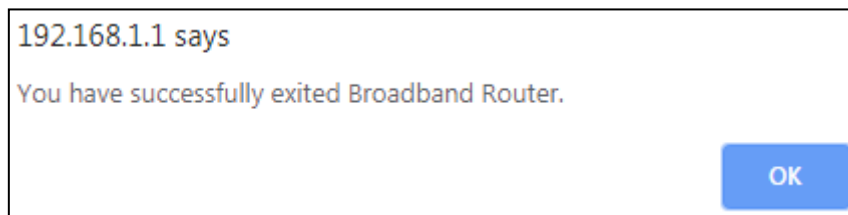
To log out from the device simply click the following icon located at the top of your screen.



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 PRT-6302, 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-45 X 4 for GELAN
- RJ-45 X 1 for 2.5GEWAN
- 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

### 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

### NAT/PAT

- Port Triggering
- Port Forwarding (Virtual Server)
- Symmetric port-overloading NAT, Full-Cone NAT
- DMZ host
- VPN Pass Through (PPTP, L2TP, IPSec)

### 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

### Firewall/Filtering

- Stateful Packet Inspection Firewall
- Stateless Packet Filter
- URI/URL Filtering
- TCP/IP/Port/Interface Filtering Rules Support Both Incoming and Outgoing Filtering

**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)

**Wireless**

- IEEE 802.11ax, 2.4GHz, 4T4R  
Backward compatible with 802.11n/g/b  
2412~2472 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/ 3.0A

**Environment**

- Operating Temperature: 0°C ~40°C (32°F ~104°F)
- Operating Humidity: 10%~90% non-condensing
- Storage Temperature: -25°C ~65°C (-23°F ~149°F)
- Storage Humidity: 5%~90% non-condensing

**Kit Weight**

(1\* PRT-6302, 1\*RJ45 cable, 1\*power adapter) = 0.8 kg

<b>NOTE:</b> 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.

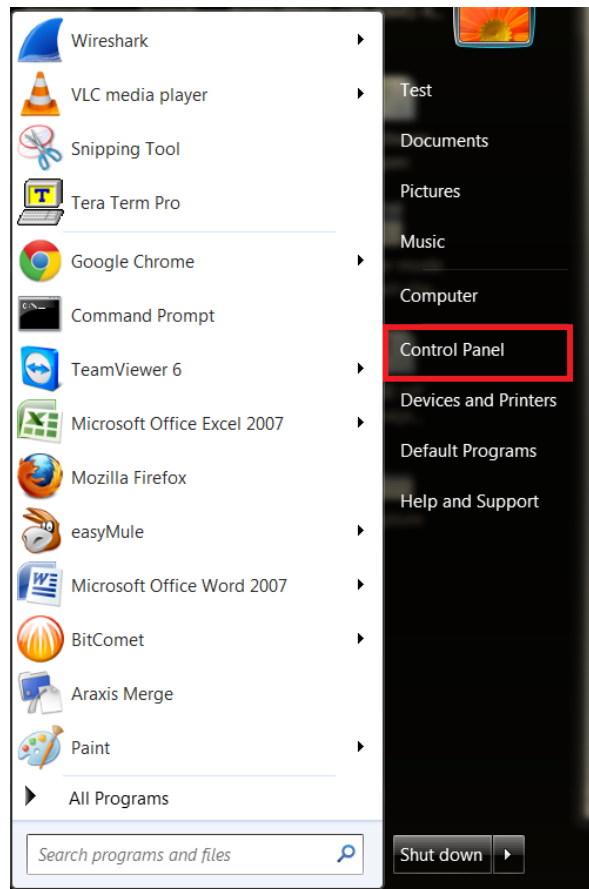
**NOTE:** This function only applies to models with a USB host port.

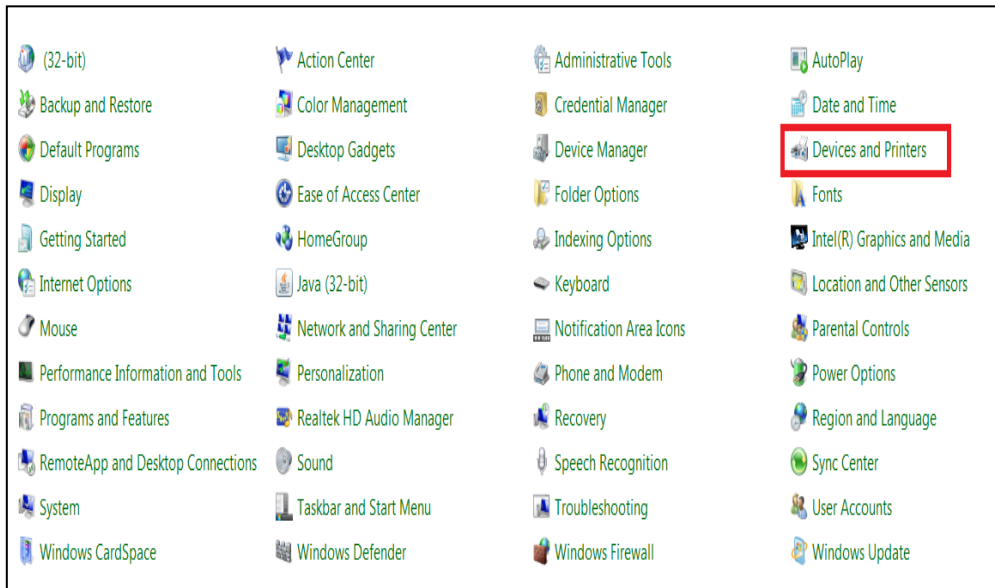
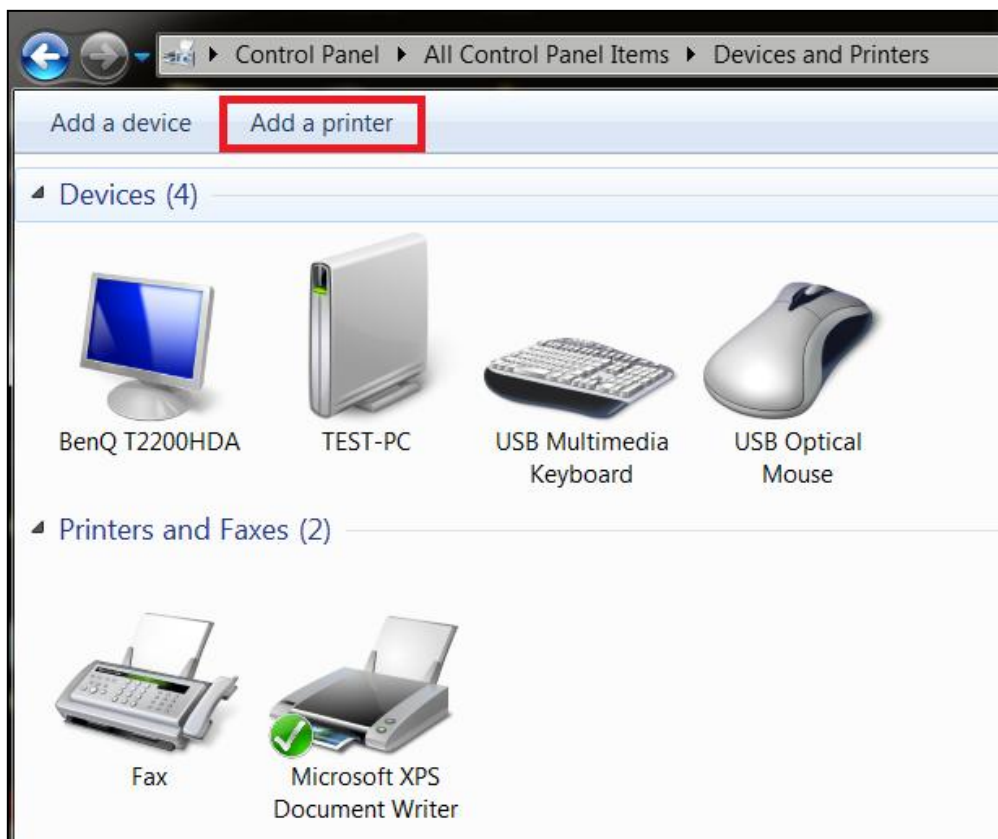
**STEP 1:** Enable Print Server from Web User Interface. Select the Enable on-board print server checkbox  and input Printer name & Make and model. Click the **Apply/Save** button.

**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.

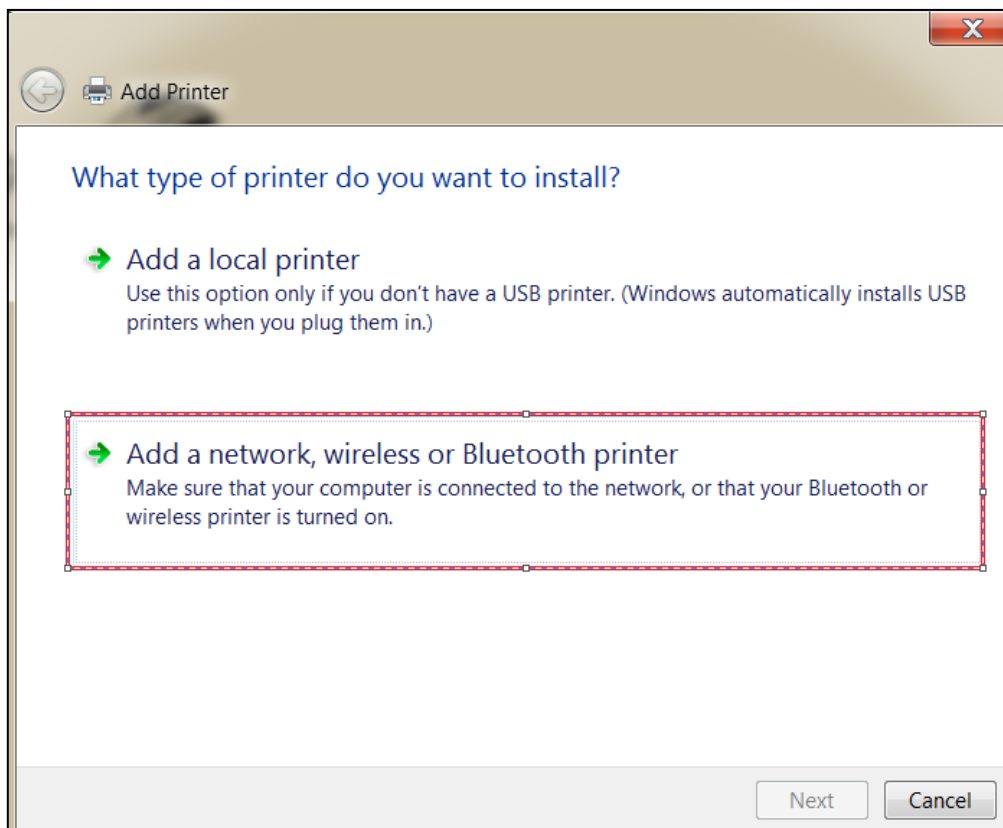
The screenshot shows the COMTREND web interface. At the top, there are navigation icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options: WAN Setup, NAT, LAN, Parental Control, Home Networking, Print Server (highlighted), DLNA, and Storage Service. The main content area is titled 'Print Server settings' and contains the following text: 'This page allows you to enable / disable printer support.' Below this, there is a checked checkbox for 'Enable on-board print server.' There are two input fields: 'Printer name' with the value 'hpdeskjet' and 'Make and model' with the value '321123'. Both input fields are highlighted with a red border. At the bottom right of the form, there is an 'Apply/Save' button.

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

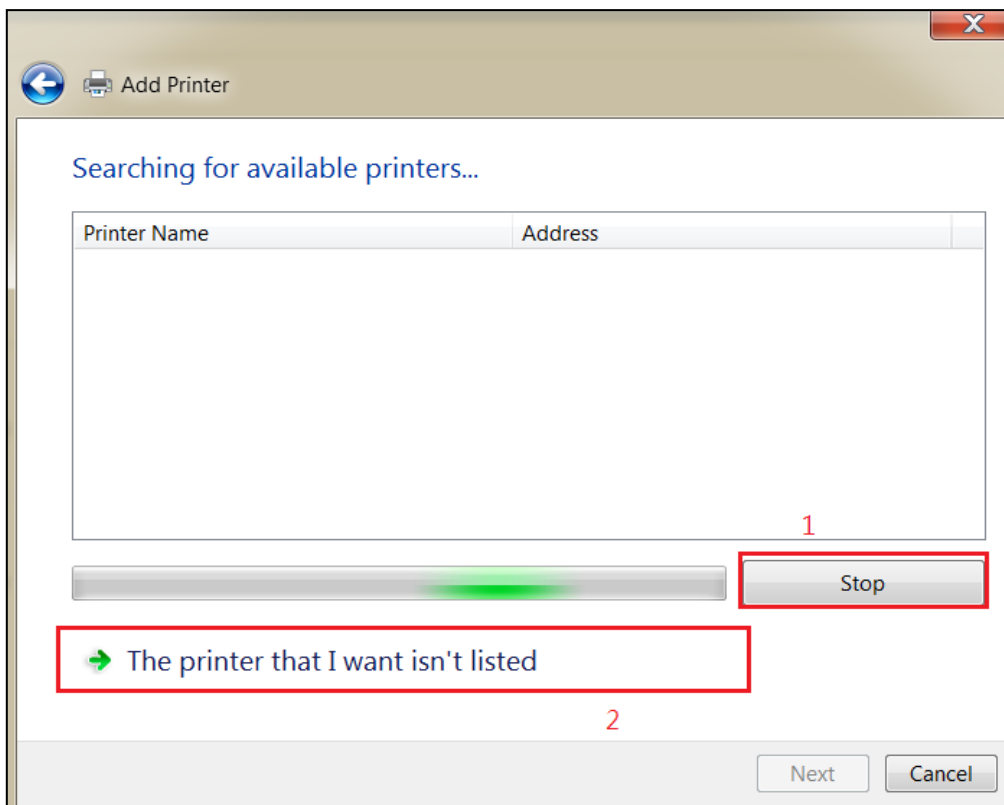


**STEP 3: Select Devices and Printers.****STEP 4: Select Add a printer.**

**STEP 5:** Select **Add a network, wireless or Bluetooth printer.**



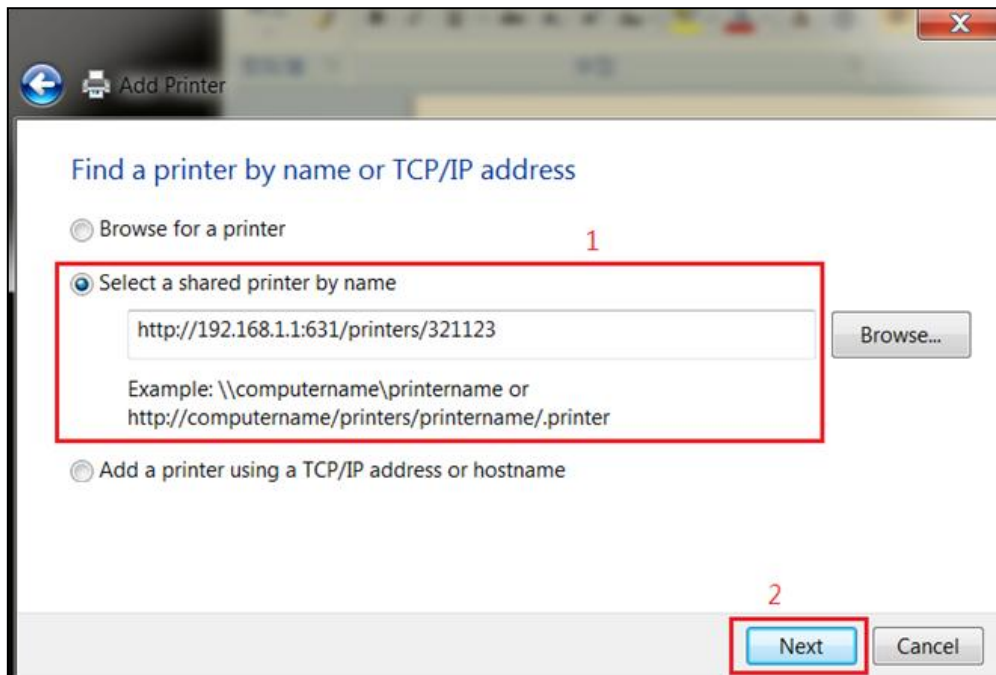
**STEP 6:** Click the **Stop** button. → Select **The printer that I want isn't listed.**



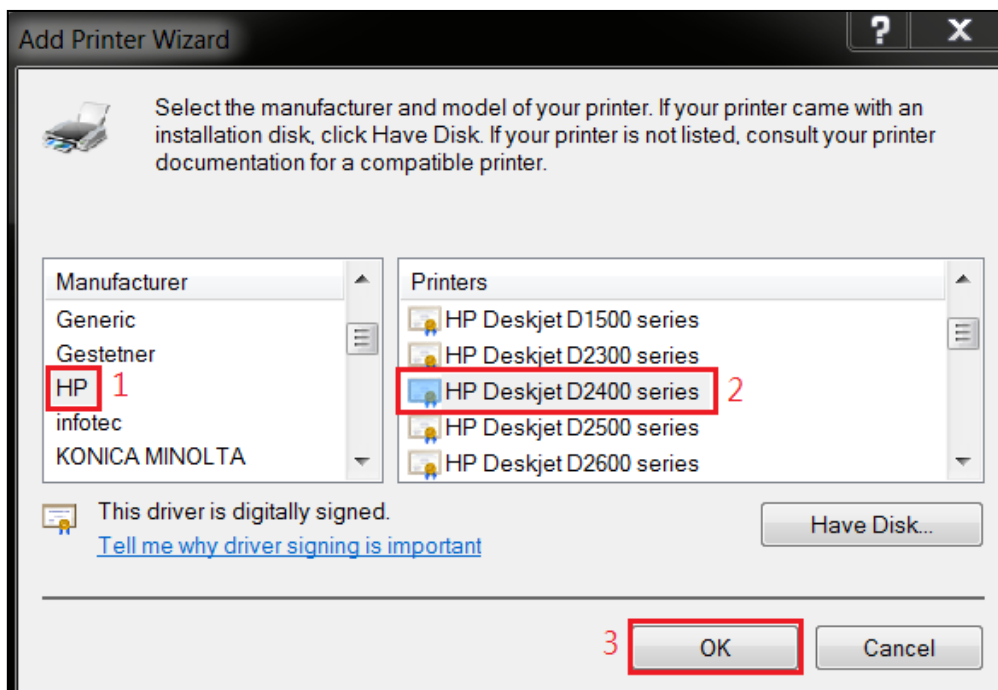
**STEP 7:** Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

<http://LAN IP:631/printers/>the name of the printer

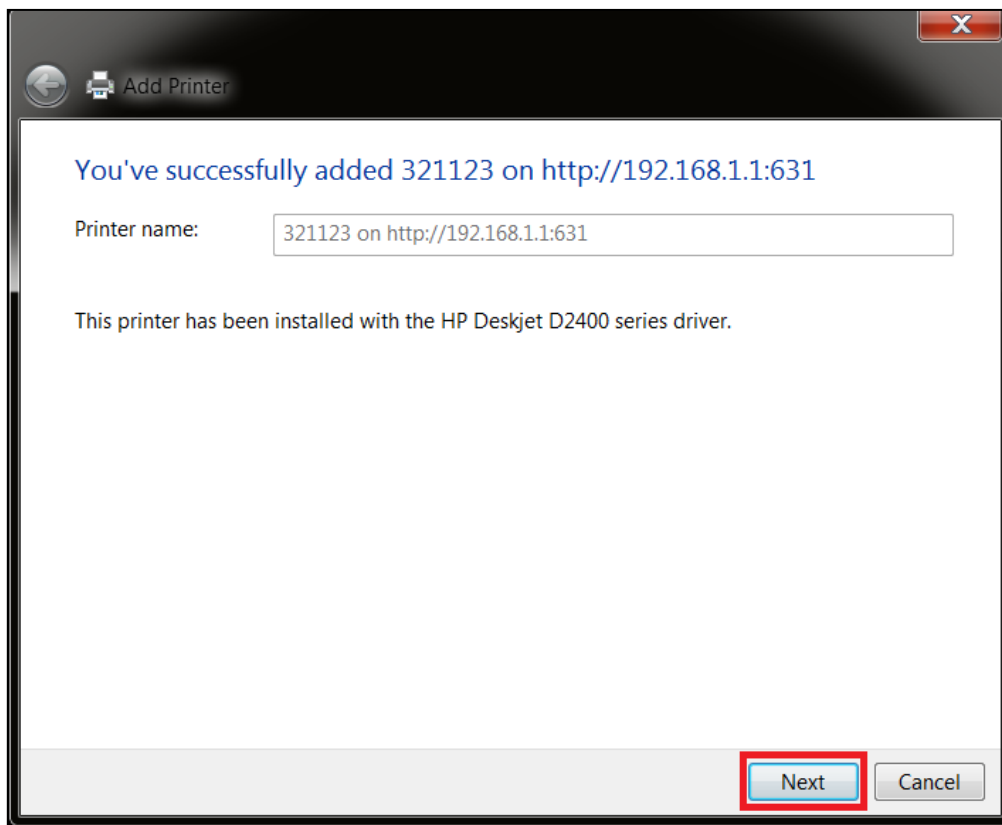
**NOTE:** The printer name must be the same name inputted in the WEB UI “printer server settings” as in step 1.



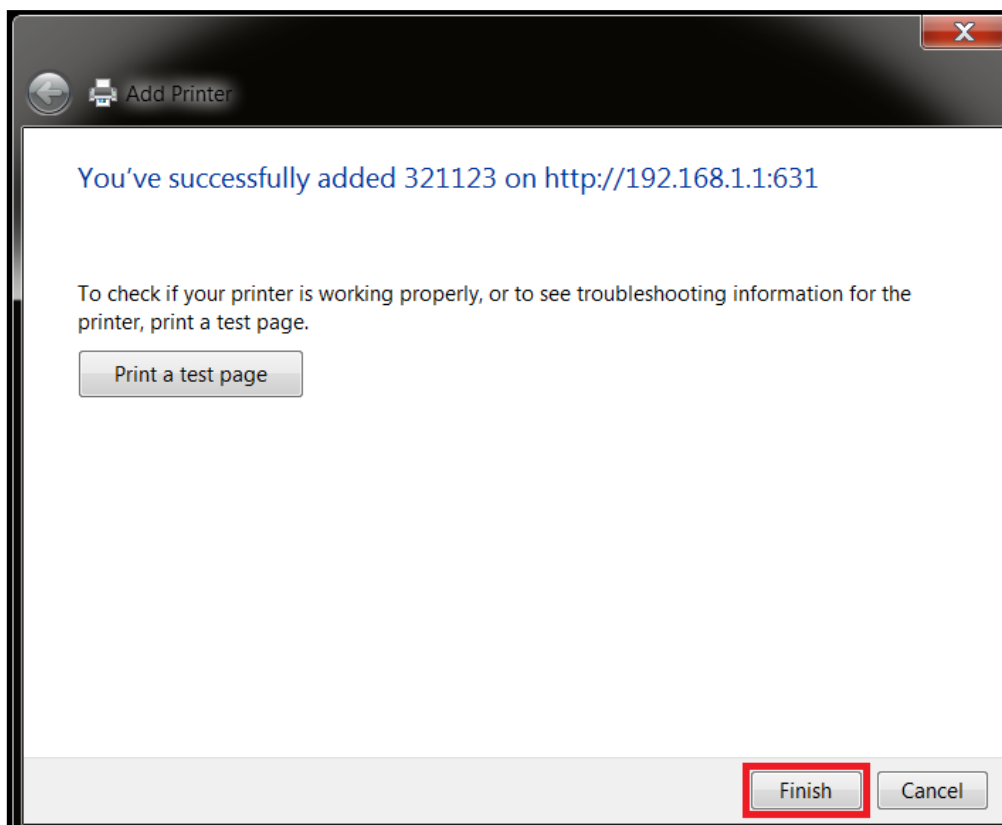
**STEP 8:** Select the **manufacturer** → and **model** of your printer → then, click **OK**.



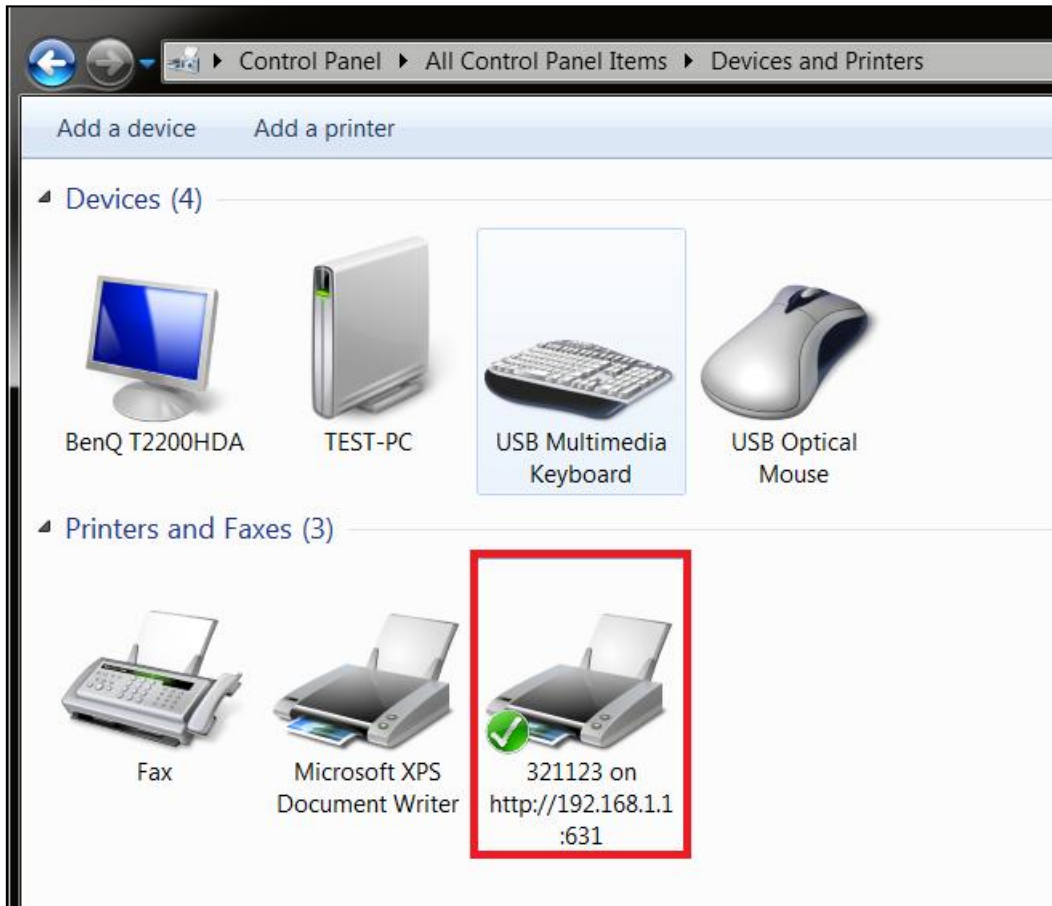
**STEP 9:** The printer has been successfully installed. Click the **Next** button.



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



**STEP 11:** Go to → **Control Panel** → **All Control Panel Items** → **Devices and Printers** 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.

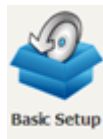
The following sections describe each stage in turn.

### 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 Ethernet WAN Interface

The PRT-6302 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 1: Layer 2 Interface**

Select new interface to add: ETHERNET Interface Add

ETH WAN Interface Configuration

Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	<span>Remove</span>

**Step 2: Wide Area Network (WAN) Service Setup**

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Manual Mode	Remove	Edit
eth0.1	ipoe_eth0	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<span>Edit</span>

Add Remove

**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.

**ETH WAN Configuration**  
This screen allows you to configure a ETH port .

Select a ETH port:

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

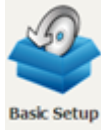
Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	<input type="button" value="Remove"/>

To add a WAN connection go to [Section F2 ~ WAN Connections](#).

## F2 ~ WAN Connections

The PRT-6302 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: Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Manual Mode	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Remove"/>															

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

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

eth0/eth0 ▼

**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.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

**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.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

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

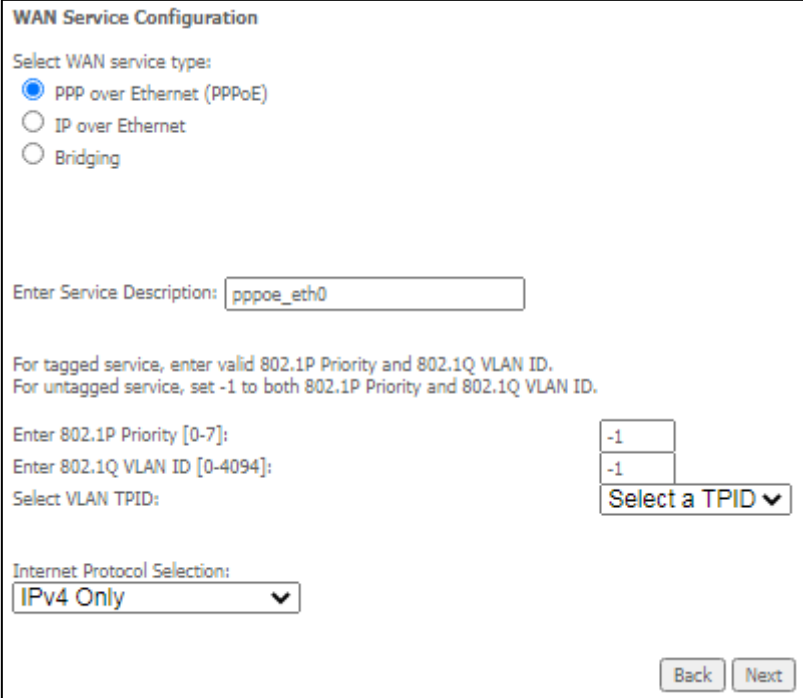
**STEP 5:** You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

- (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 (Not Supported)
- (5) For IP over ATM (IPoA) – IPv4 (Not Supported)
- (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 (Not Supported)
- (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**.



The screenshot shows the 'WAN Service Configuration' interface. It includes the following elements:

- WAN Service Configuration** (Section Header)
- Select WAN service type:** Three radio buttons:  PPP over Ethernet (PPPoE),  IP over Ethernet, and  Bridging.
- Enter Service Description:** A text input field containing 'pppoe\_eth0'.
- For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.** (Instructional text)
- Enter 802.1P Priority [0-7]:** A text input field containing '-1'.
- Enter 802.1Q VLAN ID [0-4094]:** A text input field containing '-1'.
- Select VLAN TPID:** A dropdown menu with the text 'Select a TPID' and a downward arrow.
- Internet Protocol Selection:** A dropdown menu with 'IPv4 Only' selected and a downward arrow.
- Back** and **Next** buttons at the bottom right.

**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 Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO ▼

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second) 30

Number of retries: 3

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU: 1492

Enable PPP Manual Mode

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**IGMP Multicast**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

**WAN interface with base MAC.**  
Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

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 PRT-6302 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 PRT-6302 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

**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.

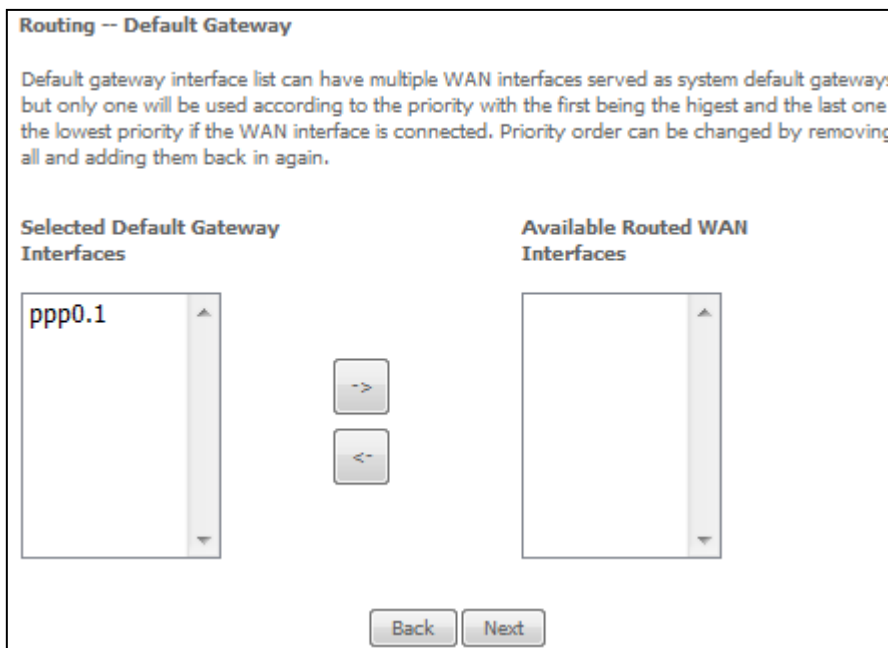
**ENABLE IGMP MULTICAST SOURCE**

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.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN with 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.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces                      Available WAN Interfaces

ppp0.1	->	
	<-	

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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.

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**.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

**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.

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.  
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.  
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 77 User ID:

Option 125:  Disable  Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

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.

**Network Address Translation Settings**

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

**WAN interface with base MAC.**  
Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

### 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.

### 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 4:** Choose an interface to be the default gateway.

**Routing -- Default Gateway**

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.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
eth0.1	

->

<-

Back Next

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.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN with 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.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

eth0.1

->

<-

Available WAN Interfaces

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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:	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.

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**.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 **Bridging**

Allow as IGMP Multicast Source  
 Allow as MLD Multicast Source

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

### **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:	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.

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

**NOTE:** If this bridge connection is your only WAN service, the PRT-6302 will be inaccessible for remote management or technical support from the WAN.

## F2.4 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**.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
 For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

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

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO** ▼

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second)

Number of retries:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable Firewall

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Launch Dhcp6c for Rapid Commit

Fixed MTU

MTU:

Enable PPP Manual Mode

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**MLD Multicast**

Enable MLD Multicast Proxy

Enable MLD Multicast Source

**WAN interface with base MAC.**  
Notice: Only one WAN interface can be cloned to base MAC address.

Enable WAN interface with base MAC

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 PRT-6302 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.

Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

### 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](#).

### 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 PRT-6302 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.

**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. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).

**Routing -- Default Gateway**

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.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
<div style="border: 1px solid #ccc; min-height: 100px; padding: 5px;">ppp0.1</div>	<div style="border: 1px solid #ccc; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">-&gt;</div> <div style="border: 1px solid #ccc; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">&lt;-</div>	<div style="border: 1px solid #ccc; min-height: 100px;"></div>

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: pppoe\_eth0/ppp0.1

Back
Next

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.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN with 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.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

IPv6: 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.

**Obtain IPv6 DNS info from a WAN interface:**

WAN Interface selected:

**Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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:	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.

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

## F2.5 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**.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.  
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

**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.

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.  
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.  
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 77 User ID:

Option 125:  Disable  Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.  
 Notice:  
 If "Obtain an IPv6 address automatically" is chosen, DHCPv6 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.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.  
 Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

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.

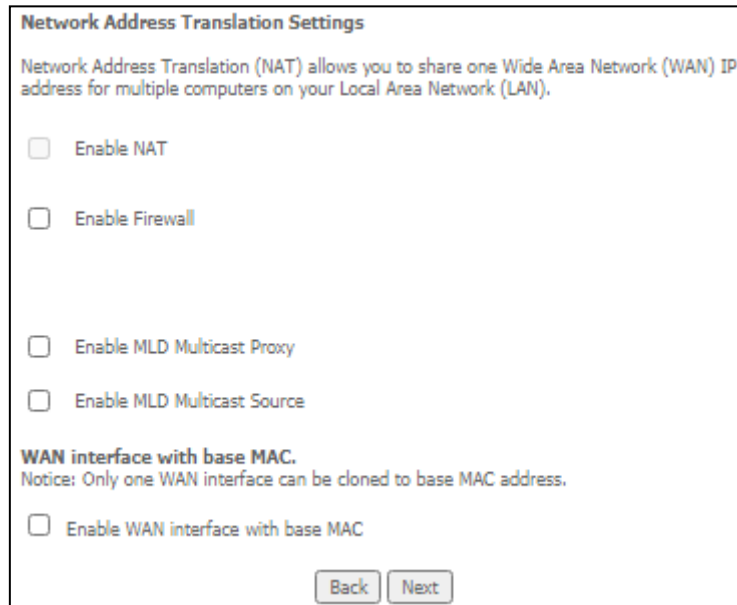
An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

**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**

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 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).

**Routing -- Default Gateway**

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.

**Selected Default Gateway Interfaces**

eth0.1

->

<-

**Available Routed WAN Interfaces**

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

Back
Next

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.

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.

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN with 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.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces	Available WAN Interfaces
eth0.1	
<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

IPv6: 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.

**Obtain IPv6 DNS info from a WAN interface:**

WAN Interface selected:

**Use the following Static IPv6 DNS address:**

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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:	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.

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