

# NexusLink 3240u, NexusLink 3240, NexusLink 3120ua, NexusLink 3120, WAP-5895ua, WR-6895

## 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.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

### CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.



### WARNING

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

## FCC & ISED

### User Information

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

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

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.  
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.  
This device complies with 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 ID: L9VNL3240U**

**IC: 4013C-NL3240U**

**US: 5SYDL01ANL3240U**

**REN: 0.1A**

### **FCC**

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

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

### **ISED**

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

Operations in the 5.15-5.25Ghz band are restricted to indoor usage only.

Le fonctionnement sur la bande 5,15–5,25Ghz est limité à une utilisation intérieure uniquement.

This radio transmitter (identify the device by certification number) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Model Name: AN2450-64D03BBF

Type: External

Gain:

2.4G: 1.2 dBi

5G: 2.5 dBi

Model Name: AN2450-64D02BBF

Type: External

Gain:

2.4G: 2.5 dBi

5G: 2.5 dBi

**The REN statement is the following:**

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

**Copyright**

Copyright©2016 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

|                                                                 |
|-----------------------------------------------------------------|
| <b>NOTE:</b> This document is subject to change without notice. |
|-----------------------------------------------------------------|

**Protect Our Environment**



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

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

# Table of Contents

|                                          |           |
|------------------------------------------|-----------|
| <b>CHAPTER 1 INTRODUCTION.....</b>       | <b>8</b>  |
| <b>CHAPTER 2 INSTALLATION.....</b>       | <b>9</b>  |
| 2.1 HARDWARE SETUP.....                  | 9         |
| 2.2 LED INDICATORS .....                 | 11        |
| <b>CHAPTER 3 WEB USER INTERFACE.....</b> | <b>13</b> |
| 3.1 DEFAULT SETTINGS .....               | 13        |
| 3.2 IP CONFIGURATION.....                | 14        |
| 3.3 LOGIN PROCEDURE.....                 | 16        |
| <b>CHAPTER 4 DEVICE INFORMATION.....</b> | <b>18</b> |
| 4.1 WAN .....                            | 19        |
| 4.2 STATISTICS.....                      | 20        |
| 4.2.1 LAN Statistics .....               | 20        |
| 4.2.2 WAN Service .....                  | 21        |
| 4.2.3 XTM Statistics.....                | 22        |
| 4.2.4 xDSL Statistics.....               | 23        |
| 4.3 ROUTE .....                          | 28        |
| 4.4 ARP.....                             | 29        |
| 4.5 DHCP .....                           | 29        |
| 4.6 NAT SESSION .....                    | 31        |
| 4.7 IGMP INFO.....                       | 32        |
| 4.8 IPV6 .....                           | 33        |
| 4.8.1 IPv6 Info.....                     | 33        |
| 4.8.2 IPv6 Neighbor .....                | 34        |
| 4.8.3 IPv6 Route .....                   | 35        |
| 4.9 CPU & MEMORY .....                   | 36        |
| 4.10 NETWORK MAP .....                   | 37        |
| 4.11 WIRELESS .....                      | 37        |
| 4.11.1 Station Info.....                 | 37        |
| 4.11.2 Site Survey.....                  | 39        |
| <b>CHAPTER 5 BASIC SETUP.....</b>        | <b>40</b> |
| 5.1 WAN SETUP .....                      | 41        |
| 5.1.1 WAN Service Setup .....            | 42        |
| 5.2 NAT .....                            | 43        |
| 5.2.1 Virtual Servers .....              | 43        |
| 5.2.2 Port Triggering.....               | 45        |
| 5.2.3 DMZ Host.....                      | 47        |
| 5.2.4 IP Address Map.....                | 48        |
| 5.2.5 ALG/Pass-Through.....              | 49        |
| 5.3 LAN.....                             | 50        |
| 5.3.1 LAN IPv6 Autoconfig.....           | 53        |
| 5.3.2 Static IP Neighbor .....           | 56        |
| 5.3.3 UPnP .....                         | 57        |
| 5.4 WIRELESS .....                       | 58        |
| 5.4.1 Basic 2.4GHz.....                  | 58        |
| 5.4.2 Security 2.4GHz.....               | 60        |
| 5.4.3 Basic 5GHz.....                    | 62        |
| 5.4.4 Security 5GHz.....                 | 63        |
| 5.5 PARENTAL CONTROL .....               | 64        |
| 5.5.1 Time Restriction.....              | 64        |
| 5.5.2 URL Filter.....                    | 65        |
| 5.6 HOME NETWORKING .....                | 67        |
| 5.6.1 Print Server .....                 | 67        |
| 5.6.2 DLNA.....                          | 67        |
| 5.6.3 Storage Service.....               | 68        |
| 5.6.4 USB Speed .....                    | 69        |

|                                                   |            |
|---------------------------------------------------|------------|
| <b>CHAPTER 6 ADVANCED SETUP .....</b>             | <b>70</b>  |
| 6.1 AUTO-DETECTION SETUP .....                    | 70         |
| 6.2 SECURITY .....                                | 75         |
| 6.2.1 IP Filtering .....                          | 75         |
| 6.2.2 MAC Filtering.....                          | 79         |
| 6.3 QUALITY OF SERVICE (QoS).....                 | 81         |
| 6.3.1 QoS Queue.....                              | 82         |
| 6.3.1.1 QoS Queue Configuration .....             | 82         |
| 6.3.1.2 Wlan Queue .....                          | 86         |
| 6.3.2 QoS Classification .....                    | 87         |
| 6.3.3 QoS Port Shaping.....                       | 89         |
| 6.4 ROUTING .....                                 | 90         |
| 6.4.1 Default Gateway.....                        | 90         |
| 6.4.2 Static Route.....                           | 91         |
| 6.4.3 Policy Routing .....                        | 92         |
| 6.4.4 RIP .....                                   | 93         |
| 6.5 DNS .....                                     | 94         |
| 6.5.1 DNS Server .....                            | 94         |
| 6.5.2 Dynamic DNS .....                           | 95         |
| 6.5.3 DNS Entries.....                            | 96         |
| 6.5.4 DNS Proxy/Relay .....                       | 97         |
| 6.6 DSL.....                                      | 98         |
| 6.7 DSL BONDING.....                              | 99         |
| 6.8 INTERFACE GROUPING .....                      | 100        |
| 6.9 IP TUNNEL .....                               | 103        |
| 6.9.1 IPv6inIPv4.....                             | 103        |
| 6.9.2 IPv4inIPv6.....                             | 104        |
| 6.10 CERTIFICATE.....                             | 105        |
| 6.10.1 Local.....                                 | 105        |
| 6.10.2 Trusted CA.....                            | 107        |
| 6.11 POWER MANAGEMENT .....                       | 108        |
| 6.12 MULTICAST .....                              | 109        |
| 6.13 WIRELESS.....                                | 111        |
| 6.13.1 Basic 2.4GHz.....                          | 111        |
| 6.13.2 Security 2.4GHz.....                       | 113        |
| 6.13.3 WPS 2.4GHz .....                           | 116        |
| 6.13.4 MAC Filter 2.4GHz .....                    | 119        |
| 6.13.5 Wireless Bridge 2.4GHz.....                | 121        |
| 6.13.6 Advanced 2.4GHz .....                      | 122        |
| 6.13.7 Basic 5GHz.....                            | 125        |
| 6.13.8 WPS 5GHz.....                              | 126        |
| 6.13.9 MAC Filter 5GHz .....                      | 128        |
| 6.13.10 Advanced 5GHz .....                       | 129        |
| <b>CHAPTER 7 VOICE.....</b>                       | <b>130</b> |
| 7.1 SIP BASIC SETTING – GLOBAL PARAMETERS.....    | 131        |
| 7.2 SIP BASIC SETTING – SERVICE PROVIDER .....    | 132        |
| 7.3 SIP ADVANCED SETTING – GLOBAL PARAMETERS..... | 135        |
| 7.4 SIP ADVANCED SETTING – SERVICE PROVIDER ..... | 136        |
| 7.5 SIP DEBUG SETTING – GLOBAL PARAMETERS .....   | 139        |
| 7.6 SIP DEBUG SETTING – SERVICE PROVIDER.....     | 140        |
| 7.7 TELEPHONE CALLS .....                         | 141        |
| <b>CHAPTER 8 DIAGNOSTICS.....</b>                 | <b>143</b> |
| 8.1 DIAGNOSTICS – INDIVIDUAL TESTS .....          | 143        |
| 8.2 ETHERNET OAM .....                            | 144        |
| 8.3 UPTIME STATUS .....                           | 146        |
| 8.4 PING .....                                    | 147        |
| 8.5 TRACE ROUTE .....                             | 148        |
| <b>CHAPTER 9 MANAGEMENT .....</b>                 | <b>149</b> |
| 9.1 SETTINGS.....                                 | 149        |

|                                           |                              |            |
|-------------------------------------------|------------------------------|------------|
| 9.1.1                                     | <i>Backup Settings</i> ..... | 149        |
| 9.1.2                                     | <i>Update Settings</i> ..... | 150        |
| 9.1.3                                     | <i>Restore Default</i> ..... | 150        |
| 9.2                                       | SYSTEM LOG .....             | 152        |
| 9.3                                       | SNMP AGENT .....             | 154        |
| 9.4                                       | TR-069 CLIENT .....          | 155        |
| 9.5                                       | INTERNET TIME .....          | 157        |
| 9.6                                       | ACCESS CONTROL .....         | 158        |
| 9.6.1                                     | <i>Accounts</i> .....        | 158        |
| 9.6.2                                     | <i>Services</i> .....        | 160        |
| 9.6.3                                     | <i>IP Address</i> .....      | 161        |
| 9.7                                       | WAKE-ON-LAN .....            | 162        |
| 9.8                                       | UPDATE SOFTWARE .....        | 163        |
| 9.9                                       | REBOOT .....                 | 164        |
| <b>CHAPTER 10 LOGOUT .....</b>            |                              | <b>165</b> |
| <b>APPENDIX A - FIREWALL .....</b>        |                              | <b>166</b> |
| <b>APPENDIX B - PIN ASSIGNMENTS .....</b> |                              | <b>169</b> |
| <b>APPENDIX C – SPECIFICATIONS .....</b>  |                              | <b>170</b> |
| <b>APPENDIX D - SSH CLIENT .....</b>      |                              | <b>172</b> |
| <b>APPENDIX E - PRINTER SERVER.....</b>   |                              | <b>173</b> |
| <b>APPENDIX F - CONNECTION SETUP.....</b> |                              | <b>179</b> |

## Chapter 1 Introduction

NexusLink 3240 is a Multi-DSL bonding solution with optional VoIP service (FXS port x2) for high-performance Internet access. In addition, NexusLink 3240 supports high power (400mw) dual bands (802.11n 2.4GHz & 802.11ac 5GHz) to create a large Wi-Fi footprint for the most seamless video experience as well as blazing fast data speed.

## Chapter 2 Installation

### 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.



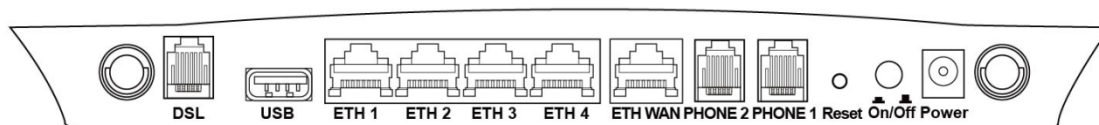
**DO NOT STACK**

#### **Non-stackable**

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

#### **BACK PANEL**

The figure below shows the back panel of the device.



#### **Power ON**

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section [2.2 LED Indicators](#)).

**Caution 1:** If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.

**Caution 2:** Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

#### **Reset Button**

Restore the default parameters of the device by pressing the Reset button for 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section [2.2 LED Indicators](#) for details).

**NOTE:** If pressed down for more than 60 seconds, the NexusLink 3240 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.

### Phone Ports

For VoIP service, connect telephone(s) to these ports with RJ11 cables.

### ETH WAN PORT

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

### Ethernet (LAN) Ports

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

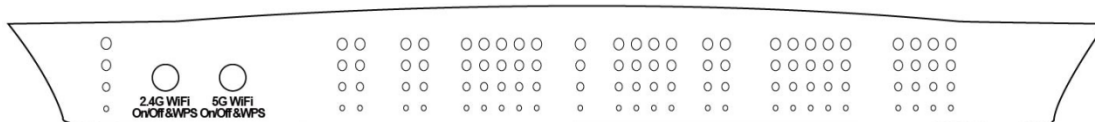
### USB Host Port (Type A)

This port can be used to connect the router to a printer, or supported USB devices.

### DSL Port

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

## FRONT PANEL



### 2.4G WiFi On/Off & WPS Button

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

### 5G WiFi On/Off & WPS Button

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

## 2.2 LED Indicators

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



| LED        | Color  | Mode  | Function                                                                                                                                                                                             |
|------------|--------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POWER      | GREEN  | On    | The device is powered up.                                                                                                                                                                            |
|            |        | Off   | The device is powered down.                                                                                                                                                                          |
|            | 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. |
| PHONE 1    | GREEN  | On    | An FXS port is off hook.                                                                                                                                                                             |
|            |        | Off   | An FXS port is on hook.                                                                                                                                                                              |
| PHONE 2    | GREEN  | On    | An FXS port is off hook.                                                                                                                                                                             |
|            |        | Off   | An FXS port is on hook.                                                                                                                                                                              |
| ETH WAN    | GREEN  | On    | WAN is connected in 1000 Mbps.                                                                                                                                                                       |
|            |        | Off   | Ethernet WAN is not connected.                                                                                                                                                                       |
|            |        | Blink | In TX/RX over 1000 Mbps                                                                                                                                                                              |
|            | YELLOW | On    | Ethernet is connected in 10/100 Mbps.                                                                                                                                                                |
|            |        | Off   | Ethernet WAN is not connected.                                                                                                                                                                       |
|            |        | Blink | In TX/RX over 10/100 Mbps.                                                                                                                                                                           |
| ETH 4 to 1 | GREEN  | On    | Ethernet is connected at 1000 Mbps.                                                                                                                                                                  |
|            |        | Off   | Ethernet is not connected.                                                                                                                                                                           |
|            |        | Blink | In TX/RX over 1000 Mbps.                                                                                                                                                                             |
|            | YELLOW | On    | Ethernet is connected at 10/100 Mbps.                                                                                                                                                                |
|            |        | Off   | Ethernet is not connected.                                                                                                                                                                           |
|            |        | Blink | In TX/RX over 10/100 Mbps.                                                                                                                                                                           |
| WPS        | GREEN  | On    | WPS(2.4G) WPS enabled and client connected to WLAN.                                                                                                                                                  |
|            |        | Off   | WPS(2.4G) WPS disabled.                                                                                                                                                                              |
|            |        | Blink | WPS(2.4G) WPS connection in progress, 120 seconds or until client connected.                                                                                                                         |
|            | YELLOW | On    | WPS(5G) WPS enabled and client connected to WLAN.                                                                                                                                                    |
|            |        | Off   | WPS(5G) WPS disabled.                                                                                                                                                                                |
|            |        | Blink | WPS(5G) WPS connection in progress, 120 seconds or until client connected.                                                                                                                           |

|              |       |       |                                                                                                                                                                                                        |
|--------------|-------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WiFi<br>2.4G | GREEN | On    | The wireless module is ready.<br>(i.e. installed and enabled).                                                                                                                                         |
|              |       | Off   | The wireless module is not ready.<br>(i.e. either not installed or disabled).                                                                                                                          |
|              |       | Blink | Data transmitting or receiving over WLAN.                                                                                                                                                              |
| WiFi<br>5G   | GREEN | On    | The wireless module is ready.<br>(i.e. installed and enabled).                                                                                                                                         |
|              |       | Off   | The wireless module is not ready.<br>(i.e. either not installed or disabled).                                                                                                                          |
|              |       | Blink | Data transmitting or receiving over WLAN.                                                                                                                                                              |
| DSL 1        | GREEN | On    | xDSL Link is established.                                                                                                                                                                              |
|              |       | Off   | xDSL Link is not established.                                                                                                                                                                          |
|              |       | Blink | The xDSL link is training or some traffic is passing<br>through xDSL.                                                                                                                                  |
| DSL 2        | GREEN | On    | xDSL Link is established.                                                                                                                                                                              |
|              |       | Off   | xDSL Link is not established.                                                                                                                                                                          |
|              |       | Blink | The xDSL link is training or some traffic is passing<br>through xDSL.                                                                                                                                  |
| INTERNET     | GREEN | On    | IP connected and no traffic detected. If an IP or<br>PPPoE session is dropped due to an idle timeout, the<br>light will remain green if an ADSL connection is still<br>present.                        |
|              |       | Off   | Modem power off, modem in bridged mode or ADSL<br>connection not present. In addition, if an IP or<br>PPPoE session is dropped for any reason, other than<br>an idle timeout, the light is turned off. |
|              |       | Blink | IP connected and IP Traffic is passing thru the<br>device (either direction)                                                                                                                           |
|              | RED   | On    | Device attempted to become IP connected and<br>failed (no DHCP response, no PPPoE response,<br>PPPoE authentication failed, no IP address from<br>IPCP, etc.)                                          |

## Chapter 3 Web User Interface

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

### 3.1 Default Settings

The factory default settings of this device are summarized below.

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

#### **Technical Note**

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

## 3.2 IP Configuration

### DHCP MODE

When the NexusLink 3240 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.

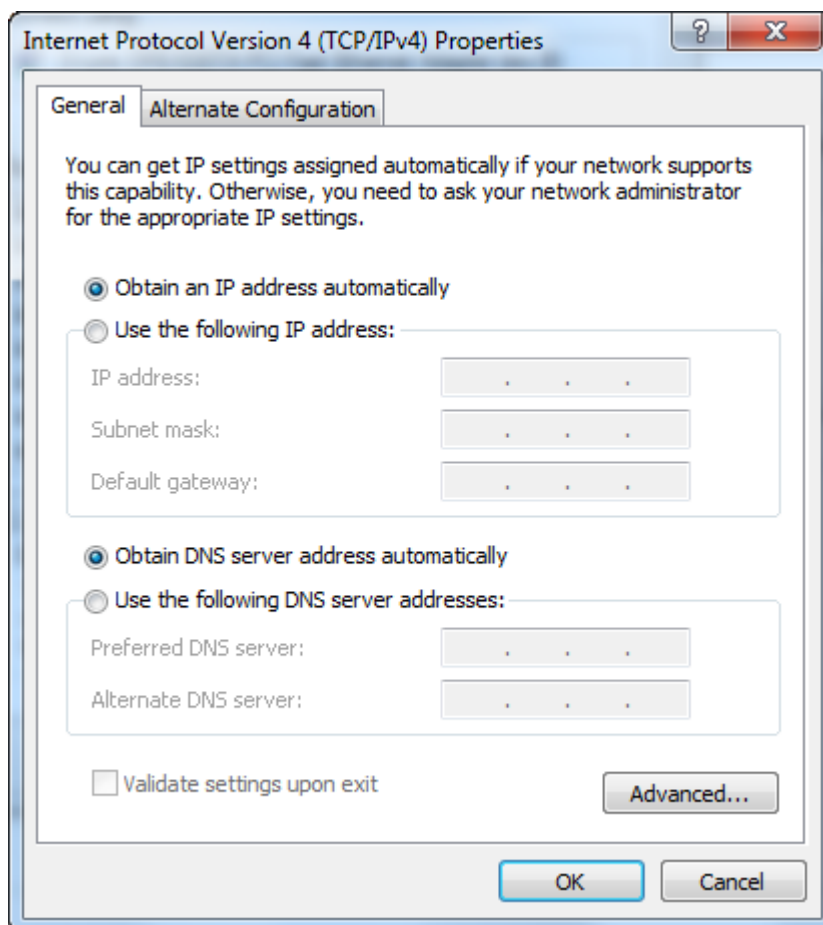
To obtain an IP address from the DHCP server, follow the steps provided below.

**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.

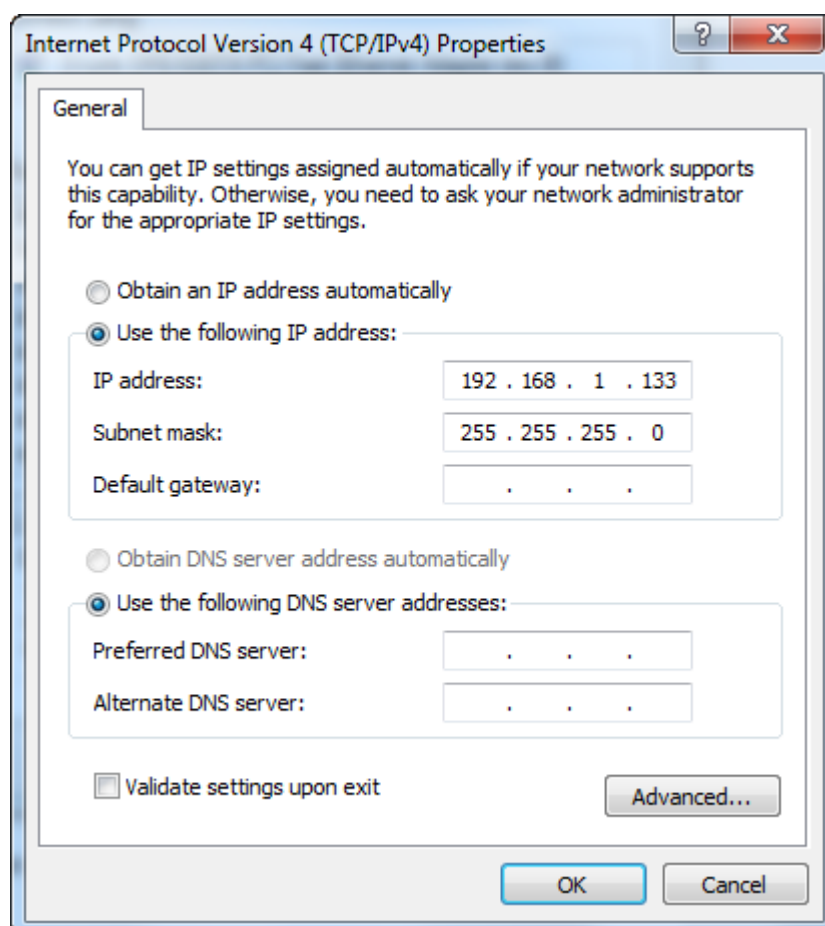
## STATIC IP MODE

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 [9.6.1 Accounts](#)).

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


**COMTREND**

 Device Info
 Basic Setup
 Advanced Setup
 Voice
 Diagnostics
 Management
 Logout

Summary

WAN

Statistics

Route

ARP

DHCP

NAT Session

IGMP Info

IPv6

CPU & Memory

Network Map

Wireless

**Device**

|                          |                                      |
|--------------------------|--------------------------------------|
| Model                    | NexusLink 3240                       |
| Board ID                 | 63138MB1-1861AC                      |
| Serial Number            | 0                                    |
| Firmware Version         | O111-S416CTU-C01_R01.A2pvh042g2.d26i |
| Bootloader (CFE) Version | 1.0.38-116.174-11                    |
| Up Time                  | 10 mins:6 secs                       |

**Wireless**

|                                                                                   |                                                                                                        |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Driver Version                                                                    | 7.14.89.3303.cpe4.16L03.0-kdb                                                                          |
| Primary SSID                                                                      | Comtrend4011_2.4GHz                                                                                    |
| Status                                                                            | Enabled                                                                                                |
| Channel                                                                           | 11                                                                                                     |
|  | Secure                                                                                                 |
| Primary Encryption                                                                | WPA2-PSK AES                                                                                           |
| Primary Passphrase/Key                                                            | <div style="display: flex; align-items: center;"> <div style="flex: 1;">•</div> <div>Show</div> </div> |

**LAN**

  
ETH1

  
ETH2

  
ETH3

  
ETH4

|                  |                   |
|------------------|-------------------|
| LAN IPv4 Address | 192.168.1.1       |
| LAN Subnet Mask  | 255.255.255.0     |
| LAN MAC Address  | 64:68:0c:32:40:11 |
| DHCP Server      | Enabled           |

**WAN**

  
DOWN

|                        |          |
|------------------------|----------|
| Traffic Type           | Inactive |
| Upstream Rate (Kbps)   | 0        |
| Downstream Rate (Kbps) | 0        |
| 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.

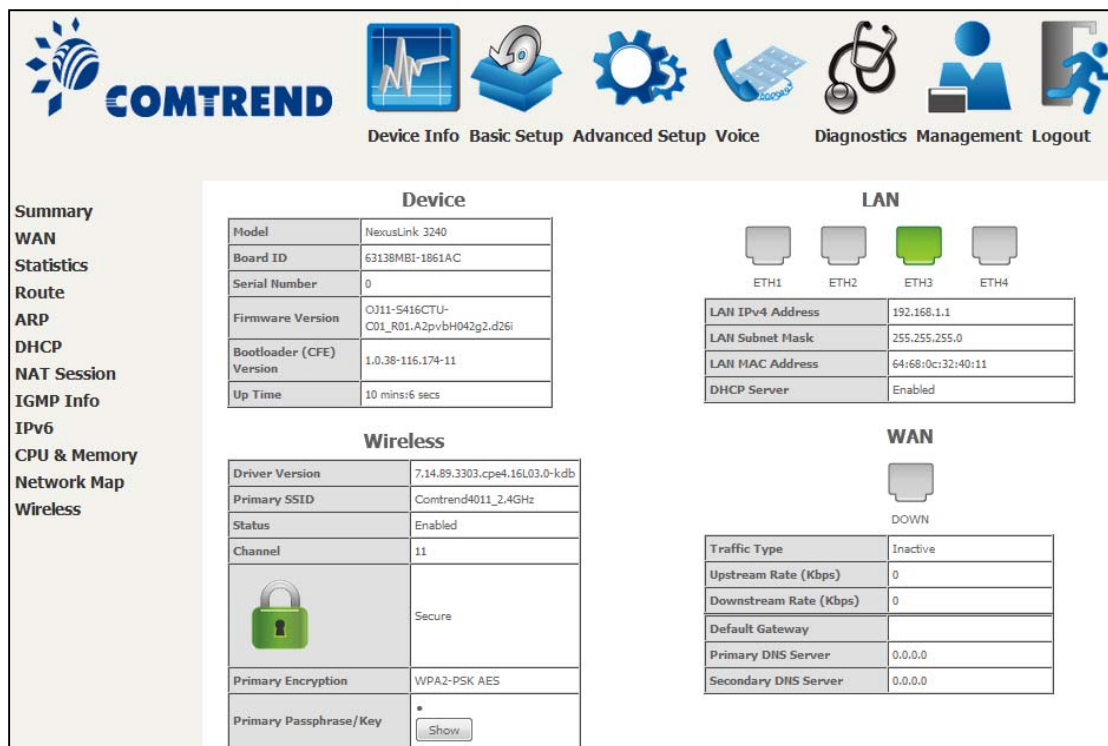


The web user interface window is divided into two frames, the main menu (on the left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

**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.



**Device**

|                          |                                       |
|--------------------------|---------------------------------------|
| Model                    | NexusLink 3240                        |
| Board ID                 | 63138MB1-1861AC                       |
| Serial Number            | 0                                     |
| Firmware Version         | OJ11-S416CTU-C01_R01.A2pvbH042g2.d26i |
| Bootloader (CFE) Version | 1.0.38-116.174-11                     |
| Up Time                  | 10 mins:6 secs                        |

**LAN**

|                                   |      |      |      |
|-----------------------------------|------|------|------|
| ETH1                              | ETH2 | ETH3 | ETH4 |
| LAN IPv4 Address 192.168.1.1      |      |      |      |
| LAN Subnet Mask 255.255.255.0     |      |      |      |
| LAN MAC Address 64:68:0c:32:40:11 |      |      |      |
| DHCP Server Enabled               |      |      |      |

**Wireless**

|                        |                               |
|------------------------|-------------------------------|
| Driver Version         | 7.14.89.3303.cpe4.16L03.0-kdb |
| Primary SSID           | Comtrend4011_2.4GHz           |
| Status                 | Enabled                       |
| Channel                | 11                            |
| Secure                 | Secure                        |
| Primary Encryption     | WPA2-PSK AES                  |
| Primary Passphrase/Key | Show                          |

**WAN**

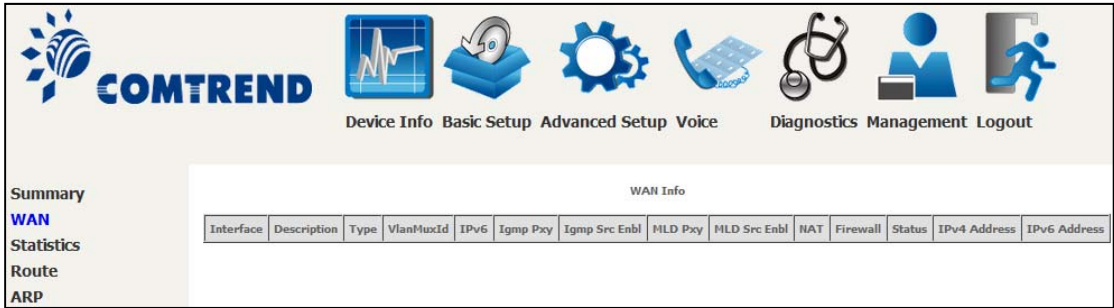
DOWN

|                        |          |
|------------------------|----------|
| Traffic Type           | Inactive |
| Upstream Rate (Kbps)   | 0        |
| Downstream Rate (Kbps) | 0        |
| 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).



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

## 4.2 Statistics

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

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

### 4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.











Summary

WAN

Statistics

LAN

WAN Service

xTM

xDSL

Route

ARP

DHCP

NAT Session

IGMP Info

IPv6

Statistics – LAN

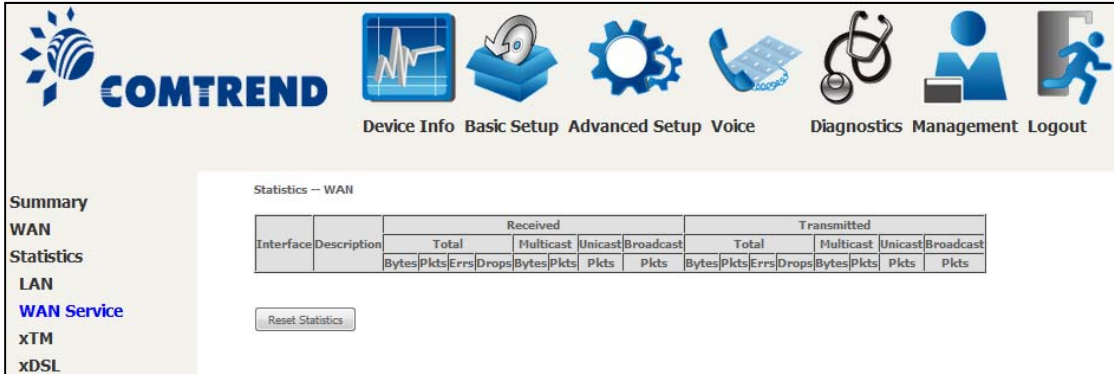
| Interface            | Received |      |      |       |           |      |      |      | Transmitted |      |      |       |           |      |      |      |
|----------------------|----------|------|------|-------|-----------|------|------|------|-------------|------|------|-------|-----------|------|------|------|
|                      | Total    |      |      |       | Multicast |      |      |      | Unicast     |      |      |       | Broadcast |      |      |      |
|                      | Bytes    | Pkts | Errs | Drops | Bytes     | Pkts | Pkts | Pkts | Bytes       | Pkts | Errs | Drops | Bytes     | Pkts | Pkts | Pkts |
| ETHWAN               | 0        | 0    | 0    | 0     | 0         | 0    | 0    | 0    | 0           | 0    | 0    | 0     | 0         | 0    | 0    | 0    |
| ETH1                 | 0        | 0    | 0    | 0     | 0         | 0    | 0    | 0    | 0           | 0    | 0    | 0     | 0         | 0    | 0    | 0    |
| ETH2                 | 0        | 0    | 0    | 0     | 0         | 0    | 0    | 0    | 0           | 0    | 0    | 0     | 0         | 0    | 0    | 0    |
| ETH3                 | 288507   | 2734 | 0    | 0     | 0         | 214  | 2264 | 256  | 564578      | 1855 | 0    | 0     | 0         | 250  | 1546 | 59   |
| ETH4                 | 0        | 0    | 0    | 0     | 0         | 0    | 0    | 0    | 0           | 0    | 0    | 0     | 0         | 0    | 0    | 0    |
| Comtrend4011_5GHz_IF | 82948    | 352  | 0    | 0     | 0         | 236  | 116  | 0    | 72273       | 690  | 0    | 0     | 0         | 279  | 114  | 297  |
| Comtrend4011_2.4GHz  | 0        | 0    | 0    | 6     | 0         | 0    | 0    | 0    | 0           | 0    | 0    | 0     | 0         | 0    | 0    | 1    |
| Comtrend4011_5GHz    | 0        | 0    | 0    | 0     | 0         | 0    | 0    | 0    | 27508       | 257  | 0    | 0     | 0         | 257  | 0    | 0    |

[Reset Statistics](#)

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

## 4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.



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

### 4.2.3 XTM Statistics

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



#### XTM Interface Statistics

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



## ADSL











Summary

WAN

Statistics

LAN

WAN Service

xTM

**xDSL**

Route

ARP

DHCP

NAT Session

IGMP Info

IPv6

Wireless

Statistics -- xDSL

Bonding Line Selection DSL1

|                                                |            |          |
|------------------------------------------------|------------|----------|
| Mode:                                          | ADSL_2plus |          |
| Traffic Type:                                  | ATM        |          |
| Status:                                        | Up         |          |
| Link Power State:                              | L0         |          |
|                                                | Downstream | Upstream |
| PhyR Status:                                   | Off        | Off      |
| Line Coding (Trellis):                         | On         | On       |
| SNR Margin (0.1 dB):                           | 61         | 74       |
| Attenuation (0.1 dB):                          | 20         | 0        |
| Output Power (0.1 dBm):                        | 42         | 94       |
| Attainable Rate (Kbps):                        | 29628      | 1441     |
|                                                | Path 0     |          |
|                                                | Downstream | Upstream |
| Rate (Kbps):                                   | 29627      | 1386     |
| MSGc (# of bytes in overhead channel message): | 51         | 18       |
| B (# of bytes in Mux Data Frame):              | 243        | 111      |
| M (# of Mux Data Frames in FEC Data Frame):    | 1          | 2        |
| T (Mux Data Frames over sync bytes):           | 4          | 1        |
| R (# of check bytes in FEC Data Frame):        | 0          | 6        |
| S (ratio of FEC over PMD Data Frame length):   | 0.2847     | 5.5421   |
| L (# of bits in PMD Data Frame):               | 6855       | 332      |
| D (interleaver depth):                         | 1          | 8        |
| Delay (msec):                                  | 0          | 11       |
| INP (DMT symbol):                              | 0.00       | 0.50     |
| Super Frames:                                  | 0          | 0        |
| Super Frame Errors:                            | 5235       | 0        |
| RS Words:                                      | 0          | 42554    |
| RS Correctable Errors:                         | 0          | 0        |
| RS Uncorrectable Errors:                       | 0          | 0        |
| HEC Errors:                                    | 870        | 0        |
| OCD Errors:                                    | 0          | 0        |
| LCD Errors:                                    | 0          | 0        |
| Total Cells:                                   | 4135034    | 176965   |
| Data Cells:                                    | 0          | 0        |
| Bit Errors:                                    | 0          | 0        |
| Total ES:                                      | 10         | 0        |
| Total SES:                                     | 10         | 0        |
| Total UAS:                                     | 87         | 77       |

xDSL BER Test
Reset Statistics
Draw Graph

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

| Field                 | Description                                                                         |
|-----------------------|-------------------------------------------------------------------------------------|
| Mode                  | VDSL, VDSL2                                                                         |
| Traffic Type          | ATM, PTM                                                                            |
| Status                | Lists the status of the DSL link                                                    |
| Link Power State      | Link output power state                                                             |
| phyR Status           | Shows the status of PhyR™ (Physical Layer Re-Transmission) impulse noise protection |
| Line Coding (Trellis) | Trellis On/Off                                                                      |

| Field                  | Description                                                      |
|------------------------|------------------------------------------------------------------|
| SNR Margin (0.1 dB)    | Signal to Noise Ratio (SNR) margin                               |
| Attenuation (0.1 dB)   | Estimate of average loop attenuation in the downstream direction |
| Output Power (0.1 dBm) | Total upstream output power                                      |
| Attainable Rate (Kbps) | The sync rate you would obtain                                   |
| Rate (Kbps)            | Current sync rates downstream/upstream                           |

**In VDSL mode, the following section is inserted.**

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

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

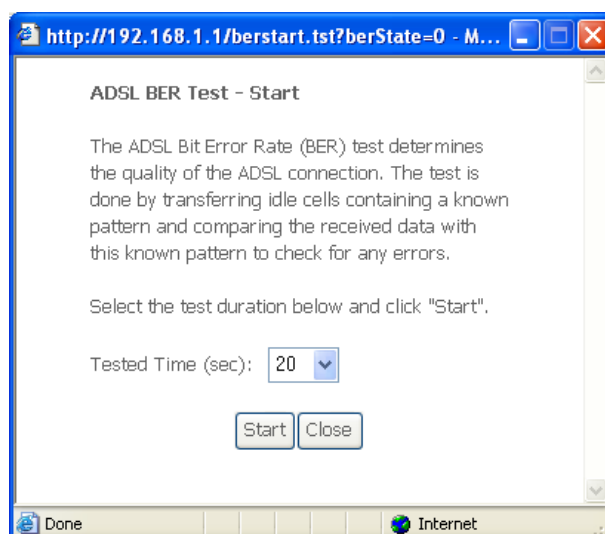
|                         |                                                    |
|-------------------------|----------------------------------------------------|
| OH Frames               | Total number of OH frames                          |
| OH Frame Errors         | Number of OH frames received with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

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

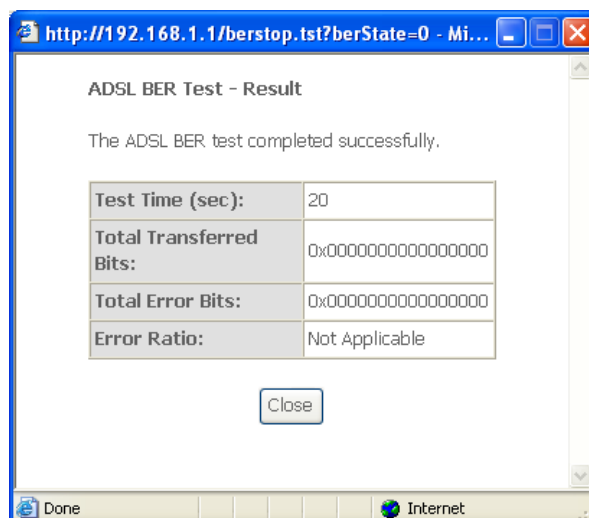
|           |                                          |
|-----------|------------------------------------------|
| Total ES  | Total Number of Errored Seconds          |
| Total SES | Total Number of Severely Errored Seconds |
| Total UAS | Total Number of Unavailable Seconds      |

### xDSL BER TEST

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

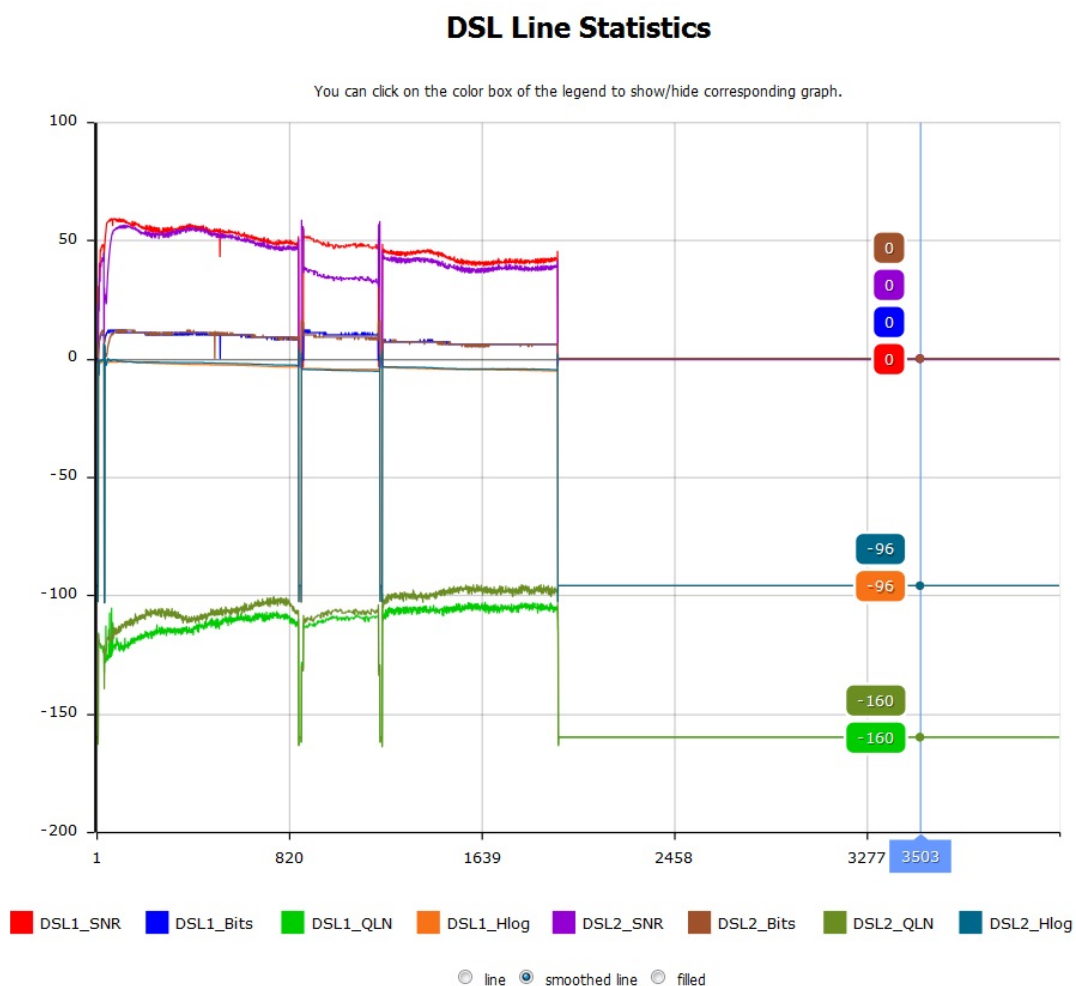


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



## xDSL TONE GRAPH

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



## 4.3 Route

Choose **Route** to display the routes that the NexusLink 3240 has found.



The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Voice, Diagnostics, Management, and Logout. The left sidebar lists Summary, WAN, Statistics, **Route** (highlighted), ARP, and DHCP. The main content area is titled 'Device Info -- Route' and displays a table of routes.

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

| Destination | Gateway | Subnet Mask   | Flag | Metric | Service | Interface |
|-------------|---------|---------------|------|--------|---------|-----------|
| 1.1.1.0     | 0.0.0.0 | 255.255.255.0 | U    | 0      |         | br0       |
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U    | 0      |         | br0       |

| Field       | Description                                                                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination | Destination network or destination host                                                                                                                                                                               |
| Gateway     | Next hop IP address                                                                                                                                                                                                   |
| Subnet Mask | Subnet Mask of Destination                                                                                                                                                                                            |
| Flag        | U: route is up<br>!: reject route<br>G: use gateway<br>H: target is a host<br>R: reinstate route for dynamic routing<br>D: dynamically installed by daemon or redirect<br>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.











Device Info Basic Setup Advanced Setup Voice
Diagnostics Management Logout

Summary

WAN

Statistics

Route

**ARP**

Device Info -- ARP

| IP address  | Flags    | HW Address        | Device |
|-------------|----------|-------------------|--------|
| 192.168.1.2 | Complete | 00:50:ba:24:29:bd | br0    |

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

## 4.5 DHCP

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











Device Info Basic Setup Advanced Setup Voice
Diagnostics Management Logout

Summary

WAN

Statistics

Route

ARP

**DHCP**

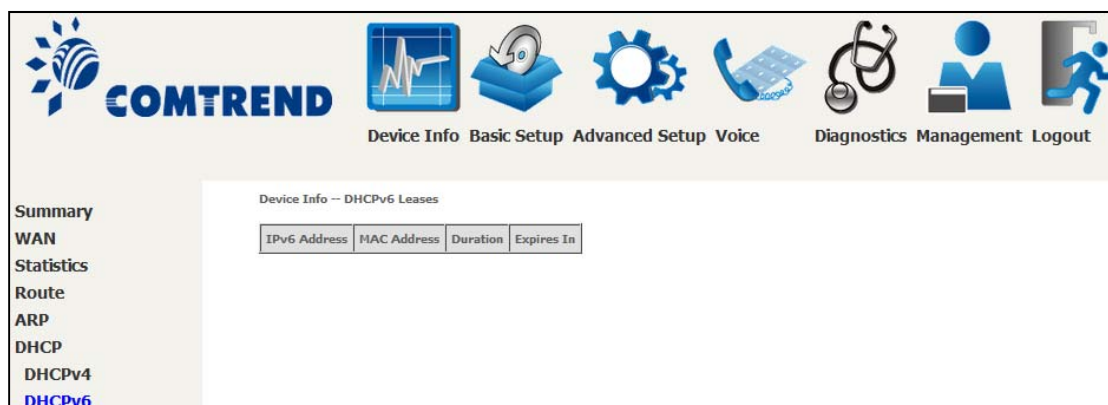
DHCPv4

DHCPv6

Device Info -- DHCP Leases

| Hostname      | MAC Address       | IP Address  | Expires In                      |
|---------------|-------------------|-------------|---------------------------------|
| TrevorOwens02 | 00:50:ba:24:29:bd | 192.168.1.2 | 23 hours, 34 minutes, 3 seconds |
|               | 00:00:00:11:11:11 | 1.1.1.2     | Expired/Unknown                 |

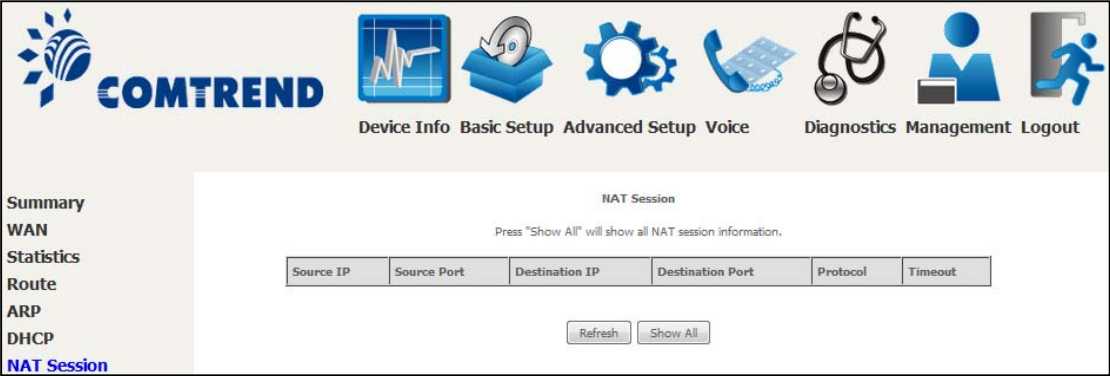
| Field       | Description                                          |
|-------------|------------------------------------------------------|
| Hostname    | Shows the device/host/PC network name                |
| MAC Address | Shows the Ethernet MAC address of the device/host/PC |
| IP Address  | Shows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



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

## 4.6 NAT Session

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



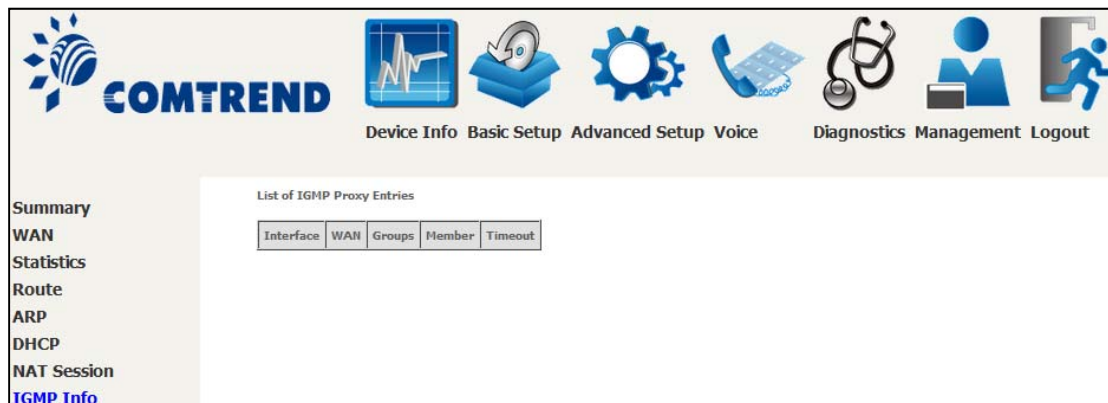
Click the “Show All” button to display the following.

| NAT Session                                                           |             |                |                  |          |         |
|-----------------------------------------------------------------------|-------------|----------------|------------------|----------|---------|
| Press "Show Less" will show NAT session information on WAN side only. |             |                |                  |          |         |
| Source IP                                                             | Source Port | Destination IP | Destination Port | Protocol | Timeout |
| 192.168.1.1                                                           | 138         | 192.168.1.255  | 138              | udp      | 23      |
| 192.168.1.2                                                           | 53247       | 192.168.1.1    | 80               | tcp      | 86399   |
| 127.0.0.1                                                             | 45000       | 127.0.0.1      | 45032            | udp      | 29      |
| <div>Refresh Show Less</div>                                          |             |                |                  |          |         |

| Field            | 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 IGMP proxy enabled wan connection.

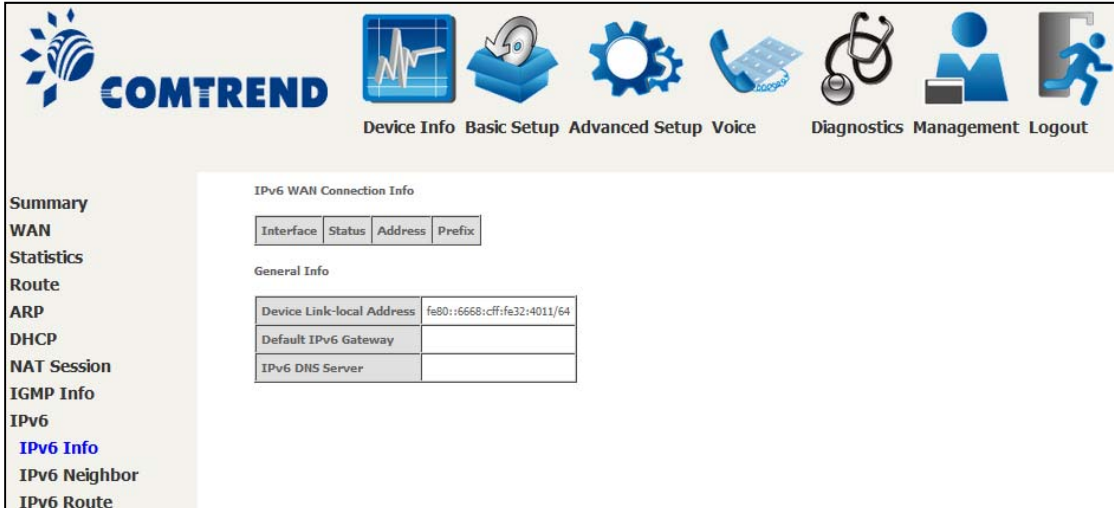


| Field     | Description                                                    |
|-----------|----------------------------------------------------------------|
| Interface | The Source interface from which the IGMP report was received   |
| WAN       | The WAN interface from which the multicast traffic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

## 4.8 IPv6

### 4.8.1 IPv6 Info

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



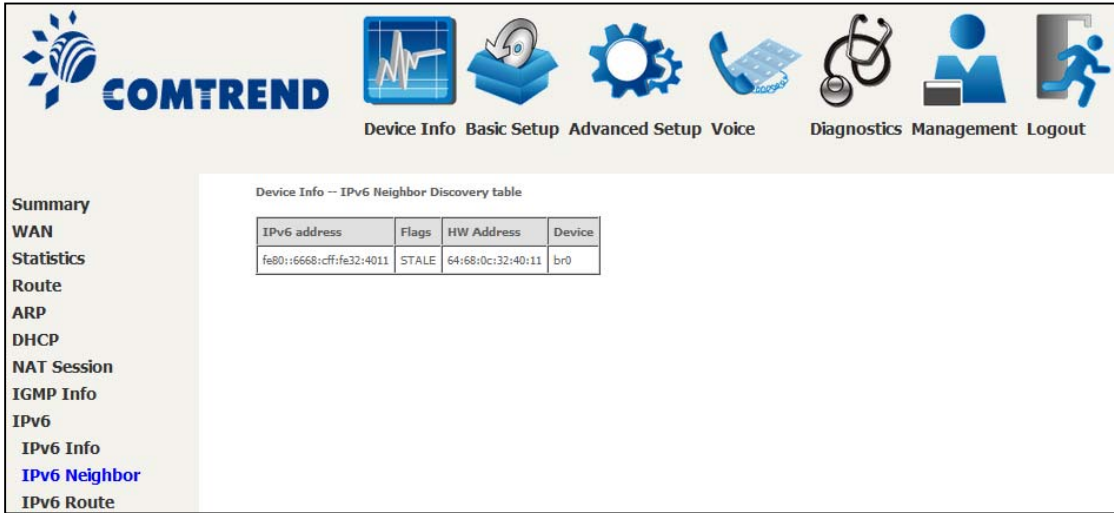
**IPv6 WAN Connection Info**

| Interface                 | Status                      | Address | Prefix |
|---------------------------|-----------------------------|---------|--------|
| General Info              |                             |         |        |
| Device Link-local Address | fe80::6668:cff:fe32:4011/64 |         |        |
| Default IPv6 Gateway      |                             |         |        |
| IPv6 DNS Server           |                             |         |        |

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

## 4.8.2 IPv6 Neighbor

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



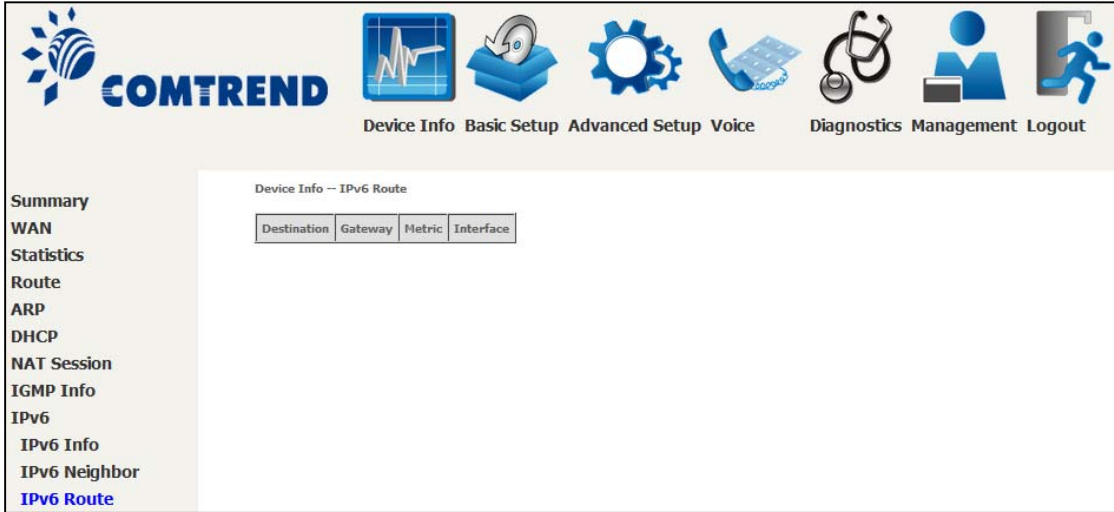
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons and labels for Device Info, Basic Setup, Advanced Setup, Voice, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with links for Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, IPv6 Info, **IPv6 Neighbor** (highlighted), and IPv6 Route. The main content area displays the title "Device Info -- IPv6 Neighbor Discovery table" above a table with the following data:

| IPv6 address             | Flags | HW Address        | Device |
|--------------------------|-------|-------------------|--------|
| fe80::6668:cff:fe32:4011 | STALE | 64:68:0c:32:40:11 | br0    |

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

### 4.8.3 IPv6 Route

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



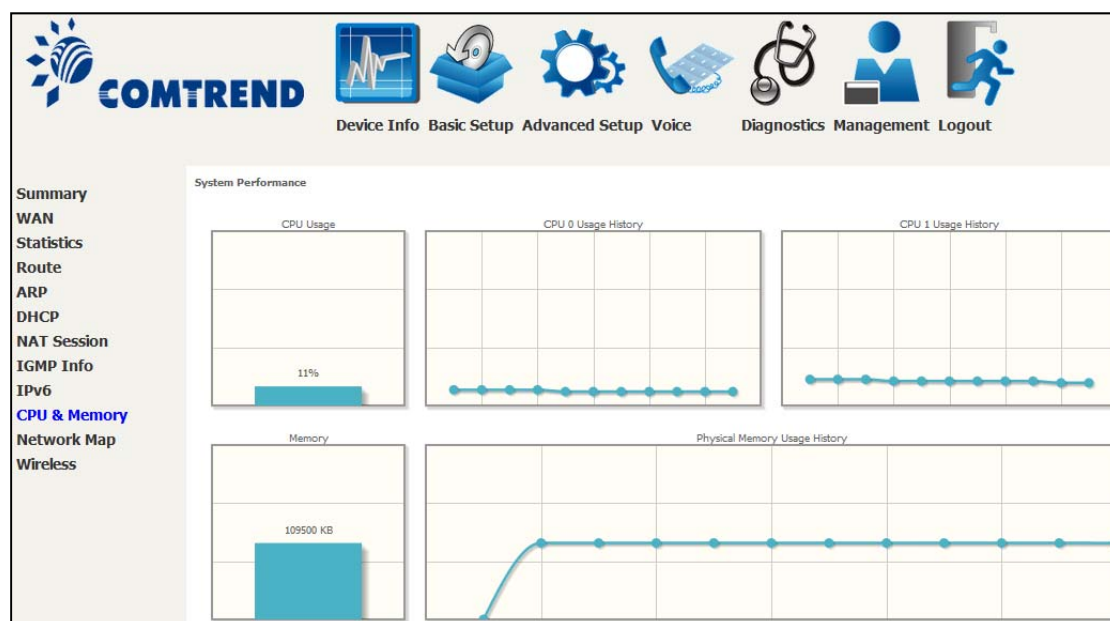
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, Voice, Diagnostics, Management, and Logout. Below the navigation bar, on the left side, there is a sidebar menu with the following items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, IPv6 Info, IPv6 Neighbor, and **IPv6 Route** (which is highlighted in blue). The main content area is titled "Device Info -- IPv6 Route" and contains a table with four columns: Destination, Gateway, Metric, and Interface.

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

## 4.9 CPU & Memory

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

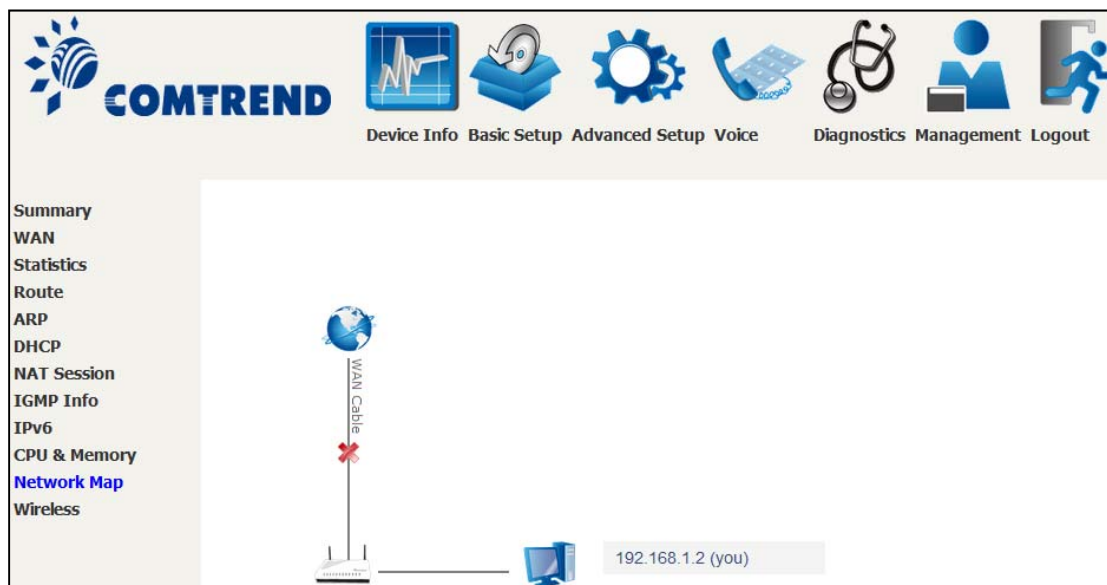
Note: This graph is unavailable for Internet Explorer users.



## 4.10 Network Map

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

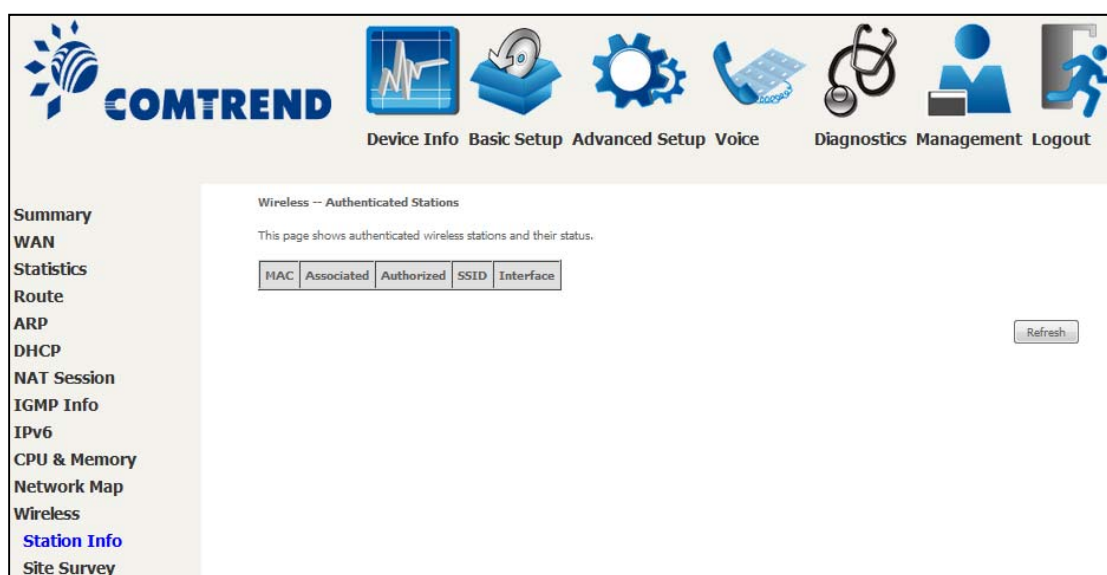
Note: This graph is unavailable for Internet Explorer users.



## 4.11 Wireless

### 4.11.1 Station Info

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

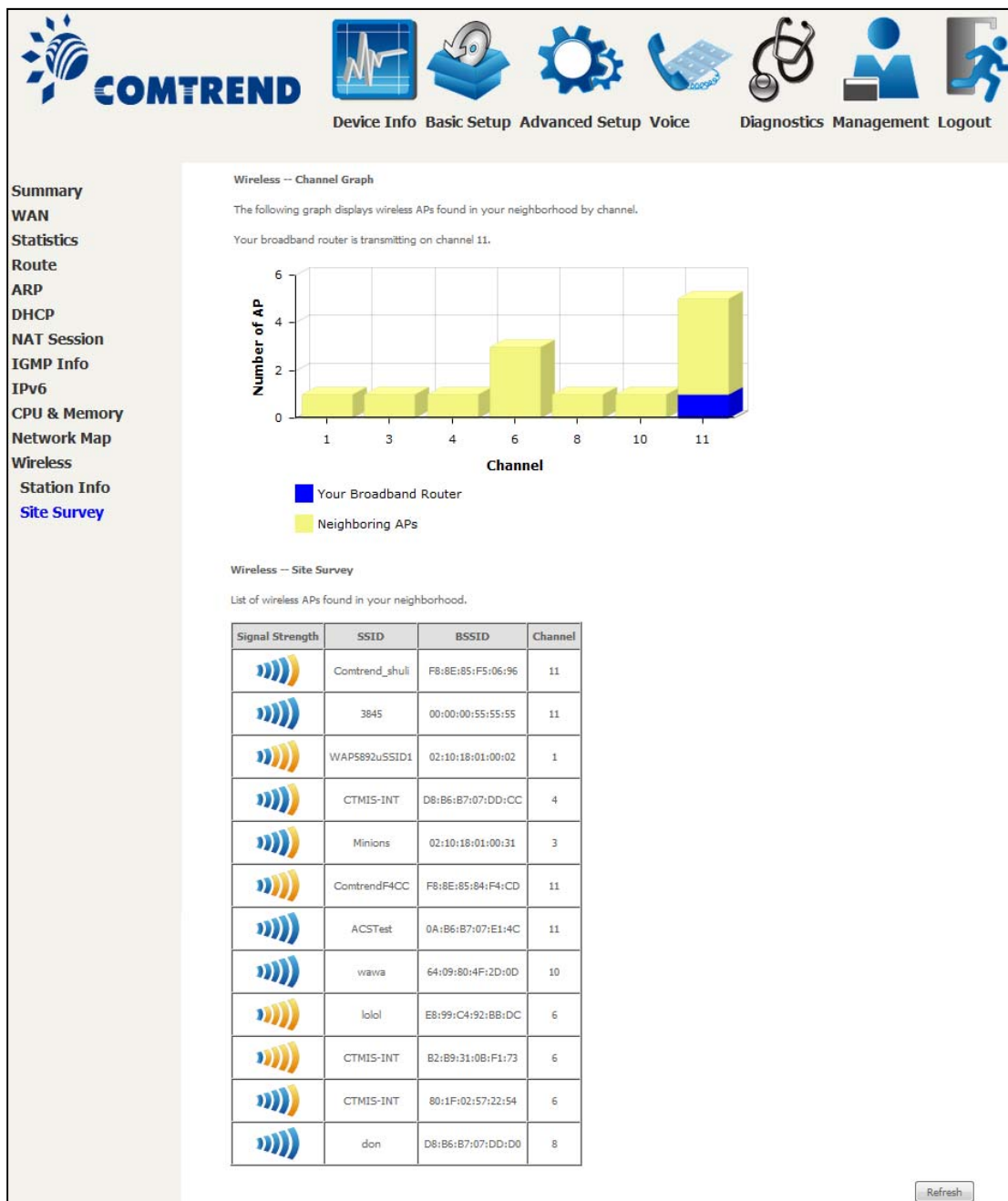


Consult the table below for descriptions of each column heading.

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

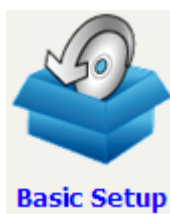
## 4.11.2 Site Survey

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



## 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.











**WAN Setup**

**NAT**

**LAN**

**Wireless**

**Parental Control**

**Home Networking**

**LAN**

ETH1

ETH2

ETH3

ETH4

|                  |                   |
|------------------|-------------------|
| LAN IPv4 Address | 192.168.1.1       |
| LAN Subnet Mask  | 255.255.255.0     |
| LAN MAC Address  | 64:68:0c:32:40:11 |
| DHCP Server      | Enabled           |

**WAN**

DOWN

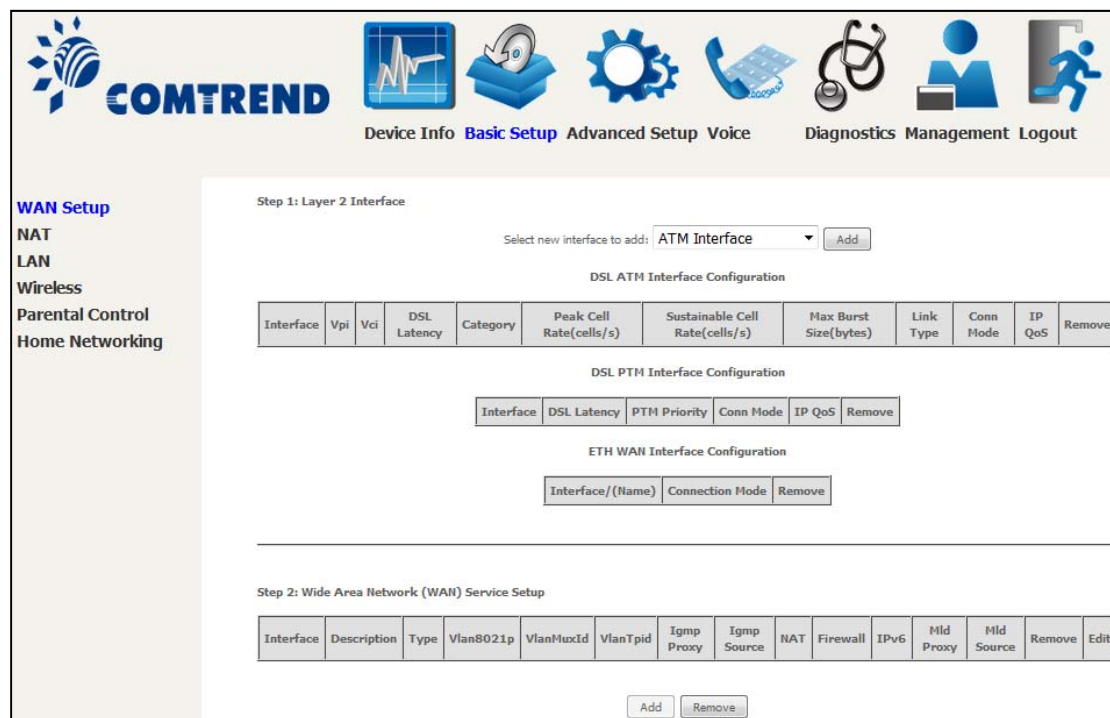
|                        |          |
|------------------------|----------|
| Traffic Type           | Inactive |
| Upstream Rate (Kbps)   | 0        |
| Downstream Rate (Kbps) | 0        |
| Default Gateway        |          |
| Primary DNS Server     | 0.0.0.0  |
| Secondary DNS Server   | 0.0.0.0  |

**Wireless**

|                                                                                     |                                       |
|-------------------------------------------------------------------------------------|---------------------------------------|
| Driver Version                                                                      | 7.14.89.3303.cpe4.16L03.0-kdb         |
| Primary SSID                                                                        | Comtrend4011_2.4GHz                   |
| Status                                                                              | Enabled                               |
| Channel                                                                             | 11                                    |
|  | Secure                                |
| Primary Encryption                                                                  | WPA2-PSK AES                          |
| Primary Passphrase/Key                                                              | * <input type="button" value="Show"/> |

## 5.1 Wan Setup

Add or remove ATM, PTM and ETH WAN interface connections here.



**COMTREND**

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

**WAN Setup**  
 NAT  
 LAN  
 Wireless  
 Parental Control  
 Home Networking

Step 1: Layer 2 Interface

Select new interface to add: ATM Interface

DSL ATM Interface Configuration

| Interface | Vpi | Vci | DSL Latency | Category | Peak Cell Rate(cells/s) | Sustainable Cell Rate(cells/s) | Max Burst Size(bytes) | Link Type | Conn Mode | IP QoS | Remove |
|-----------|-----|-----|-------------|----------|-------------------------|--------------------------------|-----------------------|-----------|-----------|--------|--------|
|-----------|-----|-----|-------------|----------|-------------------------|--------------------------------|-----------------------|-----------|-----------|--------|--------|

DSL PTM Interface Configuration

| Interface | DSL Latency | PTM Priority | Conn Mode | IP QoS | Remove |
|-----------|-------------|--------------|-----------|--------|--------|
|-----------|-------------|--------------|-----------|--------|--------|

ETH WAN Interface Configuration

| Interface/(Name) | Connection Mode | Remove |
|------------------|-----------------|--------|
|------------------|-----------------|--------|

Step 2: Wide Area Network (WAN) Service Setup

| Interface | Description | Type | Vlan8021p | VlanMuxId | VlanTpid | Igmp Proxy | Igmp Source | NAT | Firewall | IPv6 | Hld Proxy | Hld Source | Remove | Edit |
|-----------|-------------|------|-----------|-----------|----------|------------|-------------|-----|----------|------|-----------|------------|--------|------|
|-----------|-------------|------|-----------|-----------|----------|------------|-------------|-----|----------|------|-----------|------------|--------|------|

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

**NOTE:** Up to 8 ATM interfaces can be created and saved in flash memory.

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

### 5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

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 | Remove | Edit |
|--------------------------------------------------------------------------|-------------|------|-----------|-----------|----------|------------|-------------|-----|----------|------|-----------|------------|--------|------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> |             |      |           |           |          |            |             |     |          |      |           |            |        |      |

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

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

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 | Remove                           | Edit                                |
|--------------------------------------------------------------------------|--------------|-------|-----------|-----------|----------|------------|-------------|---------|----------|----------|-----------|------------|----------------------------------|-------------------------------------|
| ppp0.1                                                                   | pppoe_0_0_35 | PPPoE | N/A       | N/A       | N/A      | Disabled   | Disabled    | Enabled | Disabled | Disabled | Disabled  | Disabled   | <input checked="" type="radio"/> | <input type="button" value="Edit"/> |
| <input type="button" value="Add"/> <input type="button" value="Remove"/> |              |       |           |           |          |            |             |         |          |          |           |            |                                  |                                     |

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

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

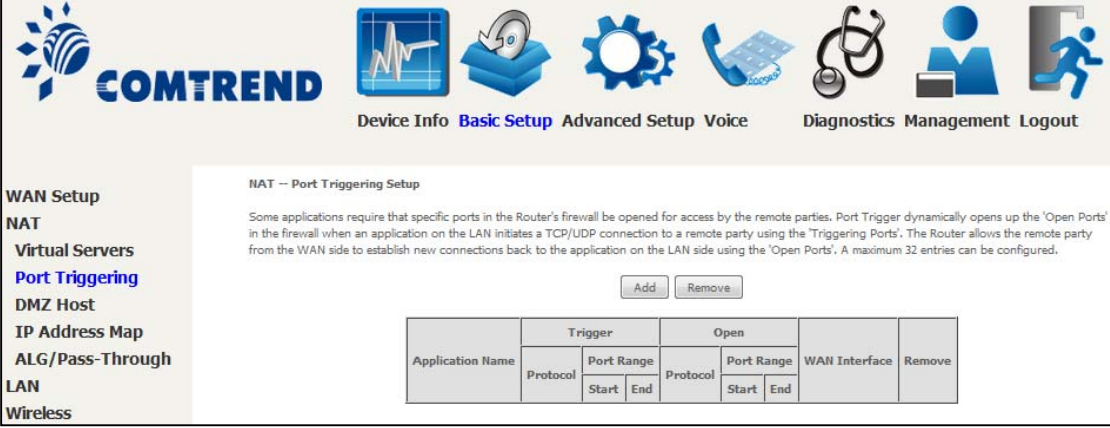
**NOTE:** Up to 16 PVC profiles can be configured and saved in flash memory.



| Field / Header                                  | Description                                                                                                                                        |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Choose All Interface                            | Virtual server rules will be created for all WAN interfaces.                                                                                       |
| Choose One Interface<br>Use Interface           | Select a WAN interface from the drop-down menu.                                                                                                    |
| Select a Service<br><b>Or</b><br>Custom Service | User should select the service from the list.<br><b>Or</b><br>User can enter the name of their choice.                                             |
| Server IP Address                               | Enter the IP address for the server.                                                                                                               |
| Enable NAT Loopback                             | Allows local machines to access virtual server via WAN IP Address                                                                                  |
| External Port Start                             | Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured. |
| External Port End                               | Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.   |
| Protocol                                        | TCP, TCP/UDP, or UDP.                                                                                                                              |
| Internal Port Start                             | Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured   |
| Internal Port End                               | Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.   |

## 5.2.2 Port Triggering

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



**COMTREND**

Device Info Basic Setup Advanced Setup Voice Diagnostics Management Logout

**WAN Setup**

**NAT**

Virtual Servers

**Port Triggering**

DMZ Host

IP Address Map

ALG/Pass-Through

**LAN**

Wireless

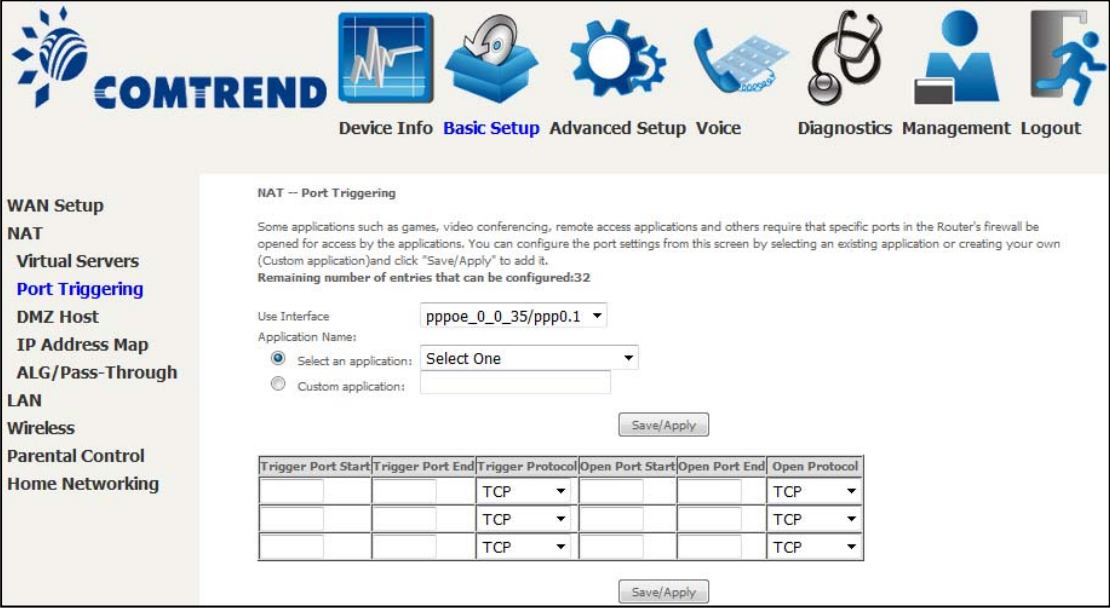
**NAT -- Port Triggering Setup**

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 Voice Diagnostics Management Logout

**WAN Setup**

**NAT**

Virtual Servers

**Port Triggering**

DMZ Host

IP Address Map

ALG/Pass-Through

**LAN**

Wireless

Parental Control

Home Networking

**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: pppoe\_0\_0\_35/ppp0.1

Application Name: Select One

☒ 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           |

Save/Apply

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

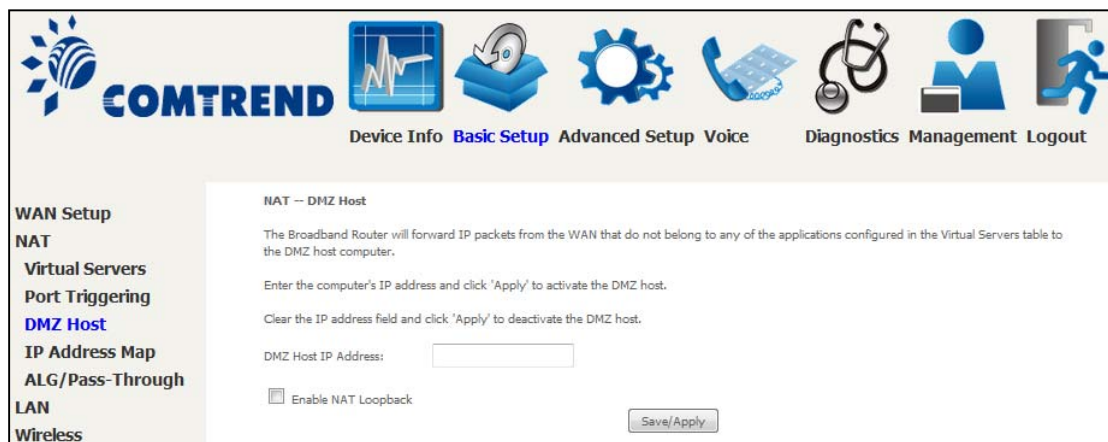
Consult the table below for field and header descriptions.

| Field / Header | Description                                     |
|----------------|-------------------------------------------------|
| Use Interface  | Select a WAN interface from the drop-down menu. |

| Field / Header                                           | Description                                                                                                                                                 |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select an Application<br><b>Or</b><br>Custom Application | User should select the application from the list.<br><b>Or</b><br>User can enter the name of their choice.                                                  |
| Trigger Port Start                                       | Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured. |
| Trigger Port End                                         | Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.   |
| Trigger Protocol                                         | TCP, TCP/UDP, or UDP.                                                                                                                                       |
| Open Port Start                                          | Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.    |
| Open Port End                                            | Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.      |
| Open Protocol                                            | TCP, TCP/UDP, or UDP.                                                                                                                                       |

### 5.2.3 DMZ Host

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



The screenshot shows the COMTREND router's web interface. At the top, there is a navigation bar with icons and labels: Device Info, Basic Setup (highlighted), Advanced Setup, Voice, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options: WAN Setup, NAT (highlighted), Virtual Servers, Port Triggering, DMZ Host (highlighted), IP Address Map, ALG/Pass-Through, LAN, and Wireless. The main content area is titled "NAT -- DMZ Host". It contains the following text: "The Broadband 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." Below this, it says: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." There is a text input field labeled "DMZ Host IP Address:". Below the input field, there is a checkbox labeled "Enable NAT Loopback". At the bottom right of the main content area, there is a "Save/Apply" button.

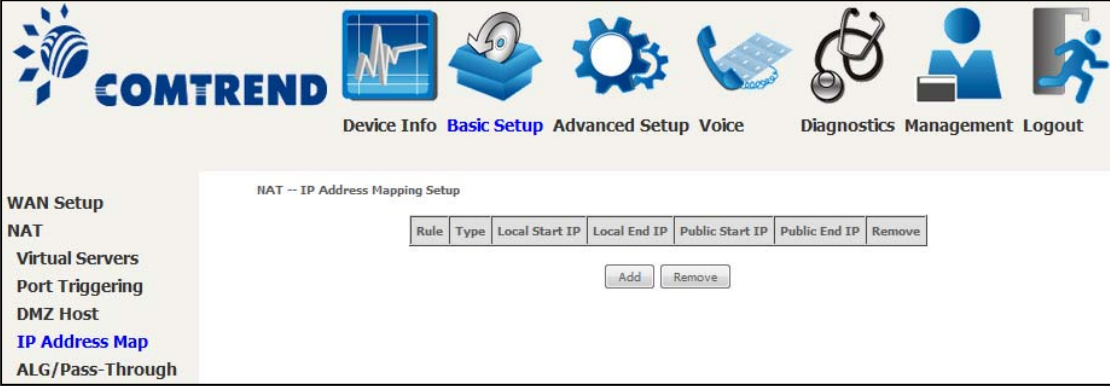
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save / Apply**.

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

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

## 5.2.4 IP Address Map

Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).



| Field / Header  | Description                       |
|-----------------|-----------------------------------|
| Rule            | The number of the rule            |
| Type            | Mapping type from local to public |
| Local Start IP  | The beginning of the local IP     |
| Local End IP    | The ending of the local IP        |
| Public Start IP | The beginning of the public IP    |
| Public End IP   | The ending of the public IP       |
| Remove          | Remove this rule                  |

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



Select a Service, then click the **Save / Apply** button.

**One to One:** mapping one local IP to a specific public IP

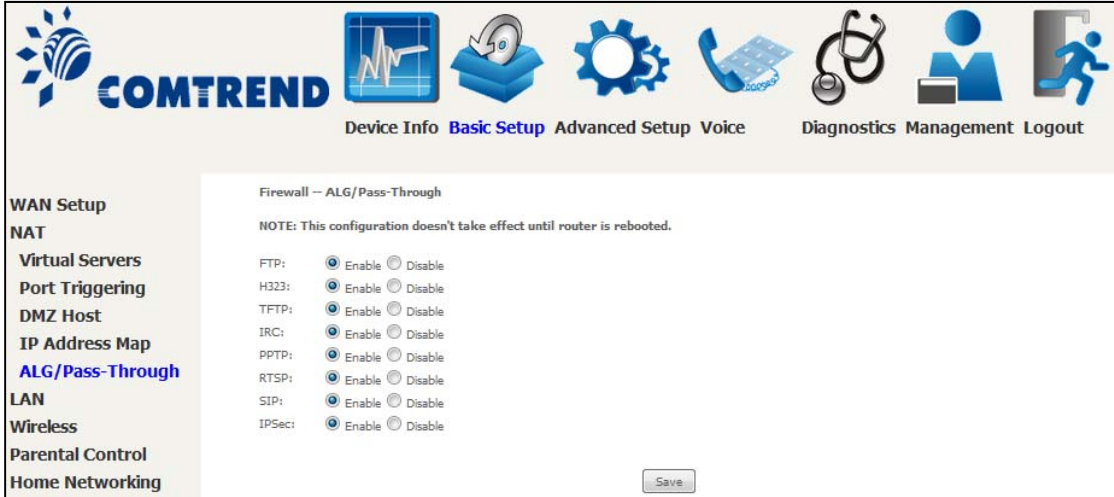
**Many to one:** mapping a range of local IP to a specific public IP

**Many to many(Overload):** mapping a range of local IP to a different range of public IP

**Many to many(No Overload):** mapping a range of local IP to a same range of public IP

### 5.2.5 ALG/Pass-Through

Support ALG Pass-through for the listed protocols.



The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup (selected), Advanced Setup, Voice, Diagnostics, Management, and Logout. The left sidebar lists various configuration sections: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, ALG/Pass-Through (selected), LAN, Wireless, Parental Control, and Home Networking. The main content area is titled "Firewall - ALG/Pass-Through" and contains a note: "NOTE: This configuration doesn't take effect until router is rebooted." Below the note, there is a list of protocols with radio buttons for "Enable" and "Disable":

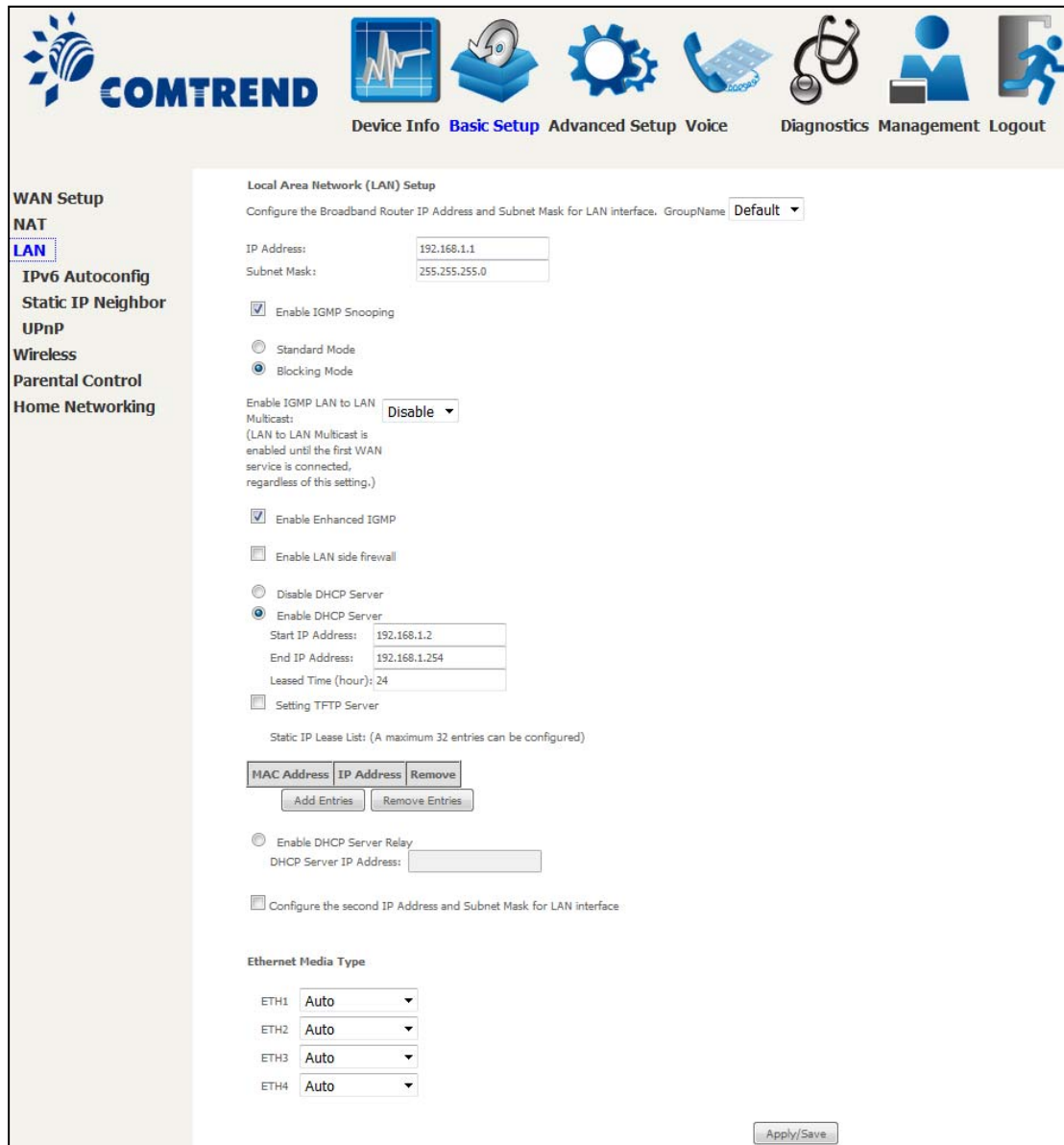
| Protocol | Enable                           | Disable               |
|----------|----------------------------------|-----------------------|
| FTP:     | <input checked="" type="radio"/> | <input type="radio"/> |
| H323:    | <input checked="" type="radio"/> | <input type="radio"/> |
| TFTP:    | <input checked="" type="radio"/> | <input type="radio"/> |
| IRC:     | <input checked="" type="radio"/> | <input type="radio"/> |
| PPTP:    | <input checked="" type="radio"/> | <input type="radio"/> |
| RTSP:    | <input checked="" type="radio"/> | <input type="radio"/> |
| SIP:     | <input checked="" type="radio"/> | <input type="radio"/> |
| IPSec:   | <input checked="" type="radio"/> | <input type="radio"/> |

A "Save" button is located at the bottom right of the configuration area.

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 screenshot shows the COMTREND web interface with the following elements:

- Top Navigation Bar:** Includes the COMTREND logo and icons for Device Info, Basic Setup (selected), Advanced Setup, Voice, Diagnostics, Management, and Logout.
- Left Sidebar:** Contains a menu with options: WAN Setup, NAT, LAN (selected), IPv6 Autoconfig, Static IP Neighbor, UPnP, Wireless, Parental Control, and Home Networking.
- Main Content Area:**
  - Local Area Network (LAN) Setup:** The main heading for the configuration page.
  - GroupName:** A dropdown menu set to "Default".
  - IP Address:** A text field containing "192.168.1.1".
  - Subnet Mask:** A text field containing "255.255.255.0".
  - Enable IGMP Snooping:** A checked checkbox.
  - Standard Mode / Blocking Mode:** Radio buttons, with "Blocking Mode" selected.
  - Enable IGMP LAN to LAN Multicast:** A dropdown menu set to "Disable". Below it, a note states: "(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)"
  - Enable Enhanced IGMP:** A checked checkbox.
  - Enable LAN side firewall:** An unchecked checkbox.
  - Disable DHCP Server / Enable DHCP Server:** Radio buttons, with "Enable DHCP Server" selected.
  - Start IP Address:** A text field containing "192.168.1.2".
  - End IP Address:** A text field containing "192.168.1.254".
  - Leased Time (hour):** A text field containing "24".
  - Setting TFTP Server:** An unchecked checkbox.
  - Static IP Lease List:** A note stating "(A maximum 32 entries can be configured)". Below it is a table with columns "MAC Address", "IP Address", and "Remove". There are "Add Entries" and "Remove Entries" buttons below the table.
  - Enable DHCP Server Relay:** An unchecked radio button. Below it is a text field for "DHCP Server IP Address".
  - Configure the second IP Address and Subnet Mask for LAN interface:** An unchecked checkbox.
  - Ethernet Media Type:** Four dropdown menus labeled ETH1, ETH2, ETH3, and ETH4, all set to "Auto".
  - Apply/Save:** A button at the bottom right of the configuration area.

Consult the field descriptions below for more details.

**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:

**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 Enhanced IGMP:** Enable by ticking the checkbox ☒. IGMP packets between LAN ports will be blocked.

**Enable LAN side firewall:** Enable by ticking the checkbox ☒.

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

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

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

| MAC Address | IP Address | Remove         |
|-------------|------------|----------------|
| Add Entries |            | Remove Entries |

To add an entry, enter MAC address and Static IP address 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.

| MAC Address       | IP Address   | Remove                              |
|-------------------|--------------|-------------------------------------|
| 12:34:56:78:90:12 | 192.168.1.33 | <input checked="" type="checkbox"/> |
| Add Entries       |              | Remove Entries                      |

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

## **2<sup>ND</sup> LAN INTERFACE**

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

|                                     |                                                                   |
|-------------------------------------|-------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | Configure the second IP Address and Subnet Mask for LAN interface |
| IP Address:                         | <input type="text"/>                                              |
| Subnet Mask:                        | <input type="text"/>                                              |

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

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

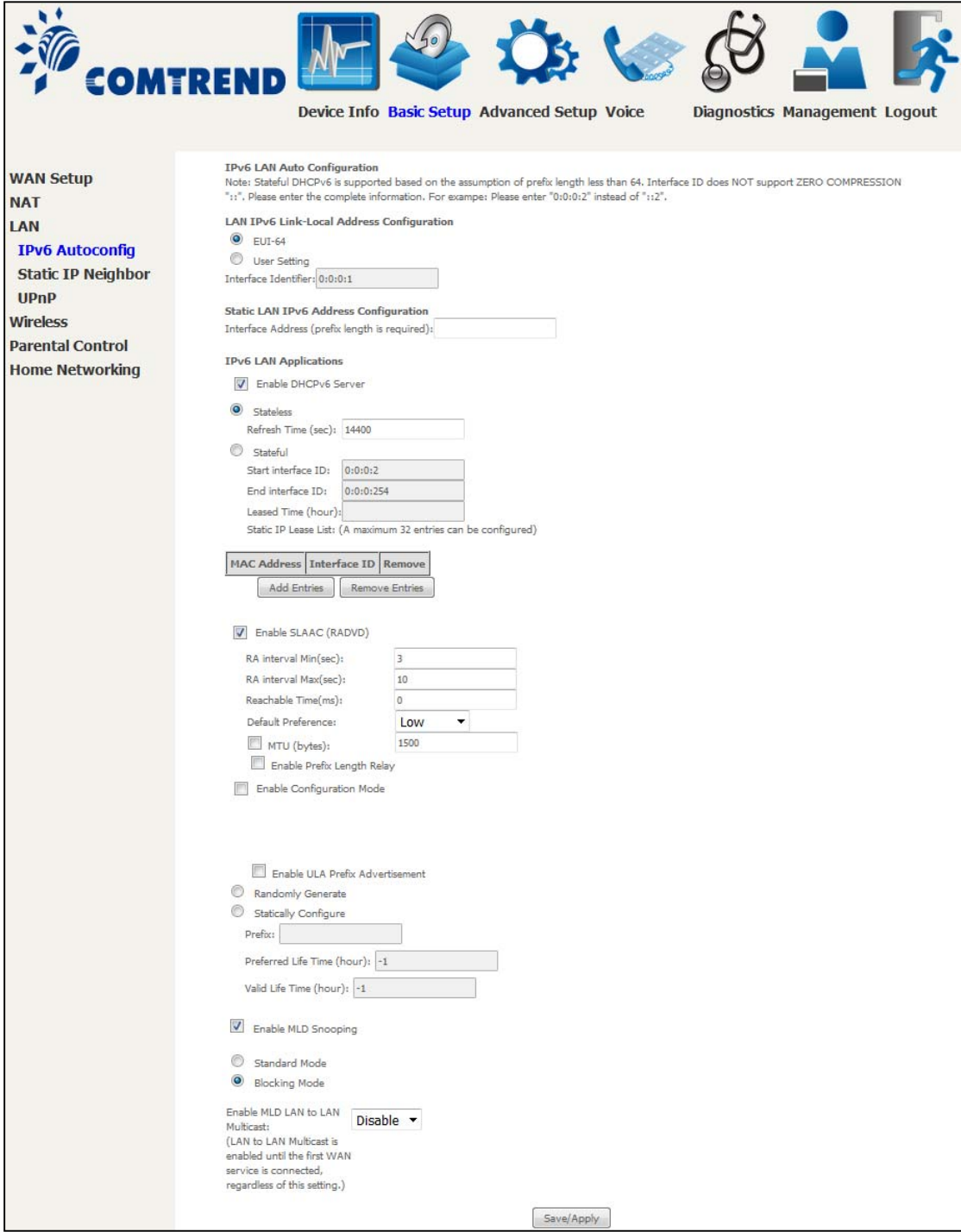
## **Ethernet Media Type:**

Configure auto negotiation, or enforce selected speed and duplex mode for the Ethernet ports.

|      |              |
|------|--------------|
| ETH1 | Auto         |
| ETH2 | Auto         |
| ETH3 | 10Mbps-Half  |
| ETH4 | 10Mbps-Full  |
|      | 100Mbps-Half |
|      | 100Mbps-Full |

### 5.3.1 LAN IPv6 Autoconfig

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



The screenshot shows the COMTREND Basic Setup page for IPv6 LAN Auto Configuration. The left sidebar contains a navigation menu with the following items: WAN Setup, NAT, LAN (selected), IPv6 Autoconfig (highlighted), Static IP Neighbor, UPnP, Wireless, Parental Control, and Home Networking. The main content area is titled "IPv6 LAN Auto Configuration" and includes a note about Stateless DHCPv6 support. The configuration is divided into several sections: "LAN IPv6 Link-Local Address Configuration" with radio buttons for "EUI-64" (selected) and "User Setting", and a text field for "Interface Identifier" set to "0:0:0:1"; "Static LAN IPv6 Address Configuration" with a text field for "Interface Address (prefix length is required)"; "IPv6 LAN Applications" with a checked "Enable DHCPv6 Server" option, radio buttons for "Stateless" (selected) and "Stateful", and fields for "Refresh Time (sec)" (14400), "Start interface ID" (0:0:0:2), "End interface ID" (0:0:0:254), and "Leased Time (hour)"; a table for "Static IP Lease List" with columns for "MAC Address", "Interface ID", and "Remove", and buttons for "Add Entries" and "Remove Entries"; "Enable SLAAC (RADVD)" with a checked option and fields for "RA interval Min(sec)" (3), "RA interval Max(sec)" (10), "Reachable Time(ms)" (0), and a "Default Preference" dropdown set to "Low"; checkboxes for "MTU (bytes)" (1500), "Enable Prefix Length Relay", and "Enable Configuration Mode"; "Enable ULA Prefix Advertisement" with radio buttons for "Randomly Generate" and "Statically Configure", and fields for "Prefix", "Preferred Life Time (hour)" (-1), and "Valid Life Time (hour)" (-1); "Enable MLD Snooping" with a checked option and radio buttons for "Standard Mode" and "Blocking Mode" (selected); and "Enable MLD LAN to LAN Multicast" with a "Disable" dropdown. A "Save/Apply" button is located at the bottom right.

Consult the field descriptions below for more details.

## LAN IPv6 Link-Local Address Configuration

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

## Static LAN IPv6 Address Configuration

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

## IPv6 LAN Applications

| Heading             | Description                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Stateless</b>    | Use stateless configuration                                                                                                     |
| Refresh Time (sec): | The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6 |
| <b>Stateful</b>     | 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                                                                     |

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

|             |            |                |
|-------------|------------|----------------|
| MAC Address | IP Address | Remove         |
| Add Entries |            | Remove Entries |

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

**DHCP Static IP Lease**

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

MAC Address:

Interface ID:

To remove an entry, tick the corresponding checkbox ☒ in the Remove column and

then click the **Remove Entries** button, as shown below.

| MAC Address       | Interface ID | Remove                              |
|-------------------|--------------|-------------------------------------|
| 00:11:22:33:44:55 | 0:0:0:2      | <input checked="" type="checkbox"/> |

| Heading                         | Description                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable RADVD</b>             | Enable use of router advertisement daemon                                                                                                                                                                                                                                                                                          |
| RA interval Min(sec):           | Minimum time to send router advertisement                                                                                                                                                                                                                                                                                          |
| RA interval Max(sec):           | Maximum time to send router advertisement                                                                                                                                                                                                                                                                                          |
| Reachable Time(ms):             | The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation                                                                                                                                                                                                                                   |
| Default Preference:             | Preference level associated with the default router                                                                                                                                                                                                                                                                                |
| MTU (bytes):                    | MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value                                                                                                                                                                                                                          |
| Enable Prefix Length Relay      | Use prefix length receive from WAN interface                                                                                                                                                                                                                                                                                       |
| Enable Configuration Mode       | Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement                                                                                                                                                                                                                       |
| Enable ULA Prefix Advertisement | Allow RADVD to advertise Unique Local Address Prefix                                                                                                                                                                                                                                                                               |
| Randomly Generate               | Use a Randomly Generated Prefix                                                                                                                                                                                                                                                                                                    |
| Statically Configure Prefix     | Specify the prefix to be used                                                                                                                                                                                                                                                                                                      |
| Preferred Life Time (hour)      | The preferred life time for this prefix                                                                                                                                                                                                                                                                                            |
| Valid Life Time (hour)          | The valid life time for this prefix                                                                                                                                                                                                                                                                                                |
| Enable MLD Snooping             | Enable/disable IPv6 multicast forward to LAN ports                                                                                                                                                                                                                                                                                 |
| Standard Mode<br>Blocking Mode  | <p>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</p> <p>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</p> |
| Enable MLD LAN To LAN Multicast | Enable/disable IPv6 multicast between LAN ports                                                                                                                                                                                                                                                                                    |

### 5.3.2 Static IP Neighbor

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



COMTREND

Device Info Basic Setup Advanced Setup Voice Diagnostics Management Logout

WAN Setup  
NAT  
LAN  
IPv6 Autoconfig  
**Static IP Neighbor**

Static ARP/IP Neighbor Configuration

Note: Using the same IP but different MAC for editing an exist record.

| IP Version              | IP Address | MAC Address | Interface | Remove |
|-------------------------|------------|-------------|-----------|--------|
| <div> Add Remove </div> |            |             |           |        |

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



COMTREND

Device Info Basic Setup Advanced Setup Voice Diagnostics Management Logout

WAN Setup  
NAT  
LAN  
IPv6 Autoconfig  
**Static IP Neighbor**  
UPnP  
Wireless

Static IP Neighbor Configuration

IP Version: IPv4

IP Address:

MAC Address:

Associated Interface: LAN/br0

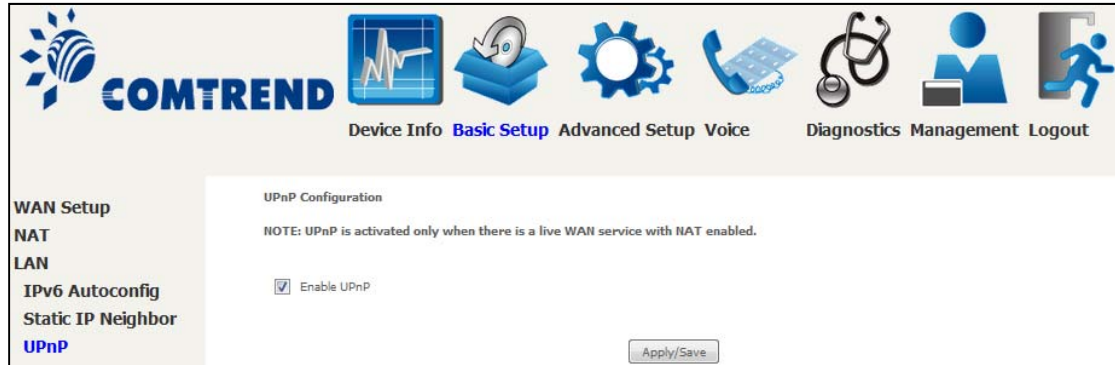
Apply/Save

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

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

### 5.3.3 UPnP

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



COMTREND

Device Info Basic Setup Advanced Setup Voice Diagnostics Management Logout

WAN Setup  
NAT  
LAN  
IPv6 Autoconfig  
Static IP Neighbor  
UPnP

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

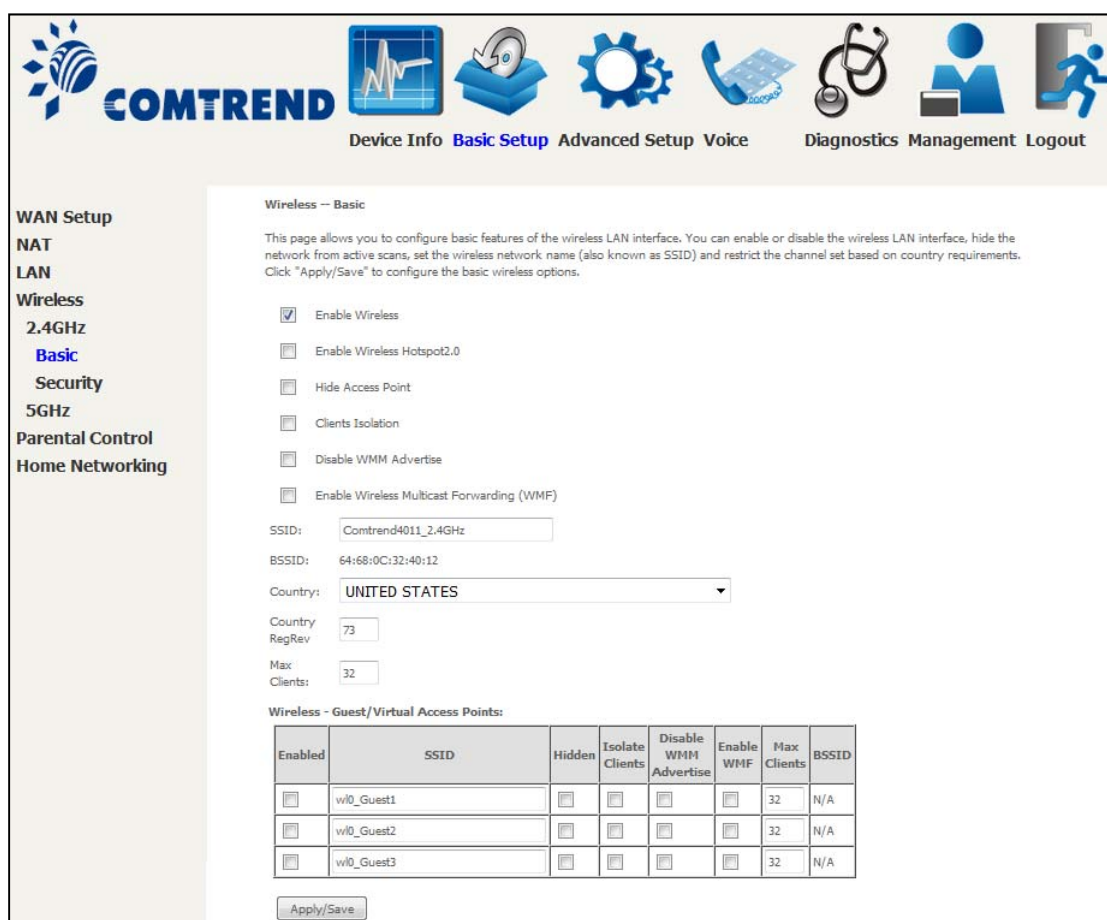
☒ Enable UPnP

Apply/Save

## 5.4 Wireless

### 5.4.1 Basic 2.4GHz

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



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

**WAN Setup**  
**NAT**  
**LAN**  
**Wireless**  
 2.4GHz  
**Basic**  
 Security  
 5GHz  
 Parental Control  
 Home Networking

**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable Wireless

☐ Enable Wireless Hotspot2.0

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☐ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Country RegRev:

Max Clients:

**Wireless - Guest/Virtual Access Points:**

| Enabled                  | SSID       | Hidden                   | Isolate Clients          | Disable WMM Advertise    | Enable WMF               | Max Clients | BSSID |
|--------------------------|------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------|-------|
| <input type="checkbox"/> | wl0_Guest1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 32          | N/A   |
| <input type="checkbox"/> | wl0_Guest2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 32          | N/A   |
| <input type="checkbox"/> | wl0_Guest3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 32          | N/A   |

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

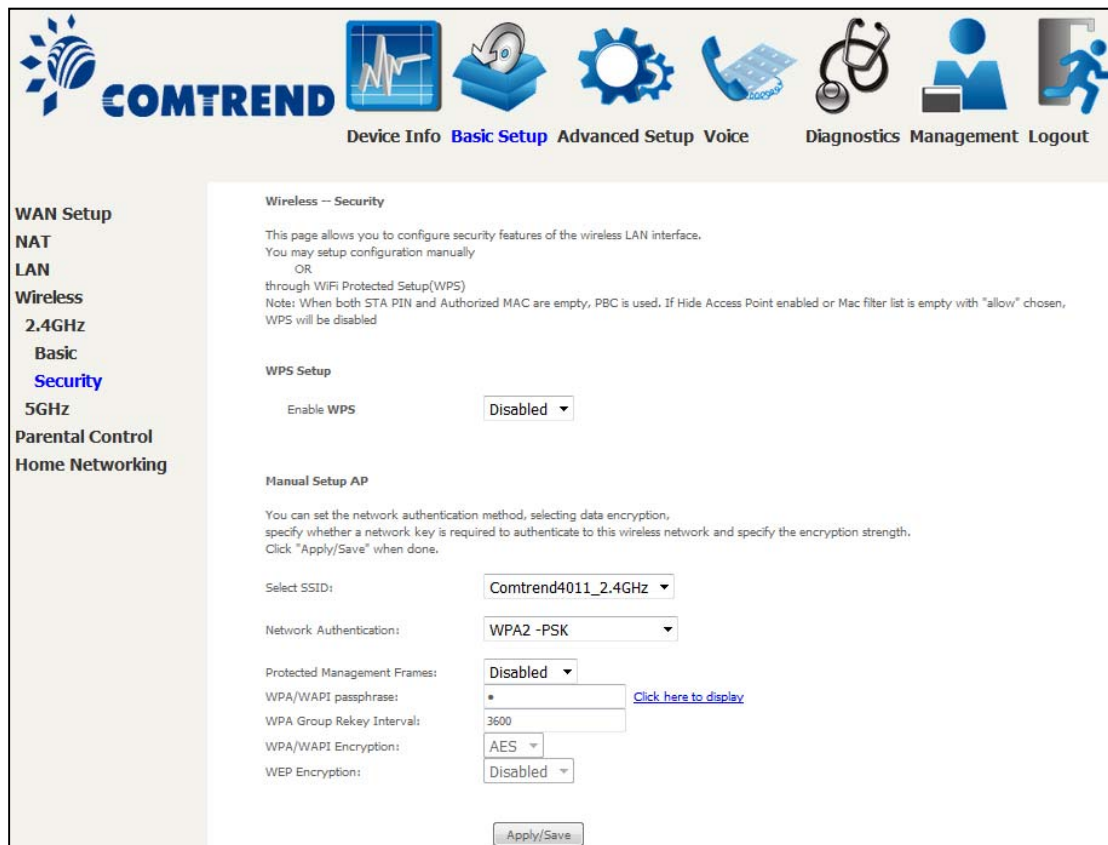
Consult the table below for descriptions of these options.

| Option                     | Description                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Wireless            | A checkbox <input checked="" type="checkbox"/> that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear. |
| Enable Wireless Hotspot2.0 | Enable Wireless Hotspot 2.0 (Wi-Fi Certified Passpoint) on the wireless interface.                                                                              |

| Option                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hide Access Point                        | Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open <b>Network Connections</b> from the <b>start</b> Menu and select <b>View Available Network Connections</b> . If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.                                                                                                                                                                                                                                                                                  |
| Clients Isolation                        | When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Disable WMM Advertise                    | Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Enable Wireless Multicast Forwarding     | Select the checkbox <input checked="" type="checkbox"/> to enable this function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SSID<br>[1-32 characters]                | Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| BSSID                                    | The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Country                                  | A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range:<br>US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Country RegRev                           | Wireless country code for transmit power limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Max Clients                              | The maximum number of clients that can access the router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Wireless - Guest / Virtual Access Points | <p>This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes <input checked="" type="checkbox"/> in the <b>Enabled</b> column. To hide a Guest SSID, select its checkbox <input checked="" type="checkbox"/> in the <b>Hidden</b> column.</p> <p>Do the same for <b>Isolate Clients</b> and <b>Disable WMM Advertise</b>. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for <b>Enable WMF</b>, <b>Max Clients</b> and <b>BSSID</b>, consult the matching entries in this table.</p> <p><b>NOTE:</b> Remote wireless hosts cannot scan Guest SSIDs.</p> |

## 5.4.2 Security 2.4GHz

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



Please see [6.13.3](#) for WPS setup instructions.

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

### WIRELESS SECURITY

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

#### Select SSID

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

#### Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

|                           |               |
|---------------------------|---------------|
| Network Authentication:   | 802.1X ▼      |
| RADIUS Server IP Address: | 0.0.0.0       |
| RADIUS Port:              | 1812          |
| RADIUS Key:               |               |
| WEP Encryption:           | Enabled ▼     |
| Encryption Strength:      | 128-bit ▼     |
| Current Network Key:      | 2 ▼           |
| Network Key 1:            | 1234567890123 |
| Network Key 2:            | 1234567890123 |
| Network Key 3:            | 1234567890123 |
| Network Key 4:            | 1234567890123 |

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

The settings for WPA2-PSK authentication are shown next.

|                              |                                         |
|------------------------------|-----------------------------------------|
| Network Authentication:      | WPA2 -PSK ▼                             |
| Protected Management Frames: | Disabled ▼                              |
| WPA/WAPI passphrase:         | • <a href="#">Click here to display</a> |
| WPA Group Rekey Interval:    | 3600                                    |
| WPA/WAPI Encryption:         | AES ▼                                   |
| WEP Encryption:              | Disabled ▼                              |

Apply/Save

### WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

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

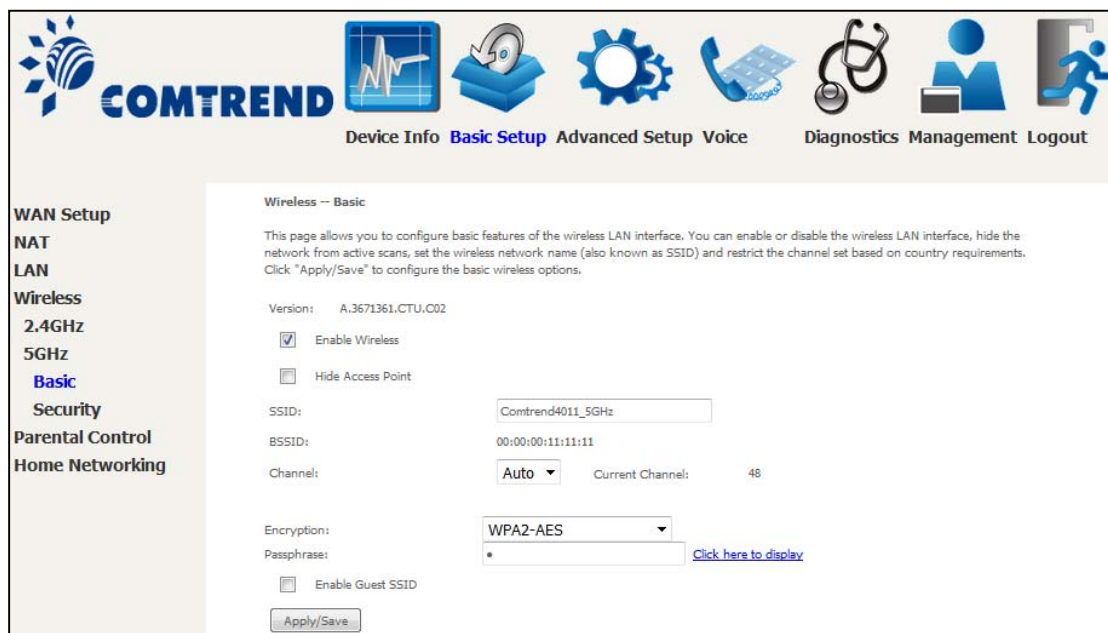
### Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

Please see [6.13](#) for MAC Filter, Wireless Bridge and Advanced Wireless features.

### 5.4.3 Basic 5GHz

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



The screenshot shows the 'Basic Setup' page for the 'Wireless' interface. The left sidebar contains a navigation menu with options: WAN Setup, NAT, LAN, Wireless (selected), 2.4GHz, 5GHz, Basic (selected), Security, Parental Control, and Home Networking. The main content area is titled 'Wireless -- Basic' and contains the following configuration options:

- Version: A.3671361.CTU.C02
- ☒ Enable Wireless
- ☐ Hide Access Point
- SSID: Comtrend4011\_5GHz
- BSSID: 00:00:00:11:11:11
- Channel: Auto (Current Channel: 48)
- Encryption: WPA2-AES
- Passphrase: [masked] [Click here to display](#)
- ☐ Enable Guest SSID
- 

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

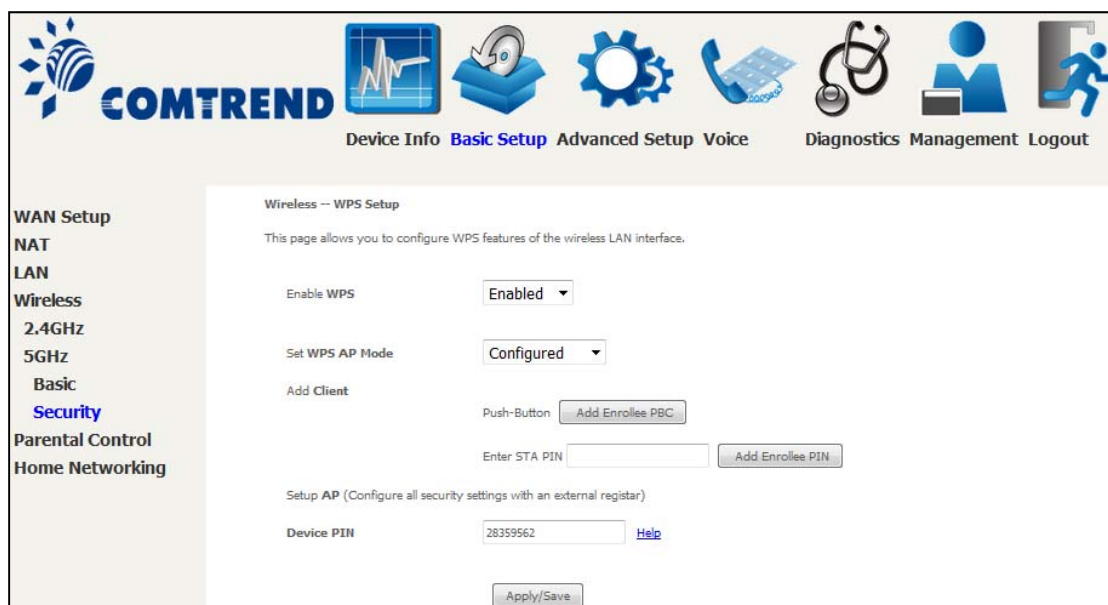
Consult the table below for descriptions of these options.

| Option            | Description                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Wireless   | A checkbox <input checked="" type="checkbox"/> that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.                                                                                                                                                                                                                                                                           |
| Hide Access Point | Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open <b>Network Connections</b> from the <b>start</b> Menu and select <b>View Available Network Connections</b> . If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration. |

| Option                    | Description                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID<br>[1-32 characters] | Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.                                                                            |
| BSSID                     | The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly. |
| Channel                   | Drop-down menu that allows selection of a specific channel.                                                                                                                                                                                                                                    |
| Encryption                | The encryption mode used for the wireless LAN interface.                                                                                                                                                                                                                                       |
| Passphrase                | Entering a passphrase of at least 8 digits is required for WPA2 mode and mixed mode wireless encryption.                                                                                                                                                                                       |
| Enable Guest SSID         | Click Enable Guest SSID to enable an additional SSID to provide varied access.                                                                                                                                                                                                                 |

#### 5.4.4 Security 5GHz

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



Please see [6.13.3](#) for WPS setup instructions.

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

Please see [6.13](#) for MAC Filter, Wireless Bridge and Advanced Wireless features.

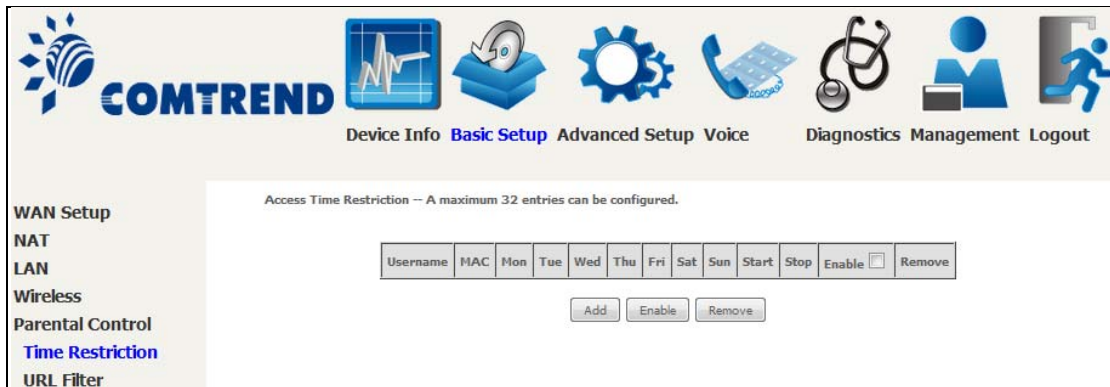
## 5.5 Parental Control

This selection provides WAN access control functionality.

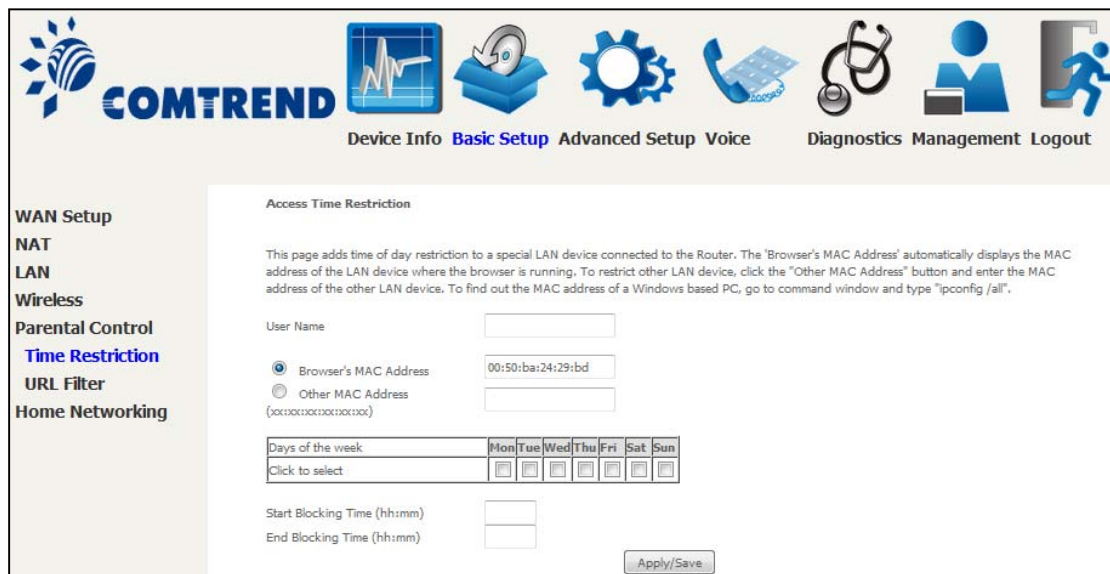
### 5.5.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section [9.5 Internet Time](#), so that the scheduled times match your local time.

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



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



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

**User Name:** A user-defined label for this restriction.

**Browser's MAC Address:** MAC address of the PC running the browser.

**Other MAC Address:** MAC address of another LAN device.

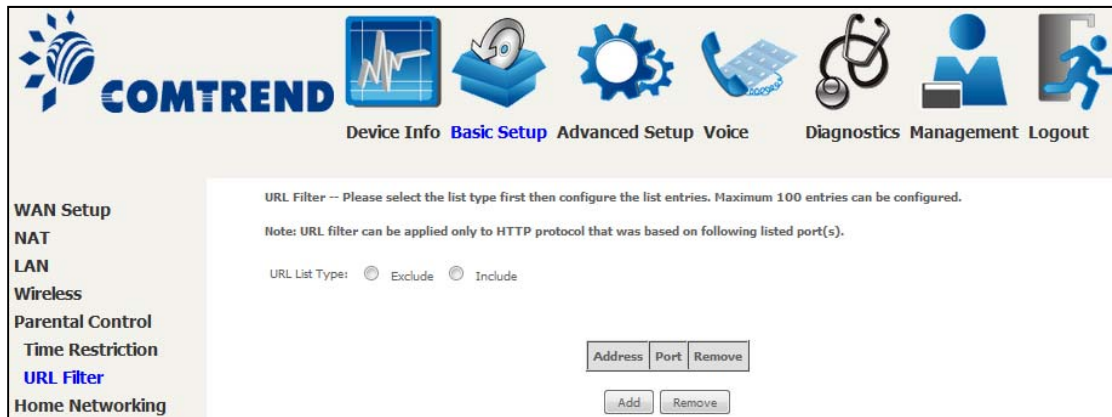
**Days of the Week:** The days the restrictions apply.

**Start Blocking Time:** The time the restrictions start.

**End Blocking Time:** The time the restrictions end.

## 5.5.2 URL Filter

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

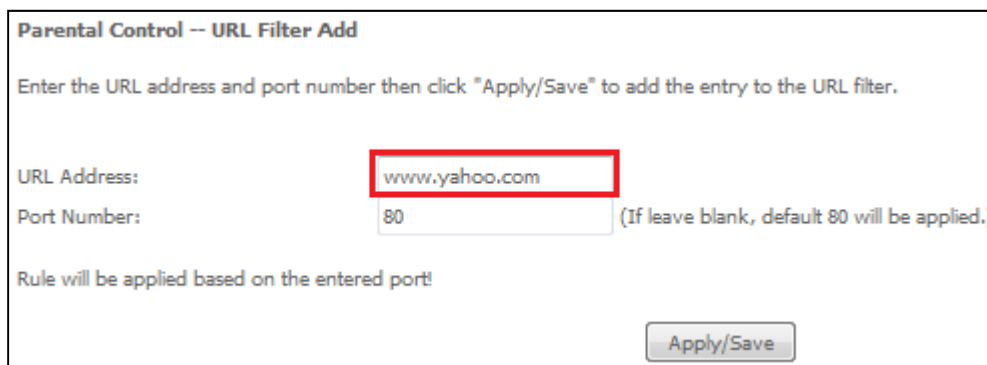


Select URL List Type: Exclude or Include.

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

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

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



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

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

**Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s).**

URL List Type: ☐ Exclude ☒ Include

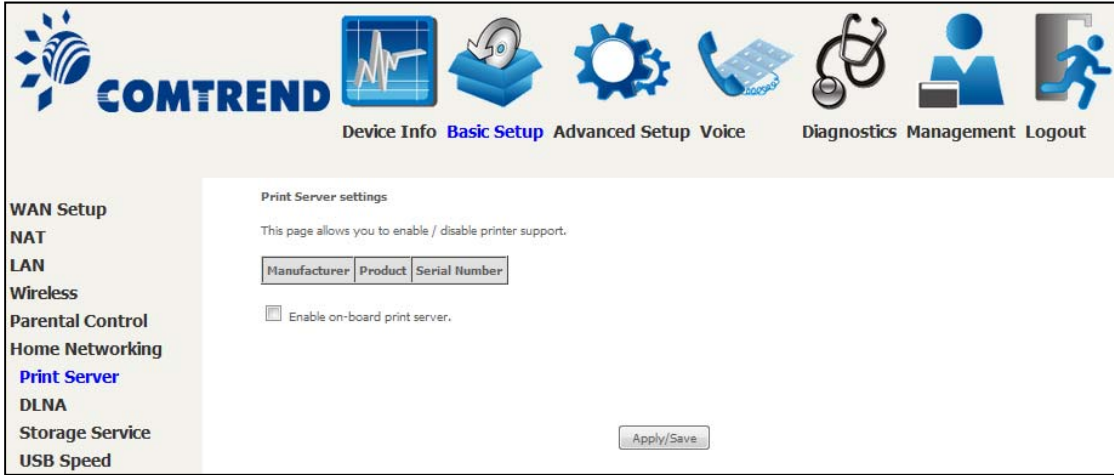
| Address       | Port | Remove                   |
|---------------|------|--------------------------|
| www.yahoo.com | 80   | <input type="checkbox"/> |

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

## 5.6 Home networking

### 5.6.1 Print Server

This page allows you to enable or disable printer support.



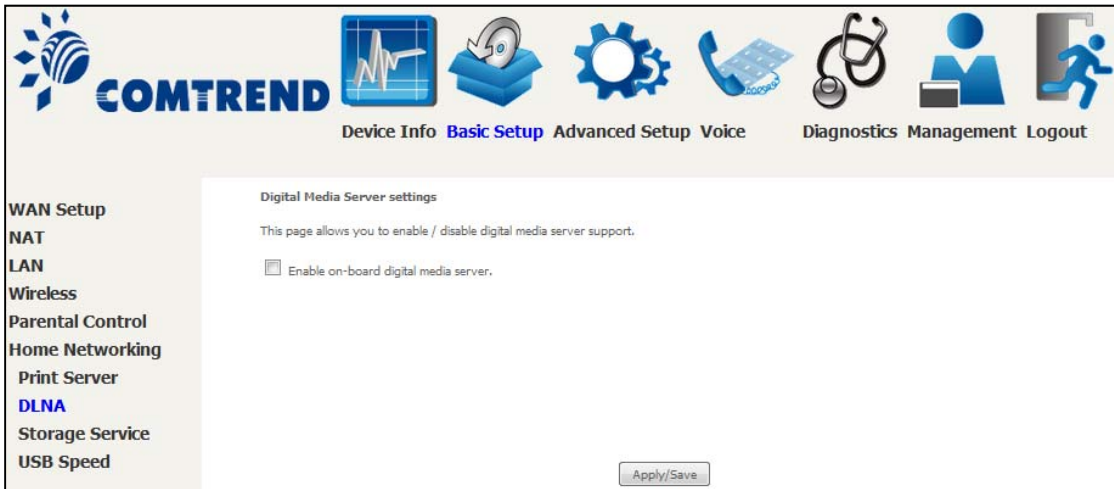
The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup (selected), Advanced Setup, Voice, Diagnostics, Management, and Logout. The left sidebar lists various setup options: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server (selected), DLNA, Storage Service, and USB Speed. The main content area is titled 'Print Server settings' and contains the text: 'This page allows you to enable / disable printer support.' Below this text are three input fields labeled 'Manufacturer', 'Product', and 'Serial Number'. A checkbox labeled 'Enable on-board print server.' is present and unchecked. An 'Apply/Save' button is located at the bottom right of the settings area.

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

### 5.6.2 DLNA

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

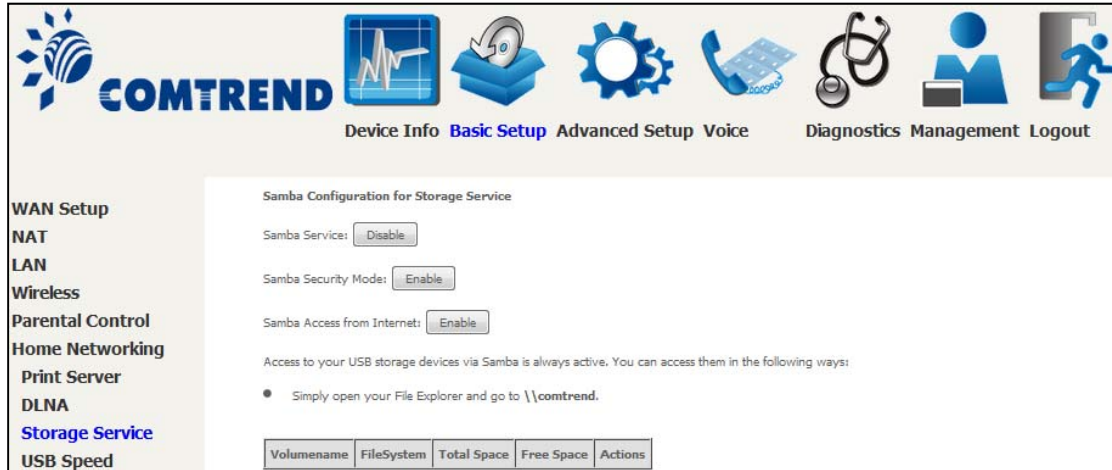
Insert the USB drive into the USB host port on the back of the router. Click Enable on-board digital media server, a dropdown list of directories found on the USB driver will be available for selection. Select media path from the drop-down list or manually modify the media library path and click **Apply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



The screenshot shows the COMTREND web interface. The top navigation bar is identical to the previous screenshot. The left sidebar lists various setup options: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA (selected), Storage Service, and USB Speed. The main content area is titled 'Digital Media Server settings' and contains the text: 'This page allows you to enable / disable digital media server support.' Below this text is a checkbox labeled 'Enable on-board digital media server.' which is unchecked. An 'Apply/Save' button is located at the bottom right of the settings area.

### 5.6.3 Storage Service

Enabling Samba service allows the user to share files on the storage device. Different levels of user access can be configured after samba security mode is enabled. This page also displays storage devices attached to the USB host.



**Samba Configuration for Storage Service**

Samba Service:

Samba Security Mode:

Samba Access from Internet:

Access to your USB storage devices via Samba is always active. You can access them in the following ways:

- Simply open your File Explorer and go to \\comtrend.

| Volumename | FileSystem | Total Space | Free Space | Actions                                      |
|------------|------------|-------------|------------|----------------------------------------------|
| usb1_1     | fat        | 30517 MB    | 1492 MB    | <input type="button" value="Safely remove"/> |

Display after storage device attached (for your reference).

| Volumename | FileSystem | Total Space | Free Space | Actions                                      |
|------------|------------|-------------|------------|----------------------------------------------|
| usb1_1     | fat        | 30517 MB    | 1492 MB    | <input type="button" value="Safely remove"/> |

### 5.6.4 USB Speed

This page allows you to enable / disable USB 3.0 device support.

Note: Enabling USB 3.0 can cause interference with the built-in 2.4GHz wireless radio. It is advised leaving the default value as USB 2.0



## Chapter 6 Advanced Setup

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



### 6.1 Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interfaces. The feature is designed for the scenario that requires only **one WAN service** in different applications.



The Auto Detection page simply provides a checkbox allowing users to enable or disable the feature. Check the checkbox to display the following configuration options.











Device Info
Basic Setup
Advanced Setup
Voice
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

DSL Bonding

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

### Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface when applicable. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.

☒ Enable auto-detect

**Auto-detection status:** Waiting for DSL or Ethernet line connect

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Select a LAN-as-WAN Ethernet port for auto-detect: ETHWAN

Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order. A maximum 7 entries can be configured.

Select Service: ATM

| VPI[0-255]                     | VCI[32-65535]                   | Service        | Option                                                                                                                                   |
|--------------------------------|---------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Disable        | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | Default Bridge |                                                                                                                                          |

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Enter the PPP username/password given by your service provider for PPP service detection.

### Select a LAN-as-WAN Ethernet port for auto-detect:

Select the Ethernet Port that will be used as ETH WAN during auto-detection. For models with ETH WAN port, only ETH WAN port is available to be used as WAN port.

Select Service ATM ▼

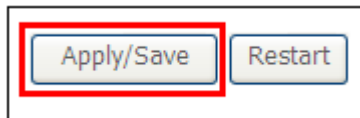
| VPI[0-255] | VCI[32-65535] | Service          |
|------------|---------------|------------------|
| 0          | 32            | Disable ▼        |
| 0          | 32            | PPPoE            |
| 0          | 32            | PPPoA            |
| 0          | 32            | IPoE             |
| 0          | 32            | Disable          |
| 0          | 32            | Disable ▼        |
| 0          | 32            | Disable ▼        |
| 0          | 32            | Disable ▼        |
| 0          | 32            | Disable ▼        |
| 0          | 32            | Default Bridge ▼ |

**WAN services list for ATM mode:** A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement and also reduce the detection cycle.

Select Service PTM/ETHWAN ▼

| VLAN ID[0-4094] | Service          |
|-----------------|------------------|
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Disable ▼        |
| -1              | Default Bridge ▼ |

**WAN services list for PTM mode:** A maximum of 7 WAN services with corresponding VLAN ID (-1 indicates no VLAN ID is required for the service) are required to be configured for ADSL/VDSL PTM mode and ETHWAN. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of the services to meet their own requirements and also reduce the detection cycle.



Click "**Apply / Save**" to activate the auto-detect function.

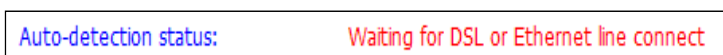
**Options for each WAN service:** These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

| VPI[0-255] | VCI[32-65535] | Service | Option                                                                                                                                                         |
|------------|---------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0          | 32            | PPPoE ▾ | <input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |

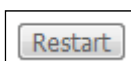
| VLAN ID[0-4094] | Service | Option                                                                                                                                                         |
|-----------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -1              | PPPoE ▾ | <input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |

### Auto Detection status and Restart

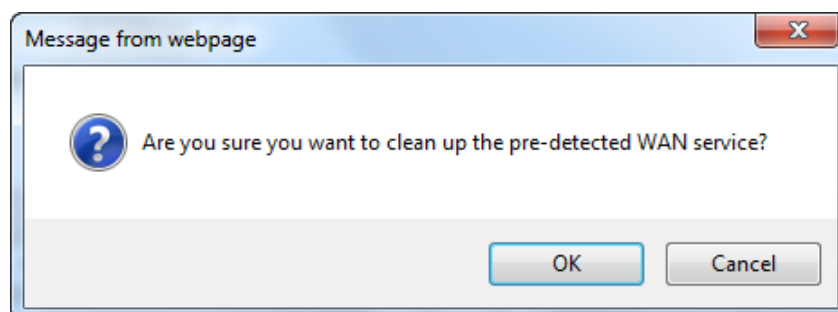
The Auto-detection status is used to display the real time status of the Auto-detection feature.



The **Restart** button is used to detect all the WAN services that are either detected by the auto-detection feature or configured manually by users.



The following window will pop up upon clicking the **Restart** button. Click the **OK** button to proceed.



### **Auto Detection notice**

**Note:** The following description concerning ETHWAN is for multiple LAN port devices only.

- 1) This feature will automatically detect one WAN service only. If customers require multiple WAN services, manual configuration is required.
- 2) If a physical ETHWAN port is detected, the Auto Detection for ETHWAN will be fixed on the physical ETHWAN port and cannot be configured for any LAN port; if the physical ETHWAN port is not detected, the Auto Detection for ETHWAN will be configured to the 4<sup>th</sup> LAN port by default and allows it to be configured for any LAN port as well.
- 3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
- 4) If none of the pre-configured services are detected, a Bridge service will be created.

## 6.2 Security

For detailed descriptions, with examples, please consult [Appendix A - Firewall](#).

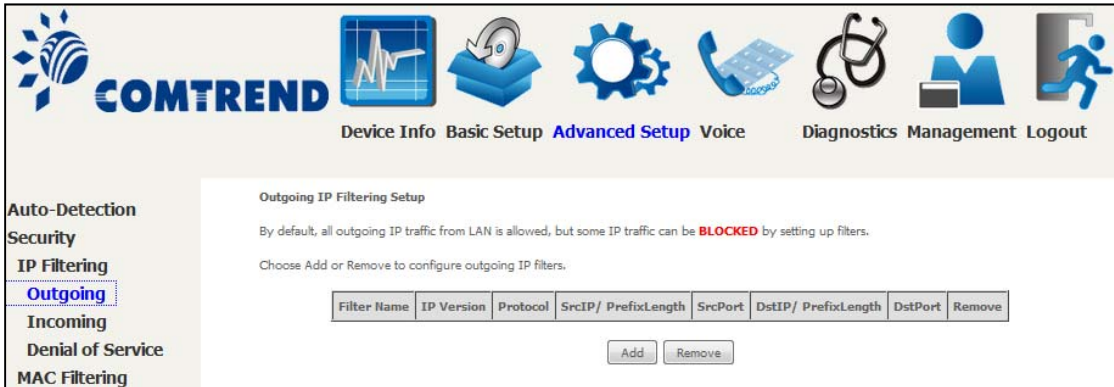
### 6.2.1 IP Filtering

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 bridge mode. Instead, [MAC Filtering](#) performs a similar function.

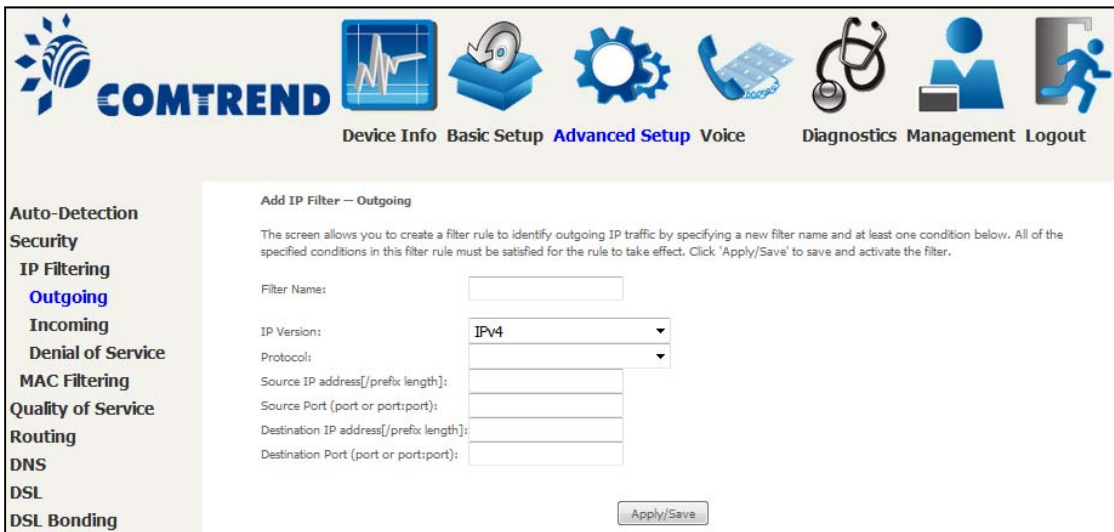
#### OUTGOING IP FILTER

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



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

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

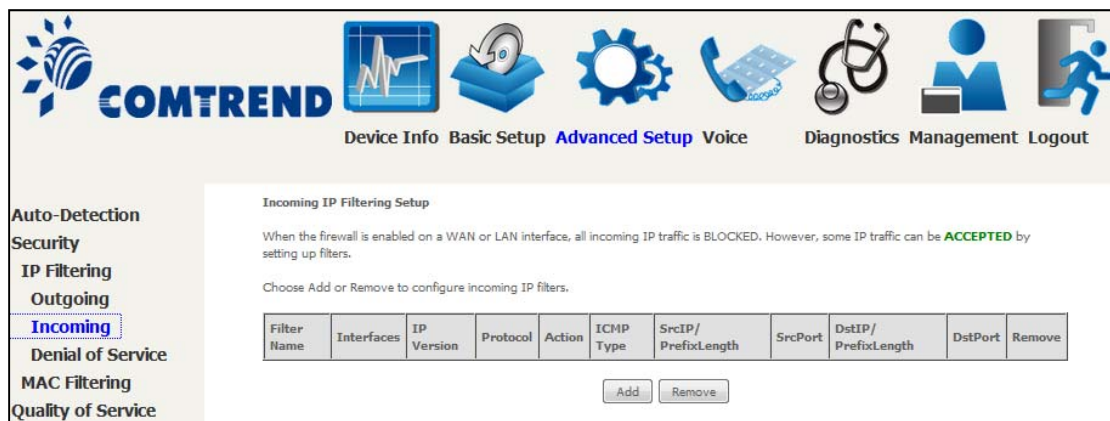


Consult the table below for field descriptions.

| Field                                | Description                             |
|--------------------------------------|-----------------------------------------|
| Filter Name                          | The filter rule label.                  |
| IP Version                           | Select from the drop down menu.         |
| Protocol                             | TCP, TCP/UDP, UDP, or ICMP.             |
| Source IP address                    | Enter source IP address.                |
| Source Port (port or port:port)      | Enter source port number or range.      |
| Destination IP address               | Enter destination IP address.           |
| Destination Port (port or port:port) | Enter destination port number or range. |

## INCOMING IP FILTER

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



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

**Auto-Detection**  
**Security**  
 IP Filtering  
 Outgoing  
**Incoming**  
 Denial of Service  
 MAC Filtering  
 Quality of Service

**Incoming IP Filtering Setup**

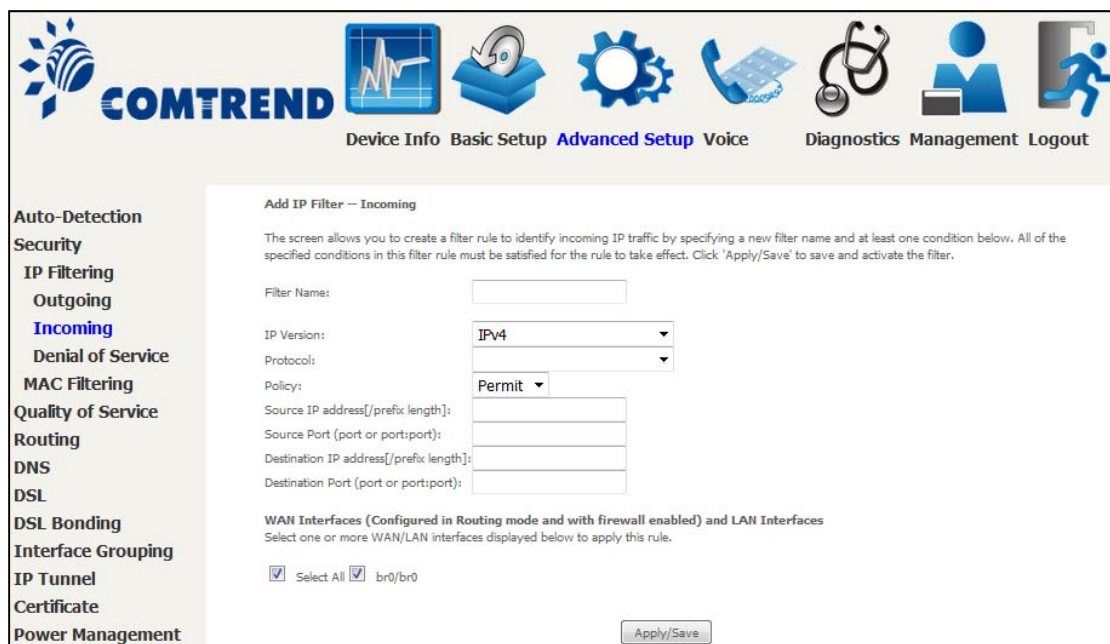
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

| Filter Name                                                                                                       | Interfaces | IP Version | Protocol | Action | ICMP Type | SrcIP/PrefixLength | SrcPort | DstIP/PrefixLength | DstPort | Remove |
|-------------------------------------------------------------------------------------------------------------------|------------|------------|----------|--------|-----------|--------------------|---------|--------------------|---------|--------|
| <div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div> |            |            |          |        |           |                    |         |                    |         |        |

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**.



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

**Auto-Detection**  
**Security**  
 IP Filtering  
 Outgoing  
**Incoming**  
 Denial of Service  
 MAC Filtering  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 DSL Bonding  
 Interface Grouping  
 IP Tunnel  
 Certificate  
 Power Management

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Policy:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**  
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

☒ Select All ☒ br0/br0

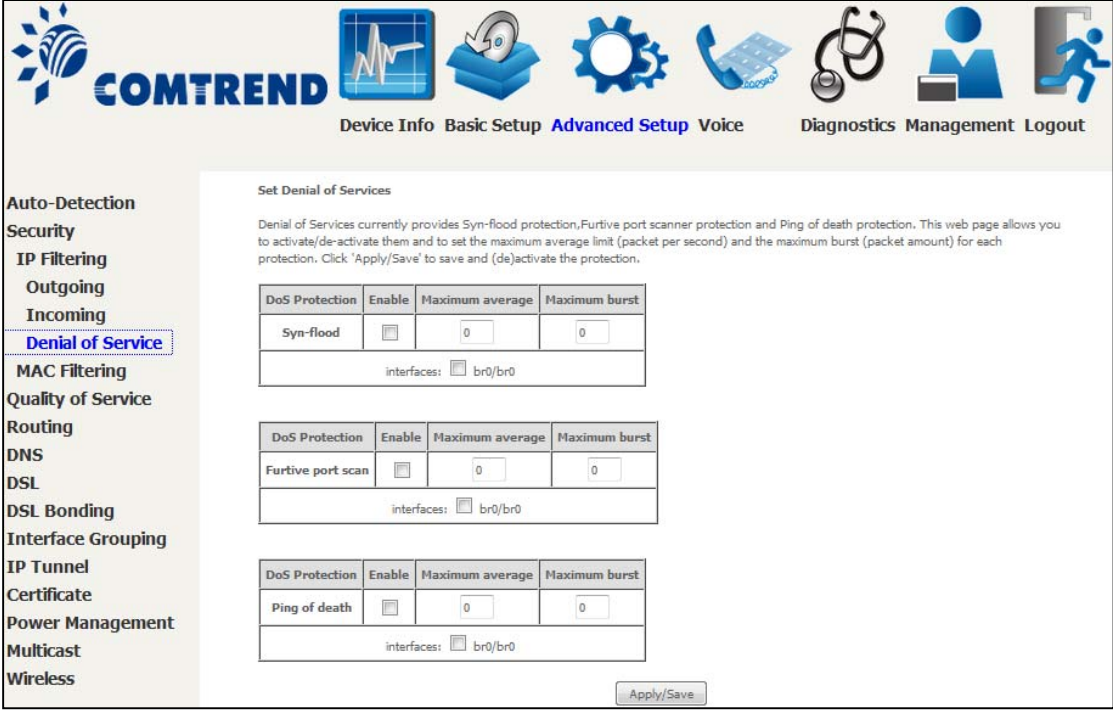
Consult the table below for field descriptions.

| Field                                | Description                                         |
|--------------------------------------|-----------------------------------------------------|
| Filter Name                          | The filter rule label.                              |
| IP Version                           | Select from the drop down menu.                     |
| Protocol                             | TCP, TCP/UDP, UDP, or ICMP.                         |
| Policy                               | Permit/Drop packets specified by the firewall rule. |
| Source IP address                    | Enter source IP address.                            |
| Source Port (port or port:port)      | Enter source port number or range.                  |
| Destination IP address               | Enter destination IP address.                       |
| Destination Port (port or port:port) | Enter destination port number or range.             |

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 bridge mode or without firewall enabled are not available.

## Denial of Service

Denial of Services currently provides Syn-flood protection, furtive port scanner protection and Ping of death protection. This web page allows you to activate/de-activate them and to set the maximum average limit (packet per second) and the maximum burst (packet amount) for each protection.



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

**Auto-Detection**  
**Security**  
 IP Filtering  
 Outgoing  
 Incoming  
**Denial of Service**  
 MAC Filtering  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 DSL Bonding  
 Interface Grouping  
 IP Tunnel  
 Certificate  
 Power Management  
 Multicast  
 Wireless

**Set Denial of Services**

Denial of Services currently provides Syn-flood protection, Furtive port scanner protection and Ping of death protection. This web page allows you to activate/de-activate them and to set the maximum average limit (packet per second) and the maximum burst (packet amount) for each protection. Click 'Apply/Save' to save and (de)activate the protection.

| DoS Protection                               | Enable                   | Maximum average | Maximum burst |
|----------------------------------------------|--------------------------|-----------------|---------------|
| Syn-flood                                    | <input type="checkbox"/> | 0               | 0             |
| interfaces: <input type="checkbox"/> br0/br0 |                          |                 |               |

| DoS Protection                               | Enable                   | Maximum average | Maximum burst |
|----------------------------------------------|--------------------------|-----------------|---------------|
| Furtive port scan                            | <input type="checkbox"/> | 0               | 0             |
| interfaces: <input type="checkbox"/> br0/br0 |                          |                 |               |

| DoS Protection                               | Enable                   | Maximum average | Maximum burst |
|----------------------------------------------|--------------------------|-----------------|---------------|
| Ping of death                                | <input type="checkbox"/> | 0               | 0             |
| interfaces: <input type="checkbox"/> br0/br0 |                          |                 |               |

Apply/Save

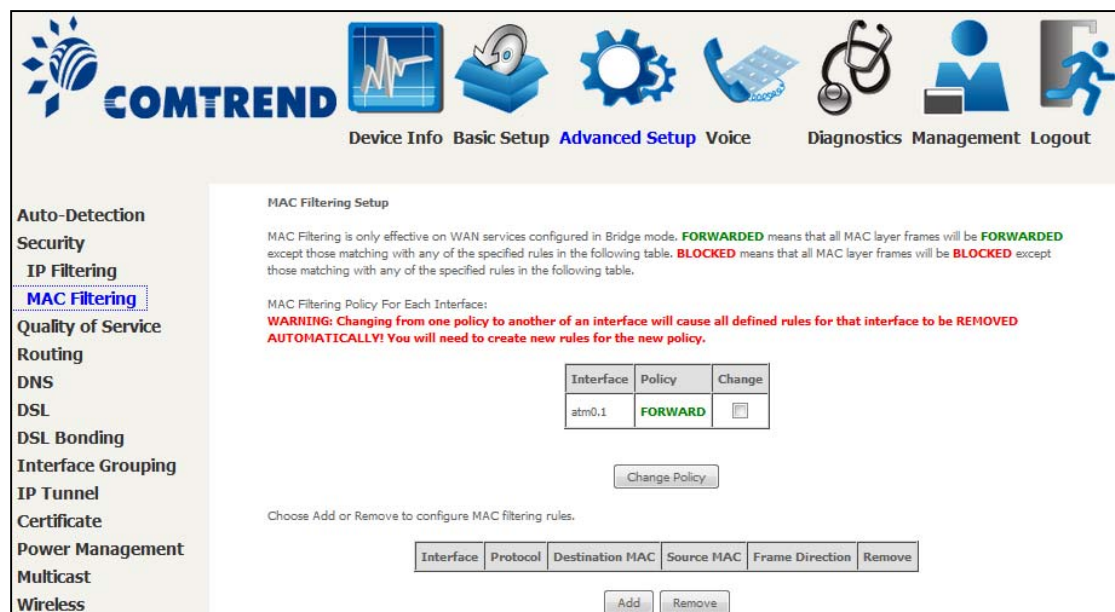
Click the **Apply/Save** button to save and (de)activate the protection.

## 6.2.2 MAC Filtering

**NOTE:** This option is only available in bridge 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 NexusLink 3240 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** Voice Diagnostics Management Logout

Auto-Detection  
Security  
IP Filtering  
**MAC Filtering**  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
Certificate  
Power Management  
Multicast  
Wireless

**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                                |
|-----------|-----------|---------------------------------------|
| atm0.1    | FORWARDED | <input type="button" value="Change"/> |

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.



**COMTREND**

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

Auto-Detection  
Security  
IP Filtering  
**MAC Filtering**  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
Certificate

**Add MAC Filter**

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

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

Consult the table below for detailed field descriptions.

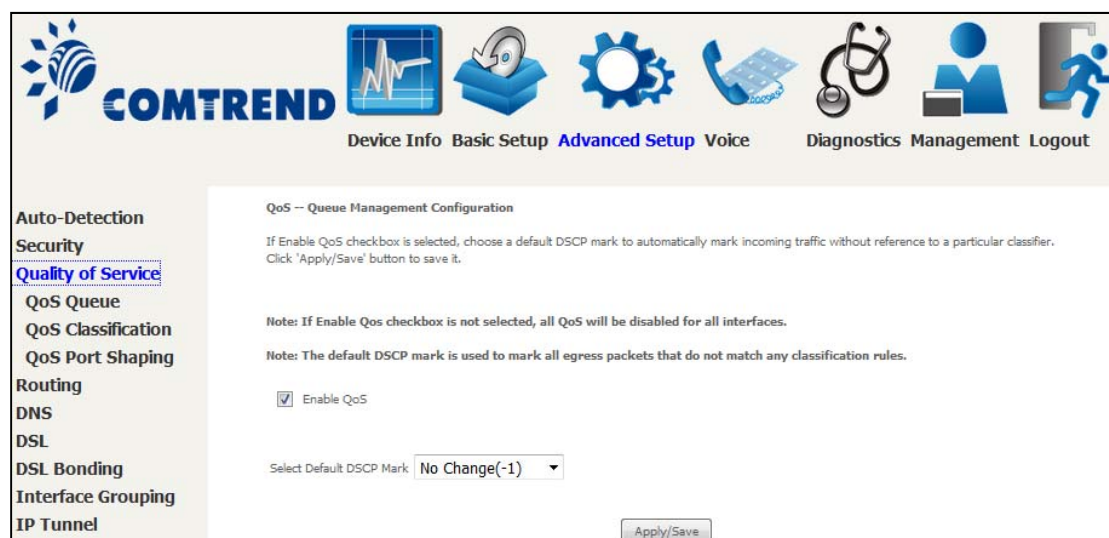
| Field                   | Description                                         |
|-------------------------|-----------------------------------------------------|
| Protocol Type           | PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP    |
| Destination MAC Address | Defines the destination MAC 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 |

## 6.3 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.

### **6.3.1 QoS Queue**

#### **6.3.1.1 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 interface, a maximum of 8 queues can be configured.

(Please see the screen on the following page).











**Auto-Detection**

**Security**

**Quality of Service**

**QoS Queue**

**Queue Configuration**

**Wlan Queue**

**QoS Classification**

**QoS Port Shaping**

**Routing**

**DNS**

**DSL**

**DSL Bonding**

**Interface Grouping**

**IP Tunnel**

**Certificate**

**Power Management**

**Multicast**

**Wireless**

**QoS Queue Setup**

In ATM mode, maximum 16 queues can be configured.  
 In PTM mode, maximum 8 queues can be configured.  
 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 unchecked 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.

| Name   | Key | Interface | Qid | Proc/Alg/Wght | DSL Latency | PTM Priority | Shaping Rate(bps) | Min Bit Rate(bps) | Burst Size(bytes) | Enable                              | Remove                   |
|--------|-----|-----------|-----|---------------|-------------|--------------|-------------------|-------------------|-------------------|-------------------------------------|--------------------------|
| LAN Q8 | 1   | eth1      | 8   | 1/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q7 | 2   | eth1      | 7   | 2/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q6 | 3   | eth1      | 6   | 3/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q5 | 4   | eth1      | 5   | 4/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q4 | 5   | eth1      | 4   | 5/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q3 | 6   | eth1      | 3   | 6/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q2 | 7   | eth1      | 2   | 7/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q1 | 8   | eth1      | 1   | 8/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q8 | 9   | eth2      | 8   | 1/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q7 | 10  | eth2      | 7   | 2/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q6 | 11  | eth2      | 6   | 3/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q5 | 12  | eth2      | 5   | 4/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q4 | 13  | eth2      | 4   | 5/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q3 | 14  | eth2      | 3   | 6/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q2 | 15  | eth2      | 2   | 7/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q1 | 16  | eth2      | 1   | 8/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q8 | 17  | eth3      | 8   | 1/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q7 | 18  | eth3      | 7   | 2/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q6 | 19  | eth3      | 6   | 3/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q5 | 20  | eth3      | 5   | 4/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q4 | 21  | eth3      | 4   | 5/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q3 | 22  | eth3      | 3   | 6/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q2 | 23  | eth3      | 2   | 7/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q1 | 24  | eth3      | 1   | 8/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q8 | 25  | eth4      | 8   | 1/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q7 | 26  | eth4      | 7   | 2/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q6 | 27  | eth4      | 6   | 3/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q5 | 28  | eth4      | 5   | 4/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q4 | 29  | eth4      | 4   | 5/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q3 | 30  | eth4      | 3   | 6/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q2 | 31  | eth4      | 2   | 7/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q1 | 32  | eth4      | 1   | 8/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q8 | 33  | eth5      | 8   | 1/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q7 | 34  | eth5      | 7   | 2/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q6 | 35  | eth5      | 6   | 3/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q5 | 36  | eth5      | 5   | 4/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q4 | 37  | eth5      | 4   | 5/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q3 | 38  | eth5      | 3   | 6/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q2 | 39  | eth5      | 2   | 7/SP          |             |              |                   |                   |                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| LAN Q1 | 40  | eth5      | 1   | 8/SP          |             |              |                   |                   |                   | <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.

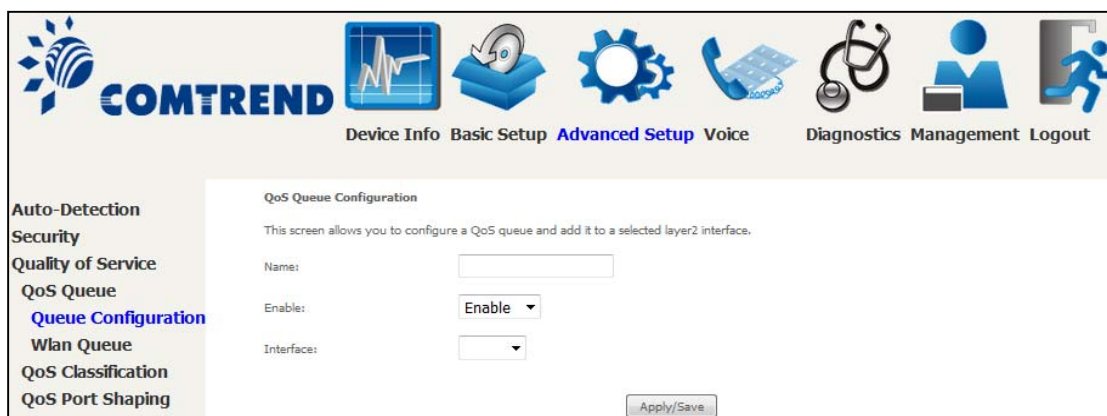
The **Enable** button will scan through every queue in the table. Queues with the enable-checkbox checked will be enabled. Queues with the enable-checkbox un-checked will be disabled.

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. You can create a new Queue entry by clicking the **Add** button.

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

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



The screenshot shows the COMTREND web interface for QoS Queue Configuration. The top navigation bar includes links for Device Info, Basic Setup, Advanced Setup (highlighted), Voice, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories, with 'Queue Configuration' selected under 'Quality of Service'. The main content area is titled 'QoS Queue Configuration' and contains a description: 'This screen allows you to configure a QoS queue and add it to a selected layer2 interface.' Below this, there are three fields: 'Name:' with a text input box, 'Enable:' with a dropdown menu set to 'Enable', and 'Interface:' with a dropdown menu. An 'Apply/Save' button is located at the bottom right of the form.

**Name:** Identifier for this Queue entry.

**Enable:** Enable/Disable the Queue entry.

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

After selecting an Interface the following will be displayed.


**COMTREND**

  
 Device Info

  
 Basic Setup

  
**Advanced Setup**

  
 Voice

  
 Diagnostics

  
 Management

  
 Logout

Auto-Detection  
 Security  
 Quality of Service  
   QoS Queue  
     **Queue Configuration**  
     Wlan Queue  
   QoS Classification  
   QoS Port Shaping  
 Routing  
 DNS  
 DSL  
 DSL Bonding

### QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: Enable ▾

Interface: eth0 ▾

Queue Precedence: 1(SP) ▾ (lower value, higher priority)  

 - The precedence list shows the scheduler algorithm configured at each precedence level.  
 - Note that precedence level with SP scheduler may have only one queue.  
 - precedence level with WRR/WFQ scheduler may have multiple queues.

Shaping Rate: -1 [1-1000000 Kbps] (-1 indicates no shaping)

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.

### 6.3.1.2 Wlan Queue

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











Device Info
Basic Setup
Advanced Setup
Voice
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

QoS Queue

Queue Configuration

Wlan Queue

QoS Classification

QoS Port Shaping

Routing

DNS

DSL

DSL Bonding

Interface Grouping

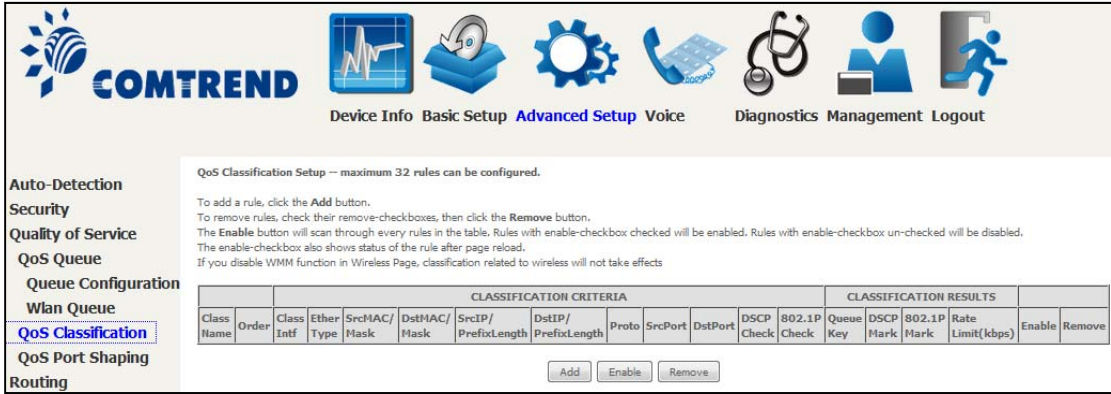
**QoS Wlan Queue Setup**

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

| Name               | Key | Interface | Qid | Prec/Alg/Wght | Enable  |
|--------------------|-----|-----------|-----|---------------|---------|
| WMM Voice Priority | 41  | wl0       | 8   | 1/SP          | Enabled |
| WMM Voice Priority | 42  | wl0       | 7   | 2/SP          | Enabled |
| WMM Video Priority | 43  | wl0       | 6   | 3/SP          | Enabled |
| WMM Video Priority | 44  | wl0       | 5   | 4/SP          | Enabled |
| WMM Best Effort    | 45  | wl0       | 4   | 5/SP          | Enabled |
| WMM Background     | 46  | wl0       | 3   | 6/SP          | Enabled |
| WMM Background     | 47  | wl0       | 2   | 7/SP          | Enabled |
| WMM Best Effort    | 48  | wl0       | 1   | 8/SP          | Enabled |

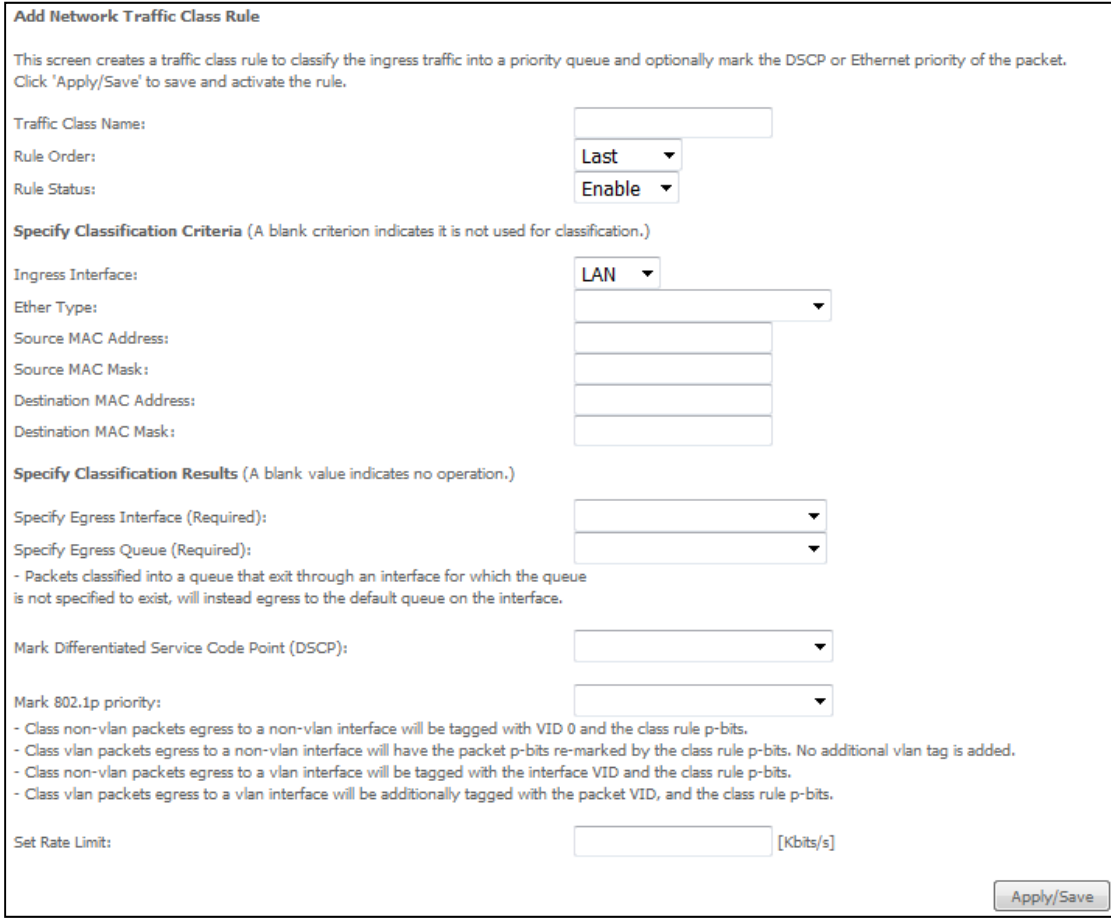
## 6.3.2 QoS Classification

The network traffic classes are listed in the following table.



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

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



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

| Field                                  | 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, wlo)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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.<br>- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.<br>- 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.<br>- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.<br>- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits. |
| Set Rate Limit                         | The data transmission rate limit in kbps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### 6.3.3 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
Voice
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

QoS Queue

Queue Configuration

Wlan Queue

QoS Classification

QoS Port Shaping

Routing

DNS

DSL

DSL Bonding

Interface Grouping

IP Tunnel

Certificate

#### 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 (Kbps) | Burst Size (bytes) |
|-----------|------|---------------------|--------------------|
| eth0      | LAN  | -1                  | 0                  |
| eth1      | LAN  | -1                  | 0                  |
| eth2      | LAN  | -1                  | 0                  |
| eth3      | LAN  | -1                  | 0                  |
| eth4      | LAN  | -1                  | 0                  |
| eth5      | LAN  | -1                  | 0                  |

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

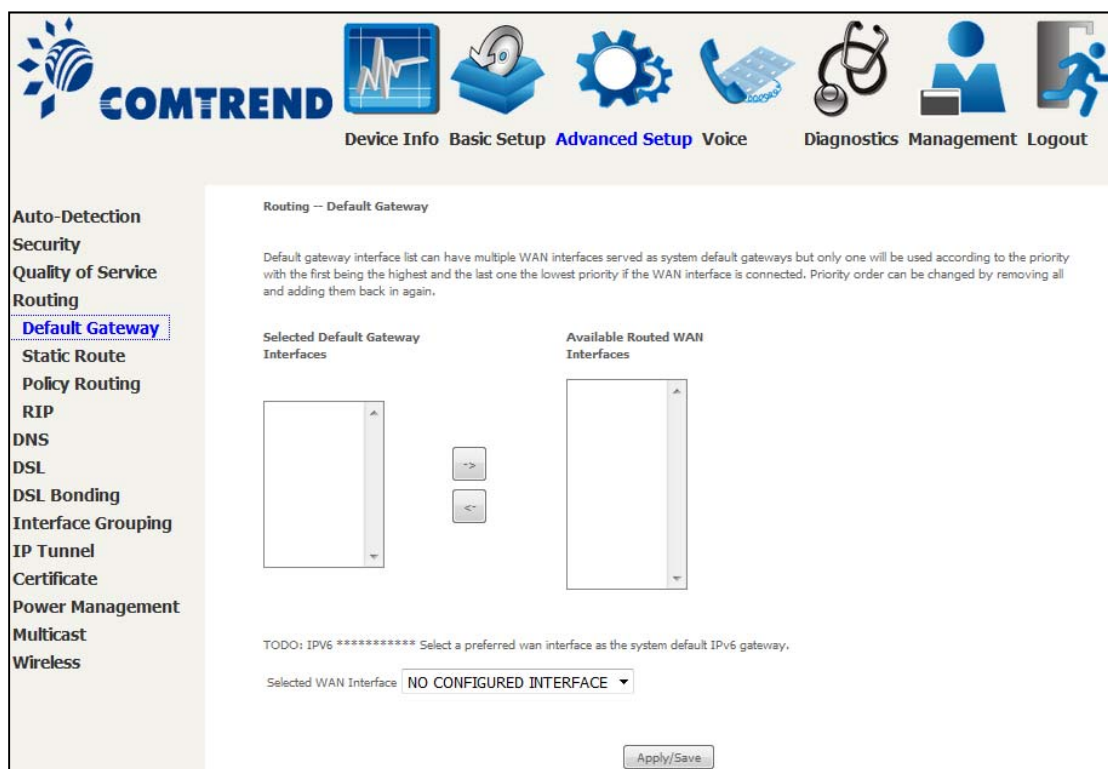
## 6.4 Routing

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

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

### 6.4.1 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.



The screenshot shows the COMTREND web interface. The top navigation bar includes links for Device Info, Basic Setup, **Advanced Setup**, Voice, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories, with **Routing** selected and **Default Gateway** highlighted. The main content area is titled "Routing -- Default Gateway" and contains the following text:

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.

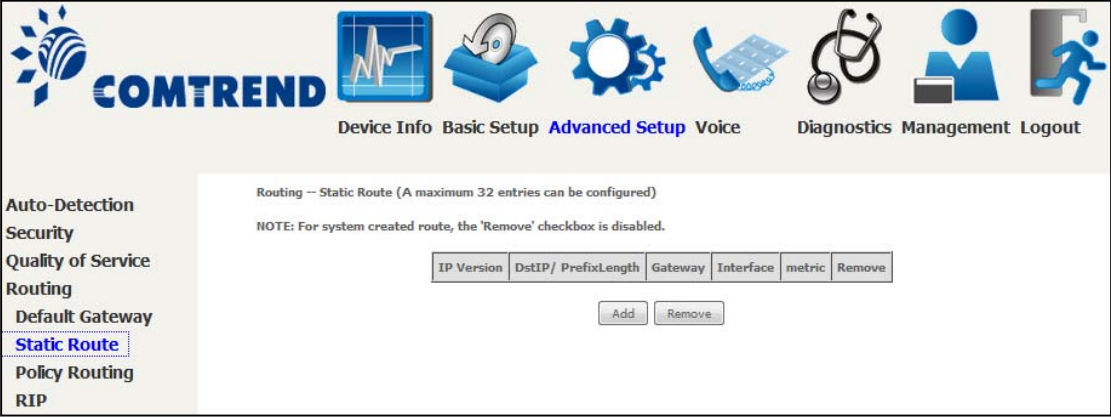
Below this text are two columns: "Selected Default Gateway Interfaces" and "Available Routed WAN Interfaces". Each column contains an empty list box. Between the list boxes are two buttons: ">" and "<".

At the bottom, there is a "TODO: IPV6 \*\*\*\*\* Select a preferred wan interface as the system default IPV6 gateway." message. Below this is a "Selected WAN Interface" dropdown menu currently set to "NO CONFIGURED INTERFACE". An "Apply/Save" button is located at the bottom right of the configuration area.

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

## 6.4.2 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.

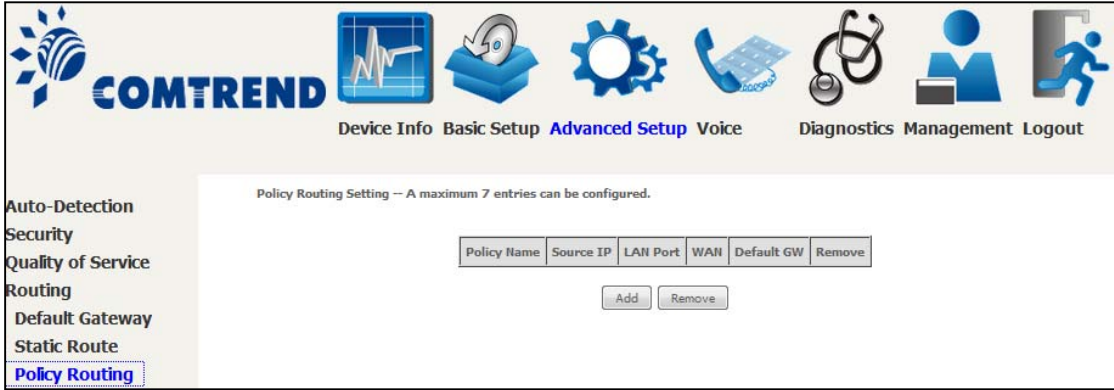


- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** Select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

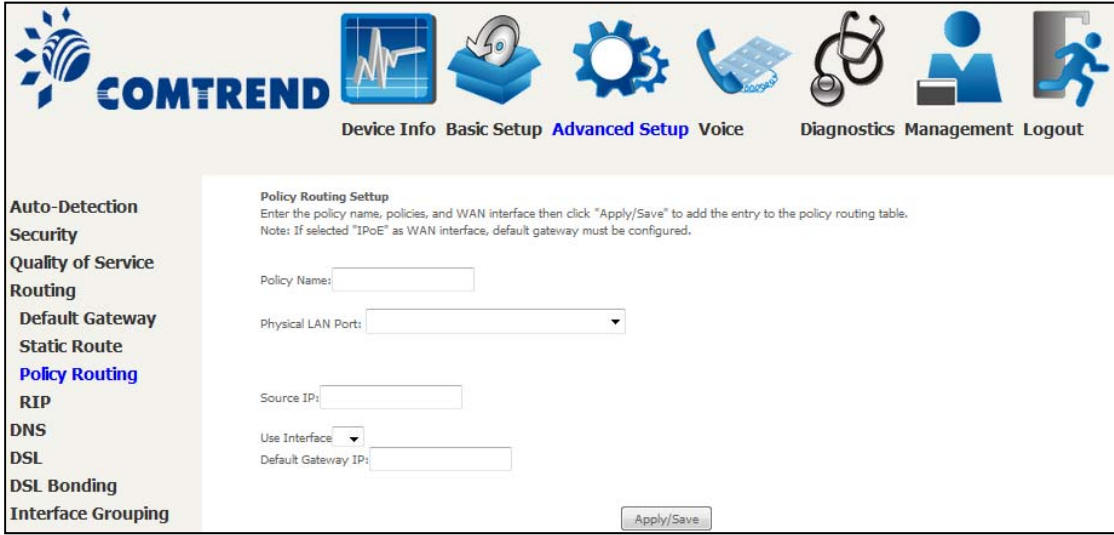
After completing the settings, click **Apply/Save** to add the entry to the routing table.

### 6.4.3 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.



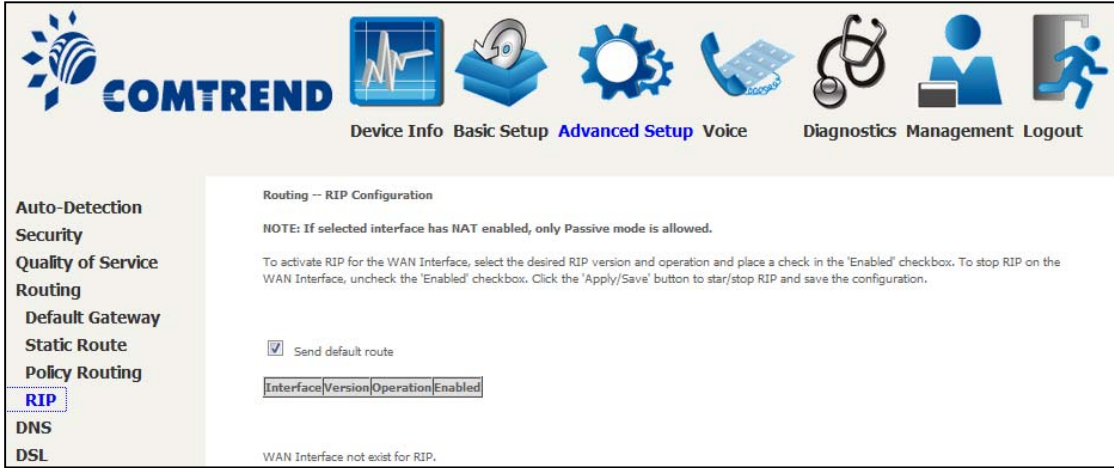
On the following screen, complete the form and click **Apply/Save** to create a policy.



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

## 6.4.4 RIP

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



The screenshot shows the COMTREND web interface. The top navigation bar includes the COMTREND logo and icons for Device Info, Basic Setup, Advanced Setup (highlighted), Voice, Diagnostics, Management, and Logout. The left sidebar lists configuration categories: Auto-Detection, Security, Quality of Service, Routing (selected), Default Gateway, Static Route, Policy Routing, RIP (highlighted), DNS, and DSL. The main content area is titled 'Routing -- RIP Configuration'. It contains a note: 'NOTE: If selected interface has NAT enabled, only Passive mode is allowed.' Below this is a paragraph explaining how to activate RIP. A checkbox labeled 'Send default route' is checked. Below that is a table with headers 'Interface', 'Version', 'Operation', and 'Enabled'. At the bottom, a message states 'WAN Interface not exist for RIP.'

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 star/stop RIP and save the configuration.

☒ Send default route

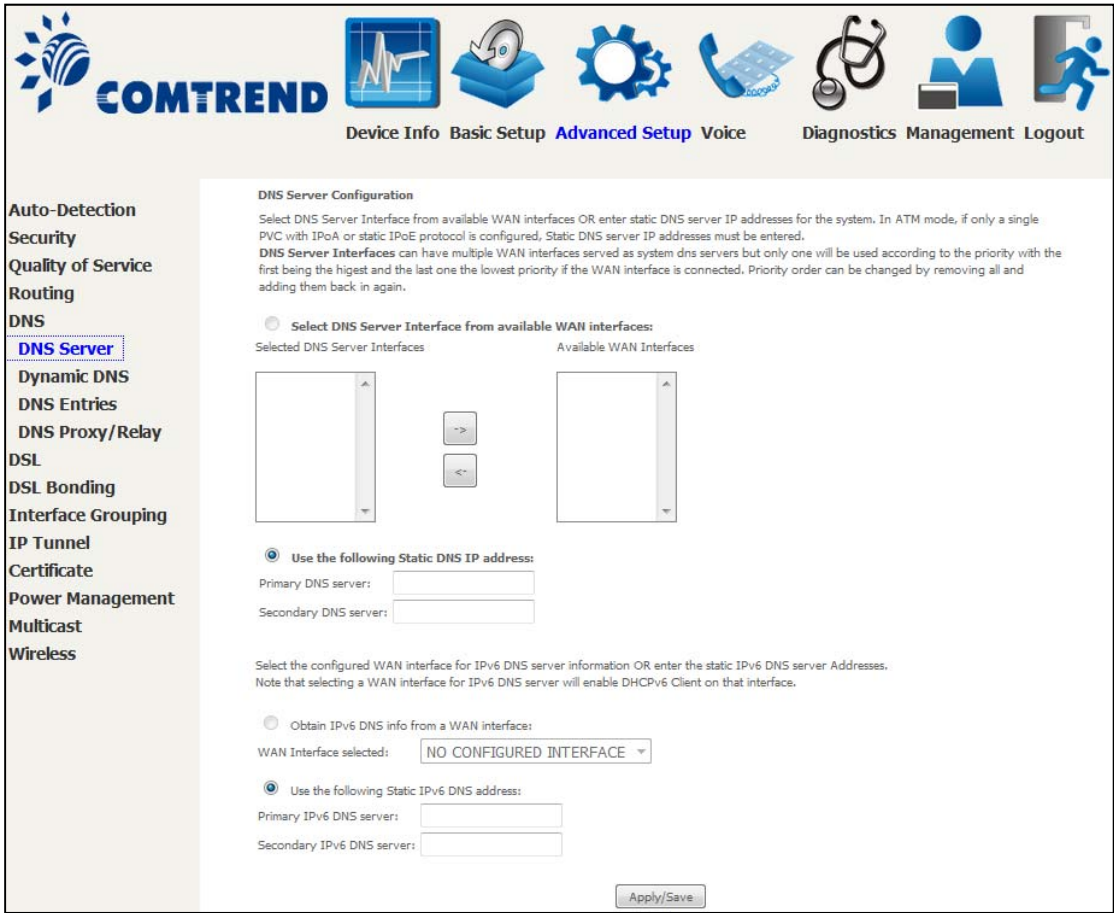
| Interface | Version | Operation | Enabled |
|-----------|---------|-----------|---------|
|           |         |           |         |

WAN Interface not exist for RIP.

## 6.5 DNS

### 6.5.1 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** Voice Diagnostics Management Logout

Auto-Detection  
Security  
Quality of Service  
Routing  
**DNS**  
Dynamic DNS  
DNS Entries  
DNS Proxy/Relay  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
Certificate  
Power Management  
Multicast  
Wireless

### DNS Server Configuration

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.

☐ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

☒ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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:

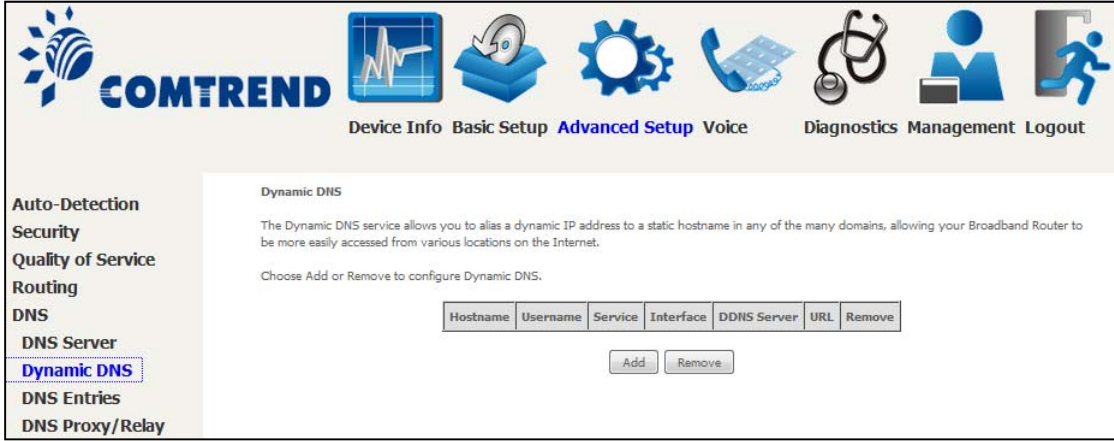
Secondary IPv6 DNS server:

Apply/Save

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

## 6.5.2 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 NexusLink 3240 to be more easily accessed from various locations on the Internet.



**COMTREND**

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

**Dynamic DNS**

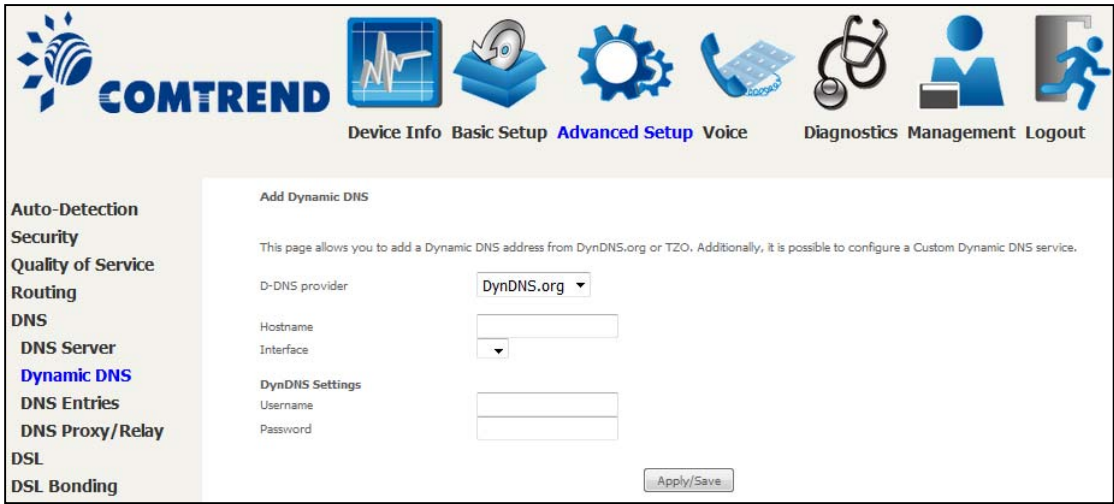
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

| Hostname                | Username | Service | Interface | DDNS Server | URL | Remove |
|-------------------------|----------|---------|-----------|-------------|-----|--------|
| <div> Add Remove </div> |          |         |           |             |     |        |

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DNS Server  
**Dynamic DNS**  
DNS Entries  
DNS Proxy/Relay

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



**COMTREND**

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

**Add Dynamic DNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO. Additionally, it is possible to configure a Custom Dynamic DNS service.

D-DNS provider: DynDNS.org

Hostname:

Interface:

DynDNS Settings

Username:

Password:

Apply/Save

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DNS Server  
**Dynamic DNS**  
DNS Entries  
DNS Proxy/Relay  
DSL  
DSL Bonding

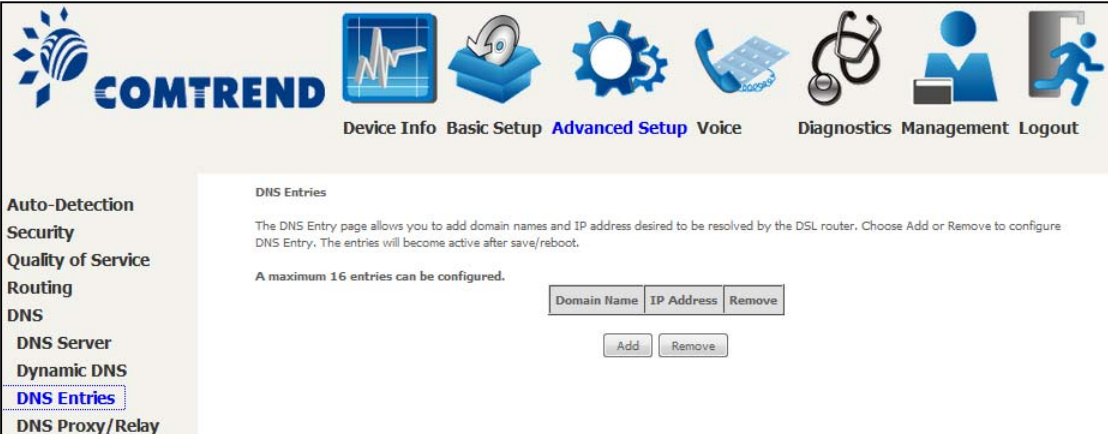
Click **Apply/Save** to save your settings.

Consult the table below for field descriptions.

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

### 6.5.3 DNS Entries

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



**COMTREND**

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DNS Server  
Dynamic DNS  
**DNS Entries**  
DNS Proxy/Relay

**DNS Entries**

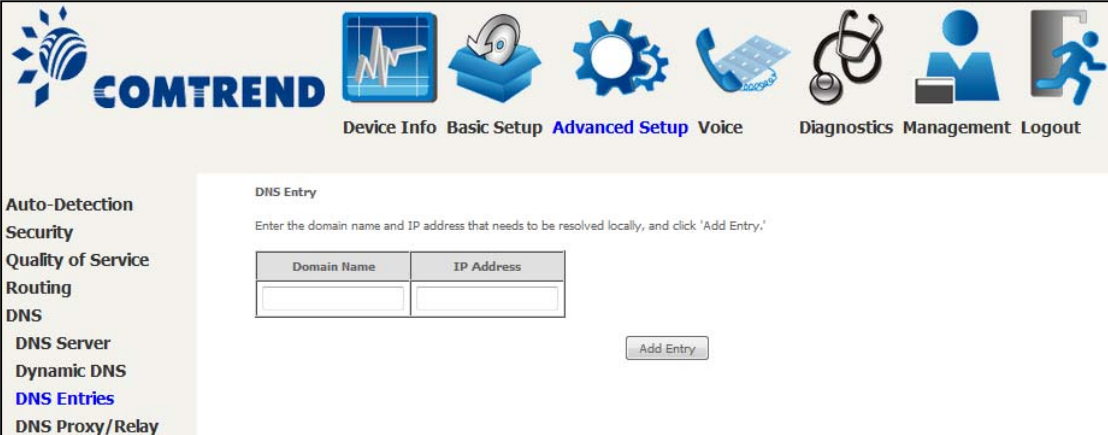
The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router. Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.

A maximum 16 entries can be configured.

| Domain Name | IP Address | Remove |
|-------------|------------|--------|
|             |            |        |

Add Remove

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



**COMTREND**

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DNS Server  
Dynamic DNS  
**DNS Entries**  
DNS Proxy/Relay

**DNS Entry**

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

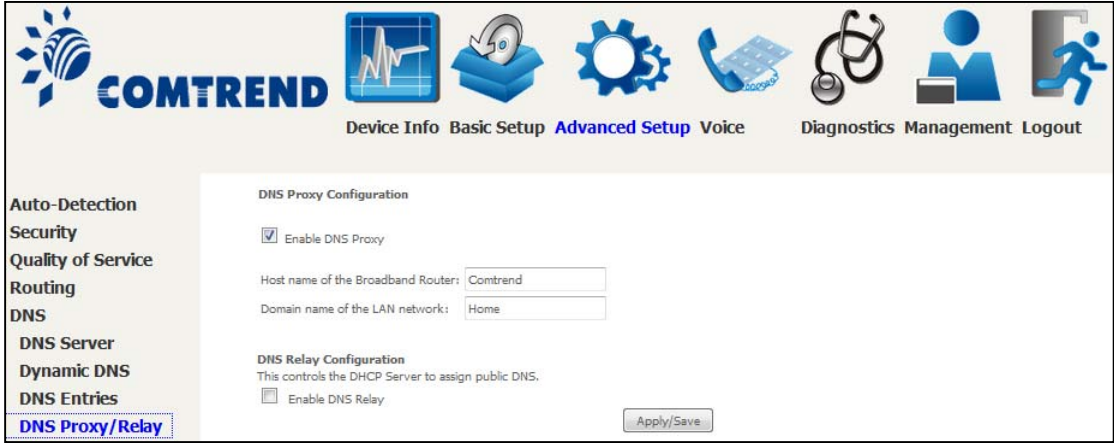
| Domain Name | IP Address |
|-------------|------------|
|             |            |

Add Entry

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

## 6.5.4 DNS Proxy/Relay

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".



The screenshot displays the Comtrend web interface for configuring DNS Proxy/Relay. The top navigation bar includes the Comtrend logo and icons for Device Info, Basic Setup, Advanced Setup (highlighted), Voice, Diagnostics, Management, and Logout. A left sidebar lists various configuration categories: Auto-Detection, Security, Quality of Service, Routing, DNS (expanded), DNS Server, Dynamic DNS, DNS Entries, and DNS Proxy/Relay (highlighted). The main content area is titled "DNS Proxy Configuration" and contains the following settings:

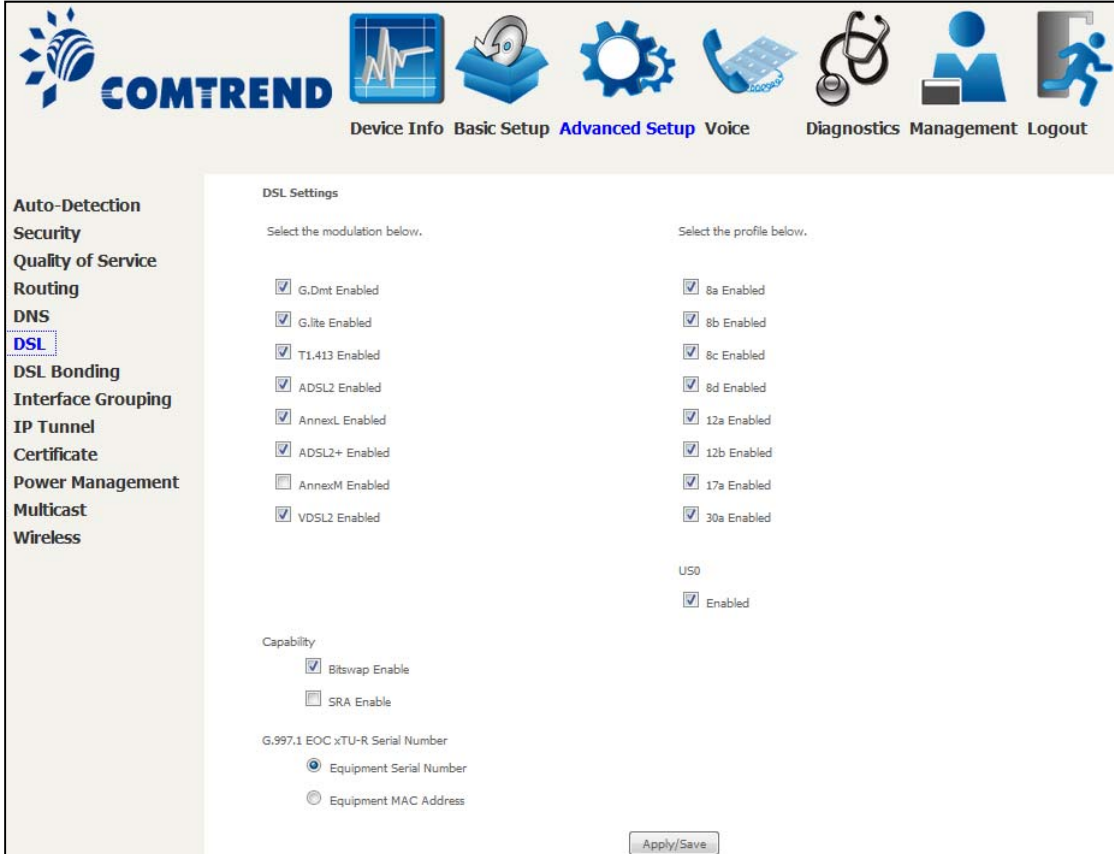
- ☒ Enable DNS Proxy
- Host name of the Broadband Router: Comtrend
- Domain name of the LAN network: Home

Below this, the "DNS Relay Configuration" section is shown, with a note: "This controls the DHCP Server to assign public DNS." It includes an unchecked checkbox for "Enable DNS Relay". An "Apply/Save" button is located at the bottom right of the configuration area.

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

## 6.6 DSL

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



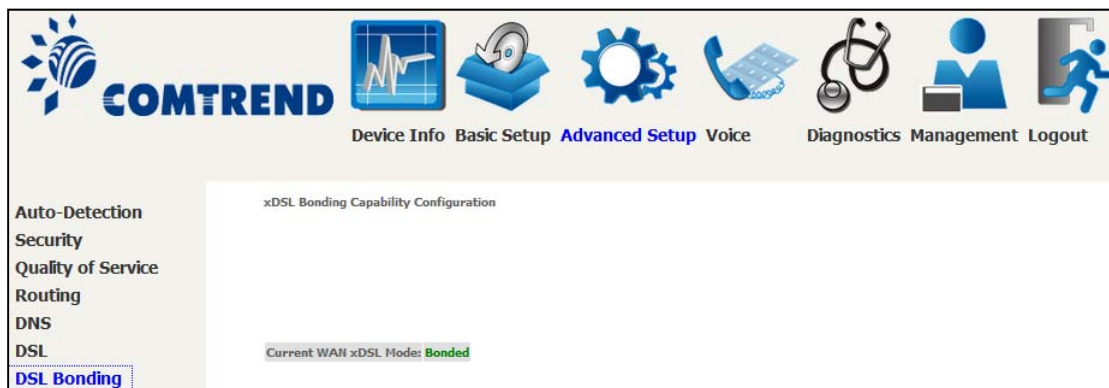
| DSL Mode | Data Transmission Rate - Mbps (Megabits per second)       |                    |
|----------|-----------------------------------------------------------|--------------------|
| G.Dmt    | Downstream: 12 Mbps                                       | Upstream: 1.3 Mbps |
| G.lite   | Downstream: 4 Mbps                                        | Upstream: 0.5 Mbps |
| T1.413   | Downstream: 8 Mbps                                        | Upstream: 1.0 Mbps |
| ADSL2    | Downstream: 12 Mbps                                       | Upstream: 1.0 Mbps |
| AnnexL   | Supports longer loops but with reduced transmission rates |                    |
| ADSL2+   | Downstream: 24 Mbps                                       | Upstream: 1.0 Mbps |
| AnnexM   | Downstream: 24 Mbps                                       | Upstream: 3.5 Mbps |
| VDSL2    | Downstream: 100 Mbps                                      | Upstream: 60 Mbps  |

| VDSL Profile | Maximum Downstream Throughput- Mbps (Megabits per second) |
|--------------|-----------------------------------------------------------|
| 8a           | Downstream 50                                             |
| 8b           | Downstream 50                                             |
| 8c           | Downstream: 50                                            |

| 8d                                   | Downstream: 50                                                                                                            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 12a                                  | Downstream: 68                                                                                                            |
| 12b                                  | Downstream: 68                                                                                                            |
| 17a                                  | Downstream: 100                                                                                                           |
| 30a                                  | Downstream: 100 Mbps      Upstream: 100 Mbps                                                                              |
| Options                              | Description                                                                                                               |
| US0                                  | Band between 20 and 138 kHz for long loops to upstream                                                                    |
| Bitswap Enable                       | Enables adaptive handshaking functionality                                                                                |
| SRA Enable                           | Enables Seamless Rate Adaptation (SRA)                                                                                    |
| G997.1 EOC<br>xTU-R Serial<br>Number | Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages |

## 6.7 DSL Bonding

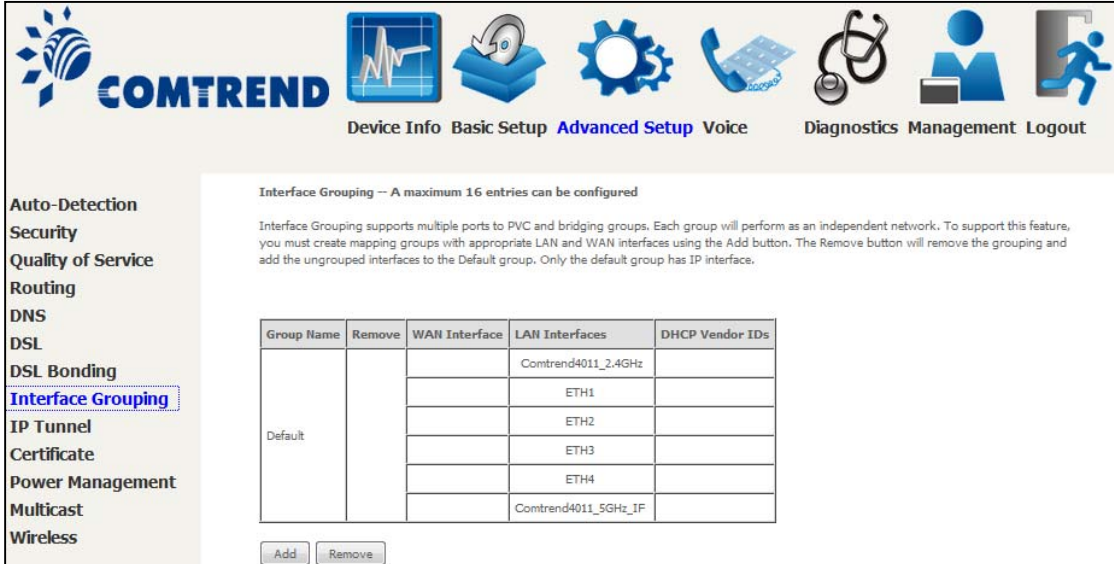
This page displays the bonding status of the connected xDSL line.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup (highlighted in blue), Voice, Diagnostics, Management, and Logout. Below the navigation bar, on the left side, there is a sidebar menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, and DSL Bonding (highlighted in blue). The main content area displays the 'xDSL Bonding Capability Configuration' page. It shows the 'Current WAN xDSL Mode' as 'Bonded' in green text.

## 6.8 Interface Grouping

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



The screenshot shows the COMTREND web interface. The top navigation bar includes icons for Device Info, Basic Setup, **Advanced Setup**, Voice, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, **Interface Grouping** (highlighted), IP Tunnel, Certificate, Power Management, Multicast, and Wireless.

The main content area is titled "Interface Grouping — A maximum 16 entries can be configured". Below the title, a paragraph explains the feature: "Interface Grouping supports multiple ports to PVC 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."

Below the text is a table with the following columns: Group Name, Remove, WAN Interface, LAN Interfaces, and DHCP Vendor IDs. The table contains one entry for the "Default" group, which has five LAN interfaces listed: Comtrend4011\_2.4GHz, ETH1, ETH2, ETH3, ETH4, and Comtrend4011\_5GHz\_IF. At the bottom of the table are "Add" and "Remove" buttons.

| Group Name | Remove | WAN Interface | LAN Interfaces       | DHCP Vendor IDs |
|------------|--------|---------------|----------------------|-----------------|
| Default    |        |               | Comtrend4011_2.4GHz  |                 |
|            |        |               | ETH1                 |                 |
|            |        |               | ETH2                 |                 |
|            |        |               | ETH3                 |                 |
|            |        |               | ETH4                 |                 |
|            |        |               | Comtrend4011_5GHz_IF |                 |

Buttons:

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
Voice
Diagnostics
Management
Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

DSL Bonding

Interface Grouping

IP Tunnel

Certificate

Power Management

Multicast

Wireless

### Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped WAN Interfaces

->

<-

Available WAN Interfaces

Grouped LAN Interfaces

->

<-

Available LAN Interfaces

ETH1  
ETH2  
ETH3  
ETH4  
Comtrend4011\_5GHz\_IF  
Comtrend4011\_2.4GHz

Automatically Add Clients With the following DHCP Vendor IDs

### 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.