

# NexusLink 3120

## A/VDSL Bonding Router

### 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](#).

**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**

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.

1.L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur. 2.Cet appareil est conforme aux limites d'exposition aux rayonnements de la IC pour un environnement non contrôlé. L'antenne doit être installé de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps.

### **ISED**

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

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

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©2024 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>41</b>
5.1 WAN SETUP.....	42
5.1.1 WAN Service Setup.....	43
5.2 NAT.....	44
5.2.1 Virtual Servers.....	44
5.2.2 Port Triggering.....	46
5.2.3 DMZ Host.....	48
5.2.4 IP Address Map.....	49
5.2.5 ALG/Pass-Through.....	50
5.3 LAN.....	51
5.3.1 Lan VLAN Setting.....	54
5.3.2 LAN IPv6 Autoconfig.....	55
5.3.3 Static IP Neighbor.....	58
5.3.4 UPnP.....	59
5.4 WIRELESS.....	60
5.4.1 Basic 2.4GHz.....	60
5.4.2 Security 2.4GHz.....	62
5.4.3 Basic 5GHz.....	64
5.4.4 Security 5GHz.....	66
5.5 PARENTAL CONTROL.....	67
5.5.1 Time Restriction.....	67
5.5.2 URL Filter.....	68
5.6 HOME NETWORKING.....	70
5.6.1 Print Server.....	70
5.6.2 DLNA.....	70
5.6.3 Storage Service.....	71

5.6.4 USB Speed.....	72
<b>CHAPTER 6 ADVANCED SETUP.....</b>	<b>73</b>
6.1 AUTO-DETECTION SETUP .....	73
6.2 SECURITY.....	78
6.2.1 IP Filtering.....	78
6.2.2 MAC Filtering.....	82
6.3 QUALITY OF SERVICE (QoS).....	84
6.3.1 QoS Queue.....	85
6.3.1.1 QoS Queue Configuration.....	85
6.3.1.2 Wlan Queue.....	89
6.3.2 QoS Classification .....	90
6.3.3 QoS Port Shaping .....	92
6.4 ROUTING.....	93
6.4.1 Default Gateway .....	93
6.4.2 Static Route .....	94
6.4.3 Policy Routing.....	95
6.4.4 RIP .....	96
6.5 DNS.....	97
6.5.1 DNS Server.....	97
6.5.2 Dynamic DNS.....	98
6.5.3 DNS Entries .....	99
6.5.4 DNS Proxy/Relay .....	100
6.6 DSL .....	101
6.7 DSL BONDING .....	102
6.8 INTERFACE GROUPING .....	103
6.9 IP TUNNEL .....	106
6.9.1 IPv6inIPv4 .....	106
6.9.2 IPv4inIPv6 .....	107
6.10 CERTIFICATE .....	108
6.10.1 Local .....	108
6.10.2 Trusted CA .....	110
6.11 POWER MANAGEMENT.....	111
6.12 MULTICAST .....	112
6.13 WIRELESS .....	114
6.13.1 Basic 2.4GHz .....	114
6.13.2 Security 2.4GHz.....	116
6.13.3 WPS 2.4GHz .....	118
6.13.4 MAC Filter 2.4GHz.....	121
6.13.5 Wireless Bridge 2.4GHz.....	123
6.13.6 Advanced 2.4GHz.....	124
6.13.7 Basic 5GHz .....	127
6.13.8 WPS 5GHz .....	129
6.13.9 MAC Filter 5GHz.....	131
6.13.10 Wireless Bridge 2.4GHz.....	132
6.13.11 Advanced 5GHz.....	133
<b>CHAPTER 7 DIAGNOSTICS.....</b>	<b>135</b>
7.1 DIAGNOSTICS – INDIVIDUAL TESTS .....	135
7.2 ETHERNET OAM.....	136
7.3 UPTIME STATUS.....	138
7.4 PING.....	139
7.5 TRACE ROUTE.....	140
<b>CHAPTER 8 MANAGEMENT.....</b>	<b>141</b>
8.1 SETTINGS .....	141
8.1.1 Backup Settings.....	141
8.1.2 Update Settings.....	142
8.1.3 Restore Default .....	142
8.2 SYSTEM LOG.....	144
8.3 SNMP AGENT.....	146
8.4 TR-069 CLIENT.....	147

8.5 INTERNET TIME .....	149
8.6 ACCESS CONTROL.....	150
8.6.1 <i>Accounts</i> .....	150
8.6.2 <i>Services</i> .....	152
8.6.3 <i>IP Address</i> .....	153
8.7 WAKE-ON-LAN.....	154
8.8 UPDATE SOFTWARE.....	155
8.9 REBOOT .....	156
<b>CHAPTER 9 LOGOUT .....</b>	<b>157</b>
<b>APPENDIX A - FIREWALL.....</b>	<b>158</b>
<b>APPENDIX B - PIN ASSIGNMENTS .....</b>	<b>161</b>
<b>APPENDIX C - SPECIFICATIONS.....</b>	<b>162</b>
<b>APPENDIX D - SSH CLIENT.....</b>	<b>164</b>
<b>APPENDIX E - PRINTER SERVER.....</b>	<b>165</b>
<b>APPENDIX F - CONNECTION SETUP.....</b>	<b>172</b>



## Chapter 1 Introduction

NexusLink 3120 is a Multi-DSL bonding router using the BCM 63138. It not only provides both ADSL and VDSL but also supports xDSL bonding for extending WAN access bandwidth. Integrated 5 Giga Ethernet ports support WLAN 802.11n 2.4GHz and 802.11ac 5GHz Frequency bands. Therefore, NexusLink 3120 is designed for high speed applications and is suitable for triple play services.

NexusLink 3120 has a USB3.0 host port which provides high speed access for USB devices such as printer server, 3G dongle, HDD, and supports DLNA and samba accessibility.

## Chapter 2 Installation

### 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.



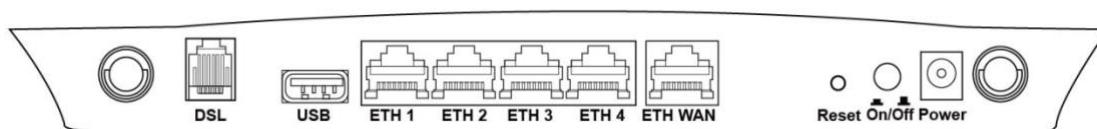
**DO NOT STACK**

#### **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 3120 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.

**ETH WAN PORT**

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

**Ethernet (LAN) Ports**

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

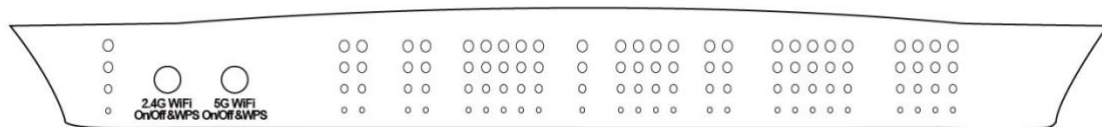
**USB Host Port (Type A)**

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

**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.
ETH WAN	GREEN	On	WAN is connected at 1000 Mbps.
		Off	Ethernet WAN is not connected.
		Blink	In TX/RX over 1000 Mbps.
	ORANGE	On	Ethernet is connected at 10/100 Mbps.
		Off	Ethernet WAN is not connected.
		Blink	In TX/RX over 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.
	ORANGE	On	Ethernet is connected at 10/100 Mbps.
		Off	Ethernet is not connected.
		Blink	In TX/RX over 10/100 Mbps.
WPS	GREEN	On	WPS(2.4G) 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.
	ORANGE	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 2.4G	GREEN	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.

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

## Chapter 3 Web User Interface

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

### 3.1 Default Settings

The factory default settings of this device are summarized below.

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

#### **Technical Note**

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

## 3.2 IP Configuration

### DHCP MODE

When the NexusLink 3120 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.

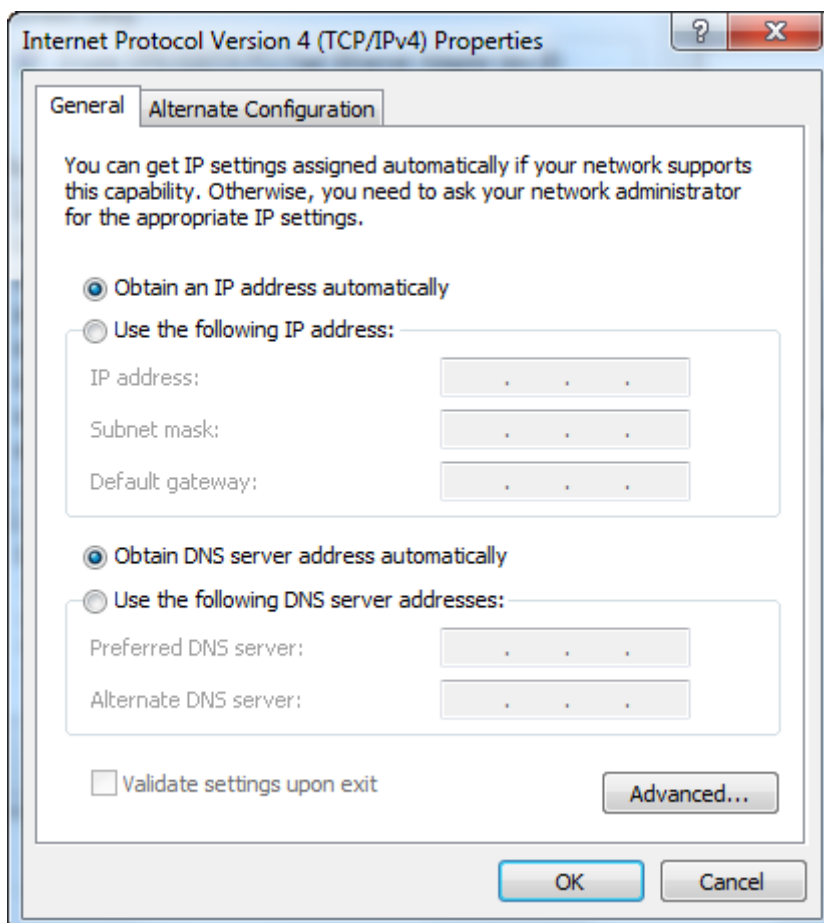
To obtain an IP address from the DHCP server, follow the steps provided below.

**NOTE:** The following procedure assumes you are running Windows XP. 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.

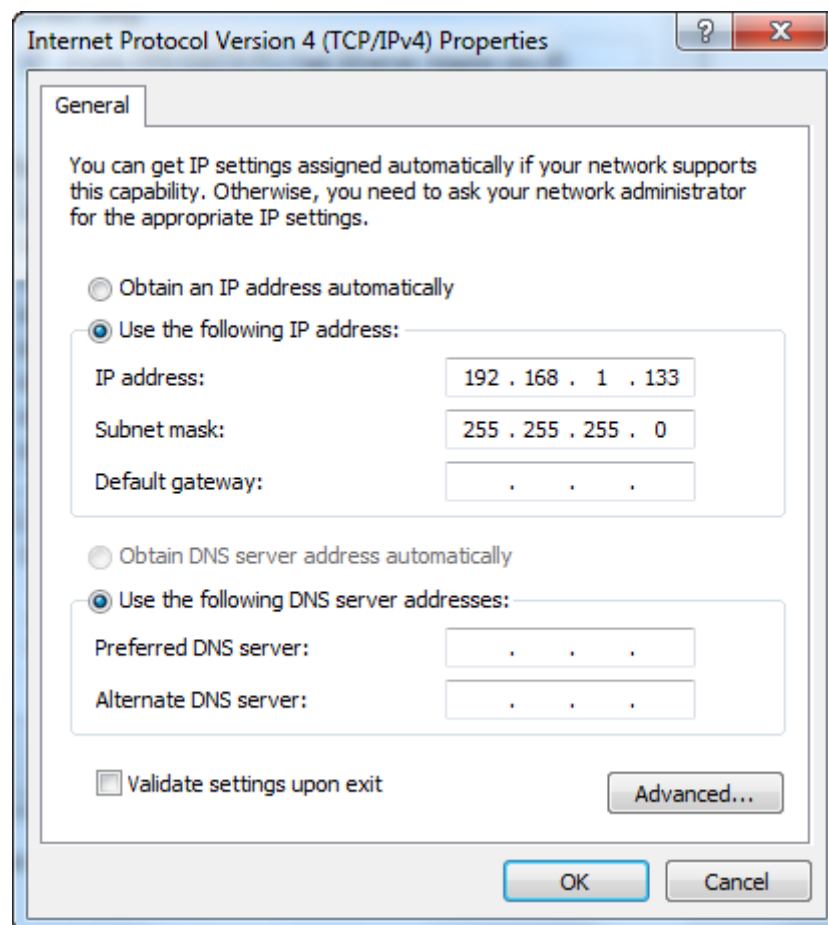
## STATIC IP MODE

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 XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

- STEP 1:** From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- STEP 2:** Select Internet Protocol (TCP/IP) **and click the Properties** button.
- STEP 3:** Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



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



## 3.3 Login Procedure

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

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

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

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

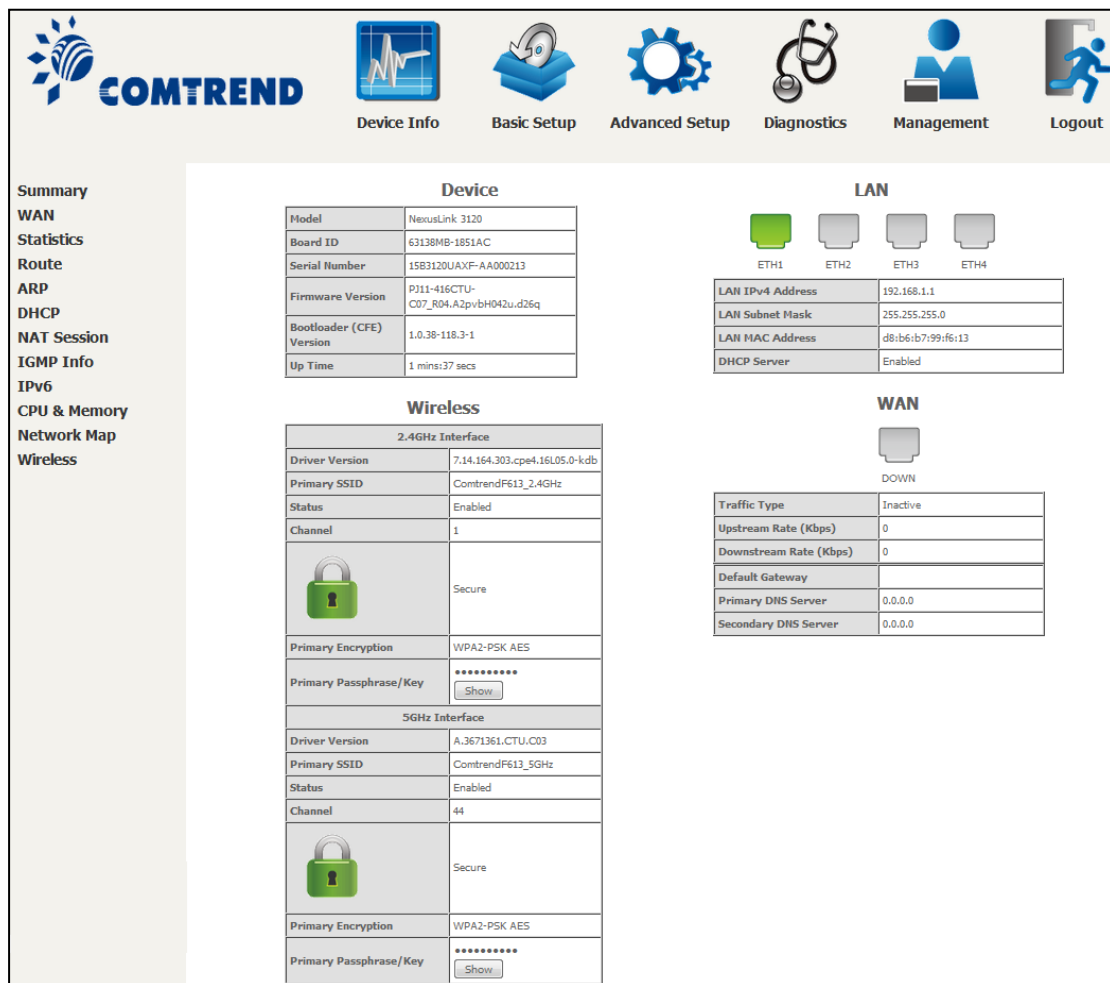
**STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in section [3.1 Default Settings](#).



Click **OK** to continue.

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

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



**Device**

Model	NexusLink 3120
Board ID	63138MB-1851AC
Serial Number	15B3120UAXF-AA000213
Firmware Version	PJ11-416CTU-C07_R04.A2pvh042u.d26q
Bootloader (CFE) Version	1.0.38-118.3-1
Up Time	1 mins:37 secs

**Wireless**

**2.4GHz Interface**

Driver Version	7.14.164.303.cpe4.16L05.0-kdb
Primary SSID	ComtrendF613_2.4GHz
Status	Enabled
Channel	1
Security	Secure
Primary Encryption	WPA2-PSK AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>

**5GHz Interface**

Driver Version	A.3671361.CTU.C03
Primary SSID	ComtrendF613_5GHz
Status	Enabled
Channel	44
Security	Secure
Primary Encryption	WPA2-PSK AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>

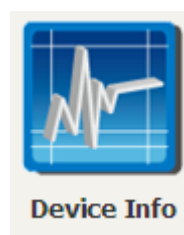
**LAN**

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:99:fe:13
DHCP Server	Enabled

**WAN**

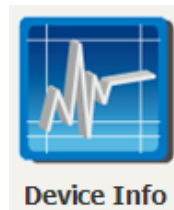
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

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.

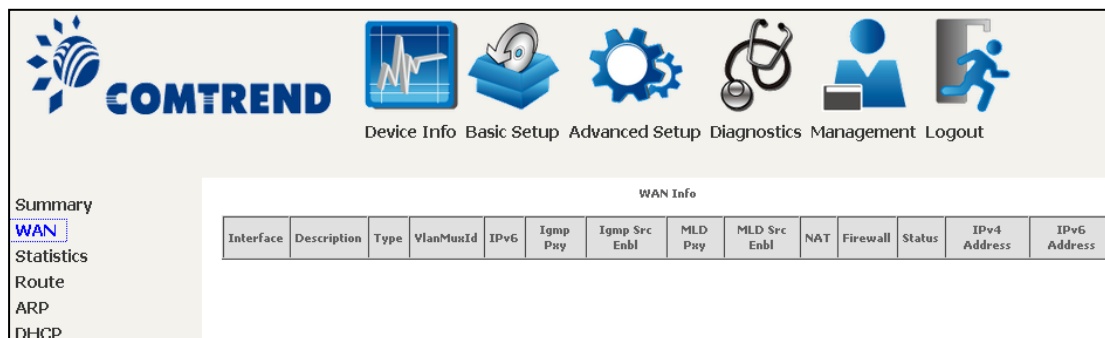
The screenshot shows the Device Info Summary screen. On the left is a main menu with options: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, CPU & Memory, Network Map, and Wireless. The central display area is divided into four sections:

- Device:** A table with fields: Model (NexusLink 3120), Board ID (63138MB-1851AC), Serial Number (15B3120UAXF-AA000213), Firmware Version (P111-416CTU-C07\_R04.A2pvh042u.d26q), Bootloader (CFE) Version (1.0.38-118.3-1), and Up Time (1 mins:37 secs).
- Wireless:** Divided into 2.4GHz and 5GHz interfaces. Both are secured with WPA2-PSK AES encryption. The 2.4GHz interface has SSID 'ComtrendF613\_2.4GHz' and channel 1. The 5GHz interface has SSID 'ComtrendF613\_5GHz' and channel 44.
- LAN:** Shows four Ethernet ports (ETH1-ETH4). A table lists: LAN IPv4 Address (192.168.1.1), LAN Subnet Mask (255.255.255.0), LAN MAC Address (d8:b6:b7:99:f6:13), and DHCP Server (Enabled).
- WAN:** Shows a 'DOW' icon and a table with: Traffic Type (Inactive), Upstream Rate (Kbps) (0), Downstream Rate (Kbps) (0), Default Gateway, Primary DNS Server (0.0.0.0), and 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.

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ETHWAN	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0
ETH1	86762	792	0	0	0	202	554	36	512553	816	0	5	133	613	70	0
ETH2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ComtrendF613_5GHz_IF	99416	551	0	0	0	217	334	0	215393	2131	0	4	1444	333	354	0
ComtrendF613_2.4GHz	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0
ComtrendF613_5GHz	0	0	0	0	0	0	0	0	108502	1004	0	0	0	1004	0	0

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

### 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

### 4.2.4 xDSL Statistics

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

#### VDSL

Bonding Line Selection DSL1 ▼

Mode:	VDSL2	
Traffic Type:	PTM	
Status:	Up	
Link Power State:	LO	
	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	251	60
Attenuation (0.1 dB):	52	0
Output Power (0.1 dBm):	145	84
Attainable Rate (Kbps):	149402	57883
	Path 0	
	Downstream	Upstream
Rate (Kbps):	92485	57883
B (# of bytes in Mux Data Frame):	247	239
M (# of Mux Data Frames in an RS codeword):	1	1
T (# of Mux Data Frames in an OH sub-frame):	22	64
R (# of redundancy bytes in the RS codeword):	6	0
S (# of data symbols over which the RS code word spans):	0.0853	0.1320
L (# of bits transmitted in each data symbol):	23808	14549
D (interleaver depth):	187	1
I (interleaver block size in bytes):	254	120
N (RS codeword size):	254	240
Delay (msec):	4	0
INP (DMT symbol):	0.00	0.00
OH Frames:	592973	329600
OH Frame Errors:	0	3
RS Words:	1213775	819097
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	325	1
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	4801215	0
Data Cells:	40	0
Bit Errors:	0	0
Total ES:	20	2
Total SES:	20	0
Total UAS:	3209	3199

xDSL BER Test Reset Statistics Draw Graph



ADSL

Bonding Line Selection

Mode:	ADSL_2plus	
Traffic Type:	ATM	
Status:	Up	
Link Power State:	LO	
	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	76	74
Attenuation (0.1 dB):	5	29
Output Power (0.1 dBm):	174	120
Attainable Rate (Kbps):	25144	1255
	Path 0	
	Downstream	Upstream
Rate (Kbps):	24791	1255
MSGc (# of bytes in overhead channel message):	59	11
B (# of bytes in Mux Data Frame):	254	77
M (# of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	3	2
R (# of check bytes in FEC Data Frame):	0	0
S (ratio of FEC over PMD Data Frame length):	0.3287	1.9746
L (# of bits in PMD Data Frame):	6206	316
D (interleaver depth):	1	1
Delay (msec):	0	0
INP (DMT symbol):	0.00	0.00
Super Frames:	573879	316877
Super Frame Errors:	0	1
RS Words:	0	7020776
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	318	1
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	202739363	10263207
Data Cells:	3940	0
Bit Errors:	0	20
Total ES:	10	1
Total SES:	10	0
Total UAS:	3185	3175

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

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

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

**In 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

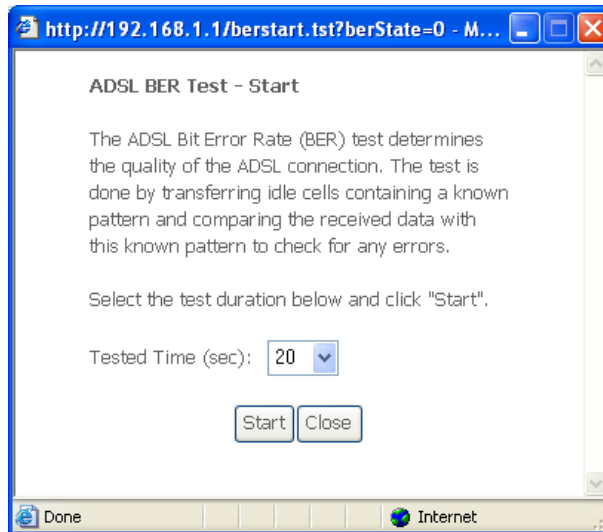
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)

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

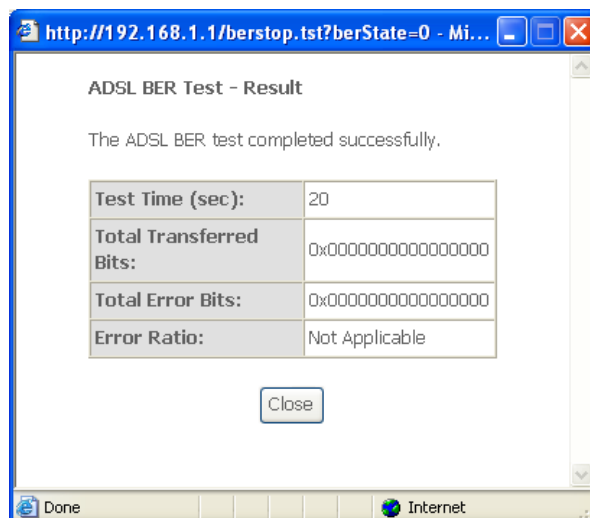
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

**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.

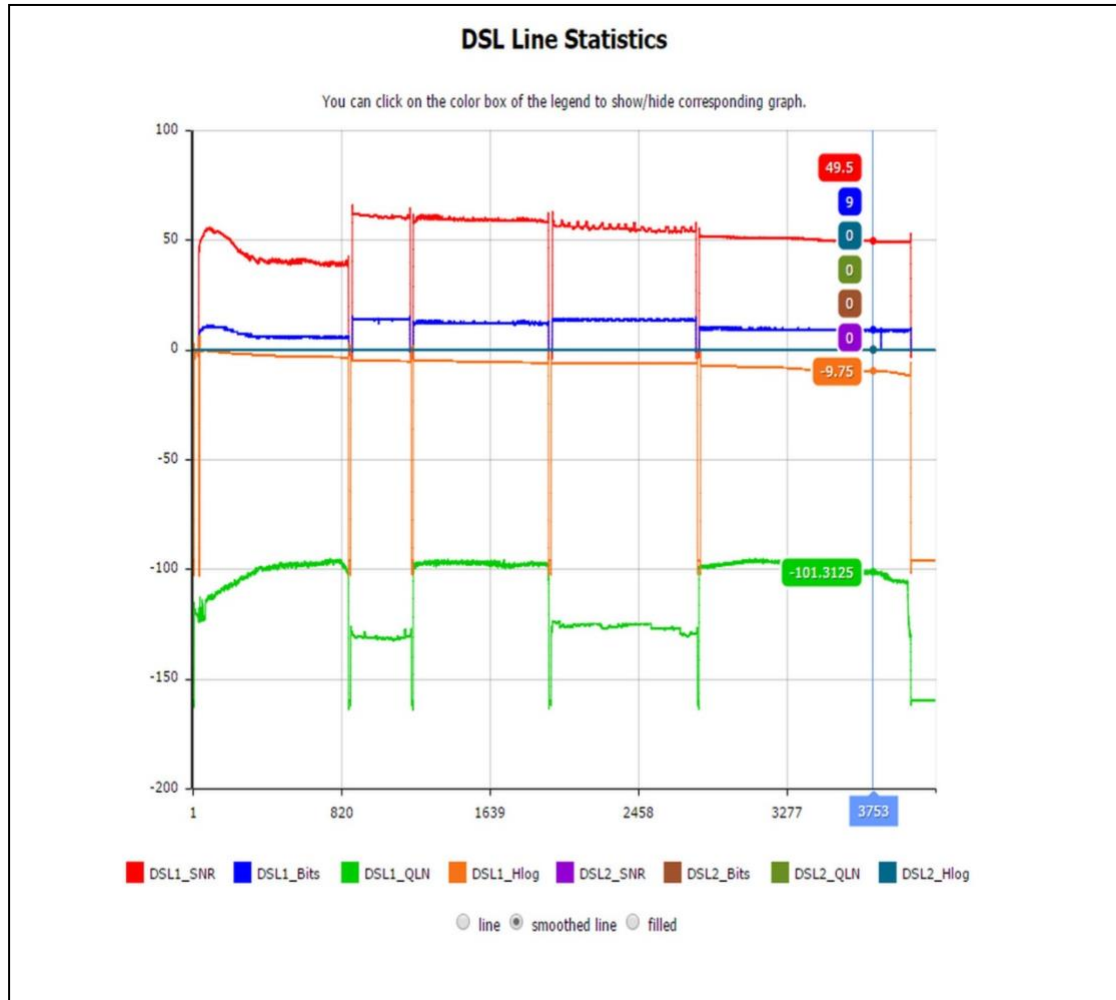


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



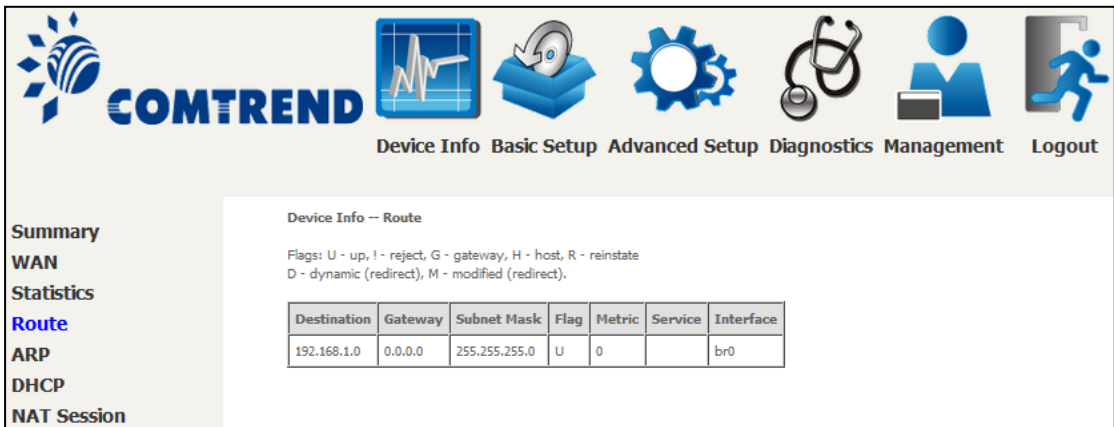
**xDSL TONE GRAPH**

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 3120 has found.



Device Info -- Route

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

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

Summary  
WAN  
Statistics  
**Route**  
ARP  
DHCP  
NAT Session

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

## 4.4 ARP

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

IP address	Flags	HW Address	Device
192.168.1.3	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.

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

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 UPD/TCP protocols passing through the device.

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

NAT Session					
Press "Show Less" will show NAT session information on WAN side only.					
Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.3	51012	192.168.1.1	80	tcp	1
192.168.1.3	51015	192.168.1.1	80	tcp	86400
192.168.1.3	51013	192.168.1.1	80	tcp	1
127.0.0.1	45000	127.0.0.1	45032	udp	29
192.168.61.1		192.168.61.2		icmp	10
192.168.61.1		192.168.61.2		icmp	20
192.168.1.3	51014	192.168.1.1	80	tcp	1

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.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary  
WAN  
Statistics  
Route  
ARP  
DHCP  
NAT Session  
**IGMP Info**

List of IGMP Proxy Entries

Interface	WAN	Groups	Member	Timeout
-----------	-----	--------	--------	---------

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.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various system information sections: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, **IPv6 Info** (highlighted), IPv6 Neighbor, and IPv6 Route. The main content area is titled 'IPv6 WAN Connection Info' and contains a table with columns for Interface, Status, Address, and Prefix. Below this table is a 'General Info' section with the following fields:

IPv6 WAN Connection Info			
Interface	Status	Address	Prefix
General Info			
Device Link-local Address	fe80::21d:20ff:feaa:bbcc/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.

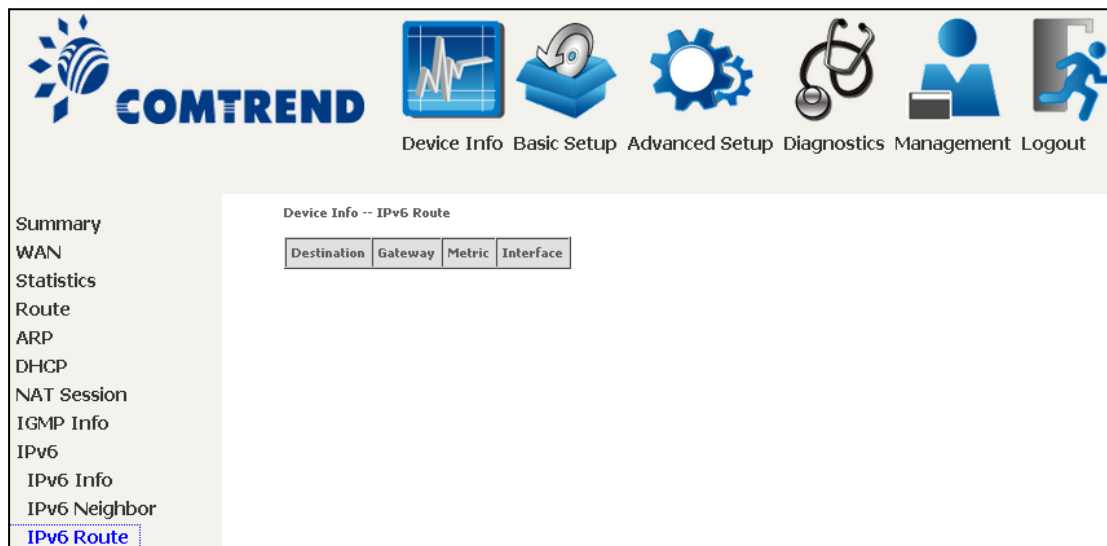
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons and labels for 'Device Info', 'Basic Setup', 'Advanced Setup', 'Diagnostics', 'Management', and 'Logout'. The 'Device Info' section is active. On the left, a sidebar menu lists various system information sections, with 'IPv6 Neighbor' highlighted in blue. The main content area displays a table titled 'Device Info -- IPv6 Neighbor Discovery table'.

IPv6 address	Flags	HW Address	Device
fe80::dab6:b7ff:fe99:f613	STALE	d8:b6:b7:99:f6:13	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.



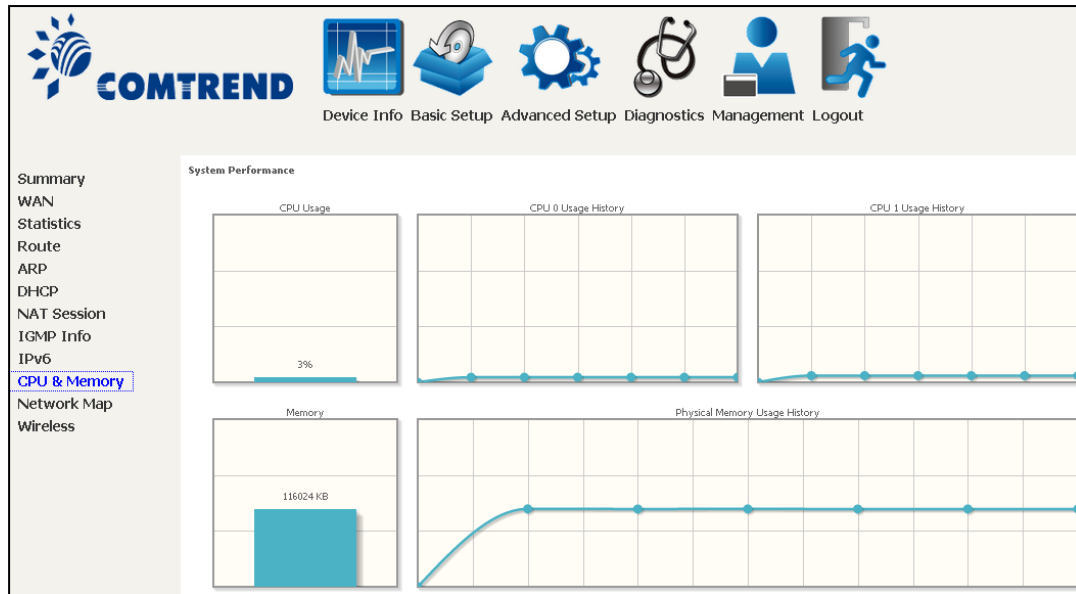
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below this, a sidebar menu lists various configuration options, with 'IPv6 Route' highlighted. The main content area displays the title 'Device Info -- IPv6 Route' and a table with the following headers:

Destination	Gateway	Metric	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

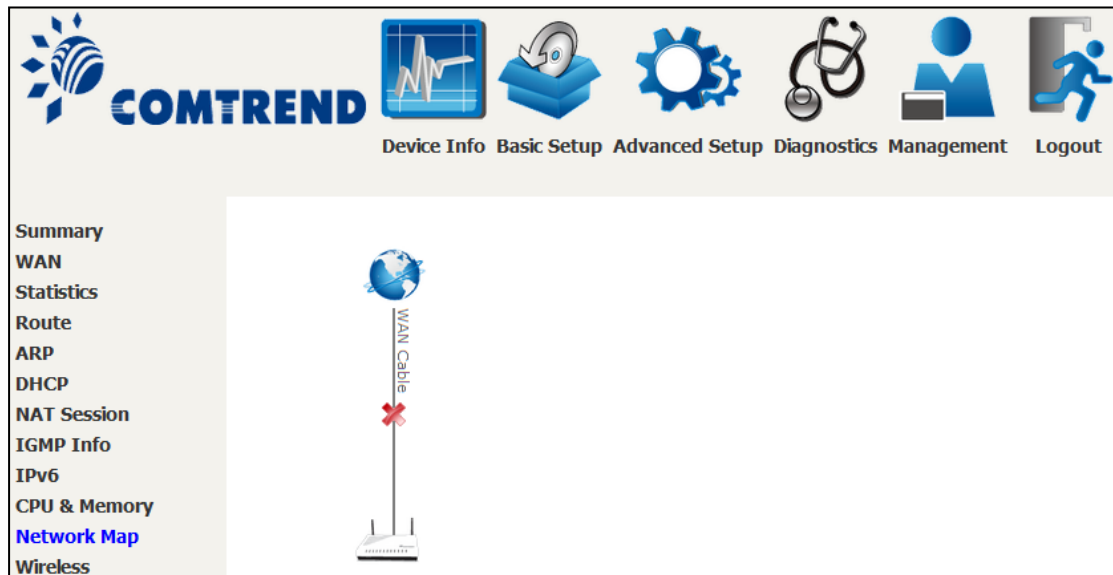
Displays the system performance graphs. Shows the current loading of the CPU and memory usage with dynamic updates.



## 4.10 Network Map

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

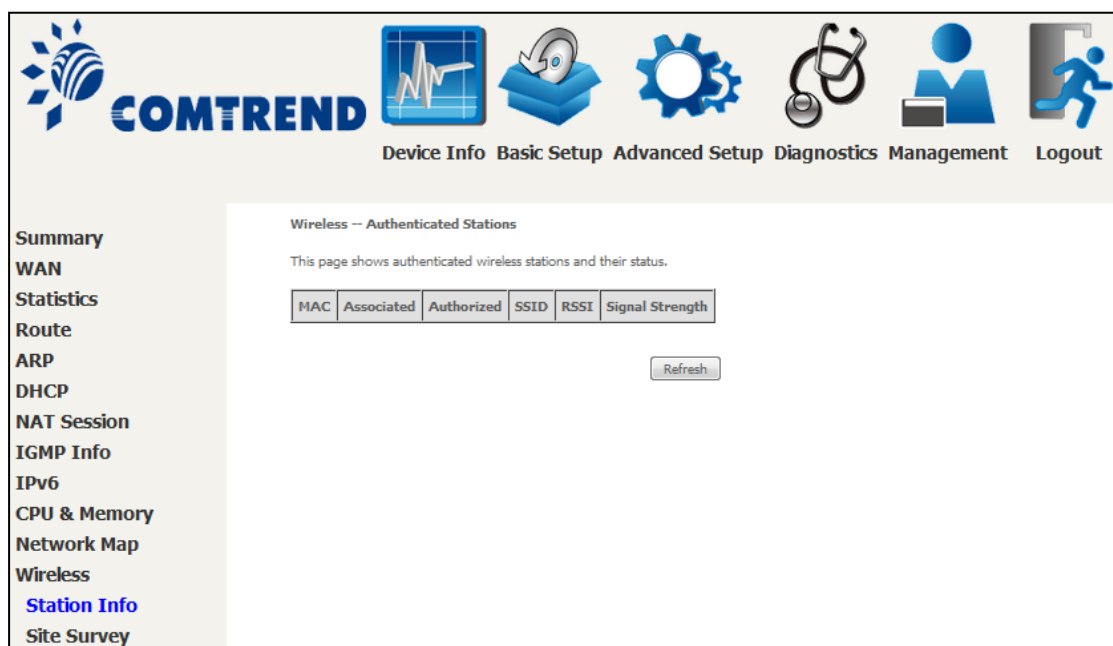
Note: This graph is unavailable for Internet Explorer users.



## 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.







<b>Field</b>	<b>Description</b>
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.
RSSI	Lists received signal strength of each station in dBm.
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.

#### 2.4GHz



**Summary**

WAN

Statistics

Route

ARP

DHCP

NAT Session

IGMP Info

IPv6

CPU & Memory

Network Map

Wireless

Station Info

Site Survey

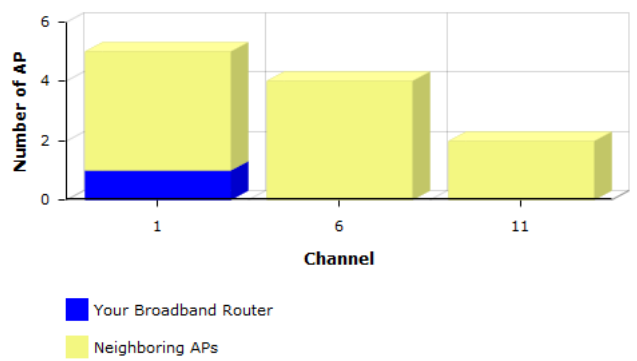
2.4GHz

5GHz

**Wireless -- Channel Graph**

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











Your broadband router is transmitting on channel 1.



Channel	Your Broadband Router	Neighboring APs
1	1	4
6	0	4
11	0	2

**Wireless -- Site Survey**

List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
	CTMIS-INT	00:1F:D4:03:DE:DE	1
	1313141413	D8:B6:B7:99:68:22	1
	1313141413	F8:8E:85:F5:07:93	1
	Jio_PLCC_JM_CHEN	F8:8E:85:C2:F4:DF	6
	3845	D8:B6:B7:BE:C2:8C	6
	12345678901234567890123456789012	52:B6:B7:BE:C2:8D	6
	CTMIS-INT	00:1F:D4:03:D9:E2	6
	Comtrend	D8:B6:B7:00:07:E8	1
	don-2.4	D8:B6:B7:BB:BB:A4	11
	Guest-5872u	1A:B6:B7:07:E1:4E	11



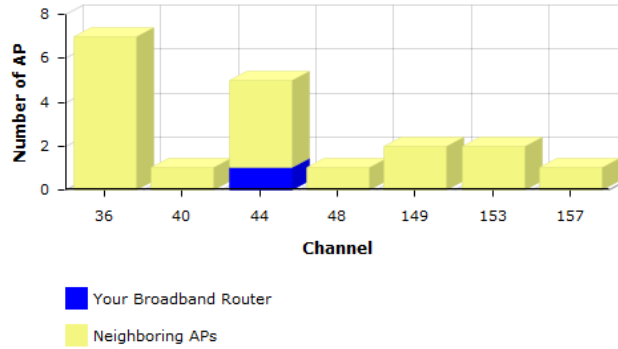
5GHz

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- NAT Session
- IGMP Info
- IPv6
- CPU & Memory
- Network Map
- Wireless
  - Station Info
  - Site Survey
  - 2.4GHz
  - 5GHz

Wireless -- Channel Graph

The following graph displays wireless APs found in your neighborhood by channel.  
Your broadband router is transmitting on channel 44.



Wireless -- Site Survey

List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
📶	COMTRENDSG_2AEA61	db:b6:b7:2a:ea:62	36
📶		80:1f:02:2e:fe:88	36
📶	Comtrend_5g	d8:b6:b7:00:07:e6	36
📶	VMP0243233	d8:b6:b7:2a:a8:10	36
📶	Comtrend0-E105_5GHz	d8:b6:b7:1b:79:2d	36
📶	comtrend-ap-08D9C4	d8:b6:b7:08:d9:c4	36
📶	COMTRENDSG_1B7913	d8:b6:b7:1b:79:14	36
📶	VMPoooooooo	d8:b6:b7:2a:dc:8c	40
📶	ComtrendF5EF_5GHz	d8:b6:b7:99:f5:ee	44
📶	ComtrendF5DD_5GHz	d8:b6:b7:99:f5:dc	44
📶	telenet-ap-0997752-5G	d8:b6:b7:2a:a6:6a	44
📶	UPC-AP-DF9A4C	d8:b6:b7:df:9a:4c	44
📶	D430AC55G	74:da:38:40:e0:ef	48
📶	000_WAP-5922-5G	74:da:38:73:0d:5b	149
📶		d8:b6:b7:a1:89:8a	149
📶	don5G	d8:b6:b7:07:e1:4f	153
📶	Guest-5872u	da:b6:b7:07:e1:4f	153
📶	icflight-master5G	c4:a8:1d:8f:16:f6	157

Refresh

## Chapter 5 Basic Setup

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



This will bring you to the following screen.

Device Info

**Basic Setup**

Advanced Setup

Diagnostics

Management

Logout

WAN Setup

NAT

LAN

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	d8:b6:b7:99:f6:13
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**

2.4GHz Interface	
Driver Version	7.14.164.303.cpe4.16L05.0-kdb
Primary SSID	ComtrendF613_2.4GHz
Status	Enabled
Channel	1
	Secure
Primary Encryption	WPA2-PSK AES
Primary Passphrase/Key	***** <input type="button" value="Show"/>
5GHz Interface	
Driver Version	A.3671361.CTU.C03
Primary SSID	ComtrendF613_5GHz
Status	Enabled
Channel	44
	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.

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

**NOTE:** Up to 16 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="checkbox"/>	<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.

## 5.2 NAT

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

### 5.2.1 Virtual Servers

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

**NAT -- Virtual Servers Setup**

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

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	NAT Loopback	Remove

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

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.  
**NOTE:** The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start". Remaining number of entries that can be configured:32

Choose All Interface  
 Choose One Interface

Use Interface:

Service Name:

Select a Service:   
 Custom Service:

Server IP Address:

Enable NAT Loopback

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		

Apply/Save

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

Consult the table below for field and header descriptions.

<b>Field/Header</b>	<b>Description</b>
Choose All Interface	Virtual server rules will be created for all WAN interfaces.
Choose One Interface Use Interface	Select a WAN interface from the drop-down menu.
Select a Service <b>Or</b> Custom Service	User should select the service from the list. <b>Or</b> User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
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.

**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.

**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:

Application Name:

Select an application:

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.

<b>Field/Header</b>	<b>Description</b>
Use Interface	Select a WAN interface from the drop-down menu.
Select an Application <b>Or</b> Custom Application	User should select the application from the list. <b>Or</b> User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	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.

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

**WAN Setup**  
**NAT**  
 Virtual Servers  
 Port Triggering  
**DMZ Host**  
 IP Address Map  
 ALG/Pass-Through  
 LAN  
 Wireless

**NAT -- DMZ Host**

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.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

Enable NAT Loopback

Save/Apply

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.

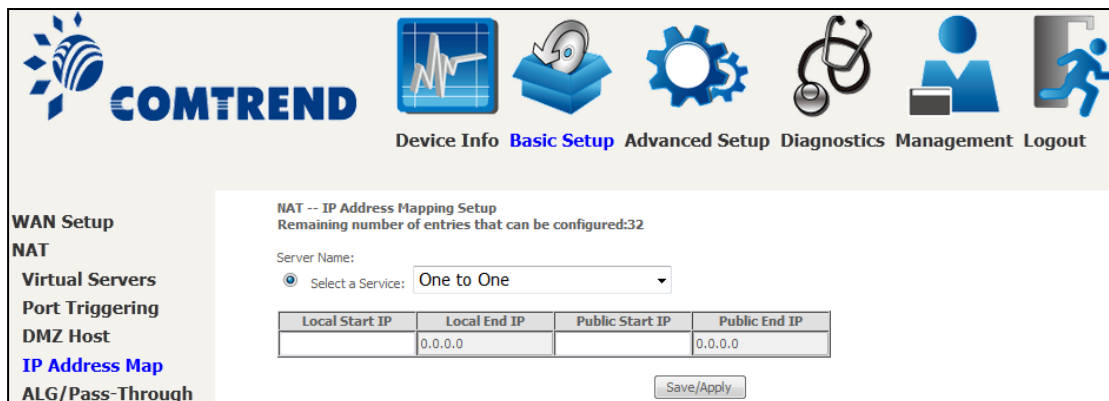
### 5.2.4 IP Address Map

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

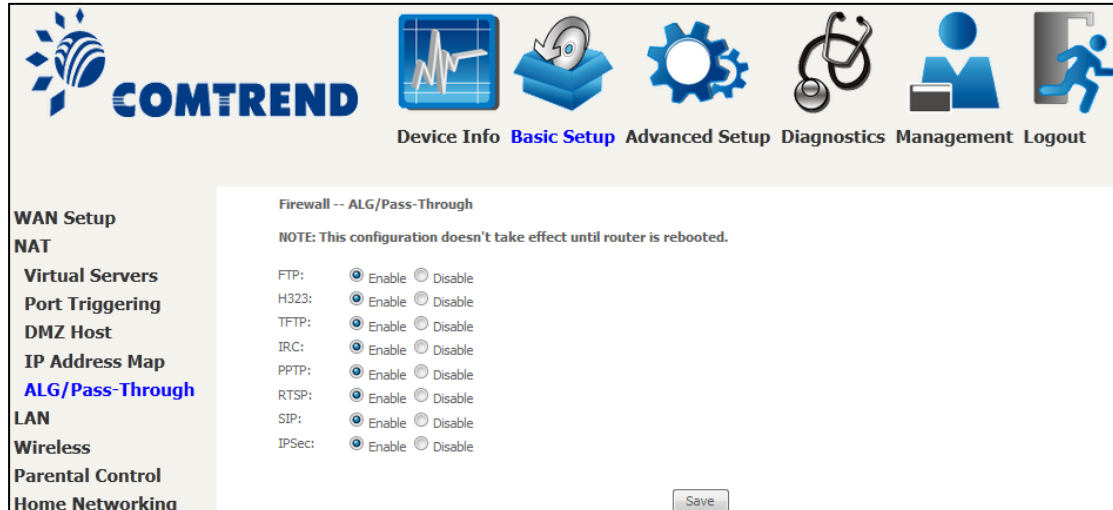
**Many to one:** mapping a range of local IP to a specific public IP

**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 displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different system functions: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, the main content area is titled "Firewall -- ALG/Pass-Through". A note states: "NOTE: This configuration doesn't take effect until router is rebooted." The configuration section lists several 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. On the left side of the interface, there is a sidebar menu with the following items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, ALG/Pass-Through (highlighted), LAN, Wireless, Parental Control, and Home Networking.

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**.

**Local Area Network (LAN) Setup**

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

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable IGMP LAN to LAN Multicast: **Disable** ▼  
(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Setting TFTP Server

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

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

**Ethernet Media Type**

ETH1: **Auto** ▼

ETH2: **Auto** ▼

ETH3: **Auto** ▼

ETH4: **Auto** ▼

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.

**Enable Automatic Static IP Reservation:** The Automatic Static IP Reservation function supports automatically adding DHCP client IP & MAC address to the static IP pool. When enabled, connected DHCP clients will be added to the static IP list and always receive the same IP address.

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

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

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.

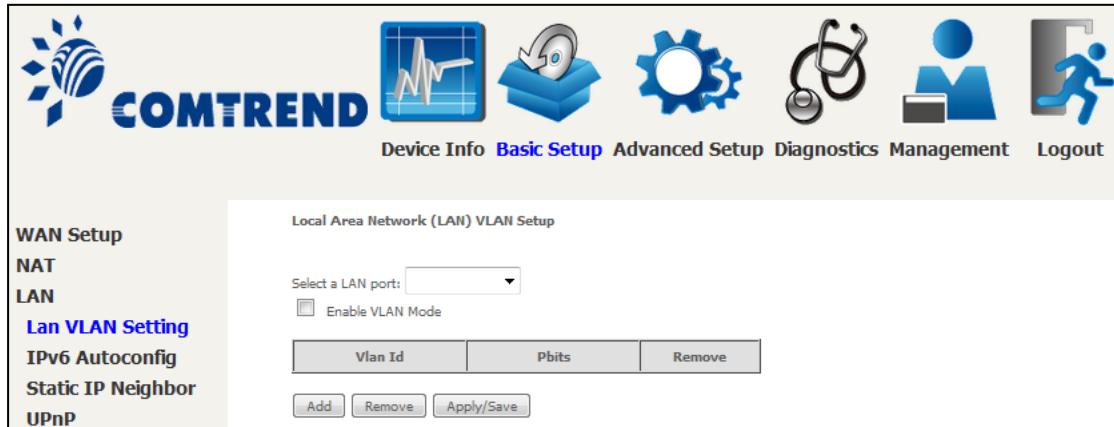
## **Ethernet Media Type:**

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

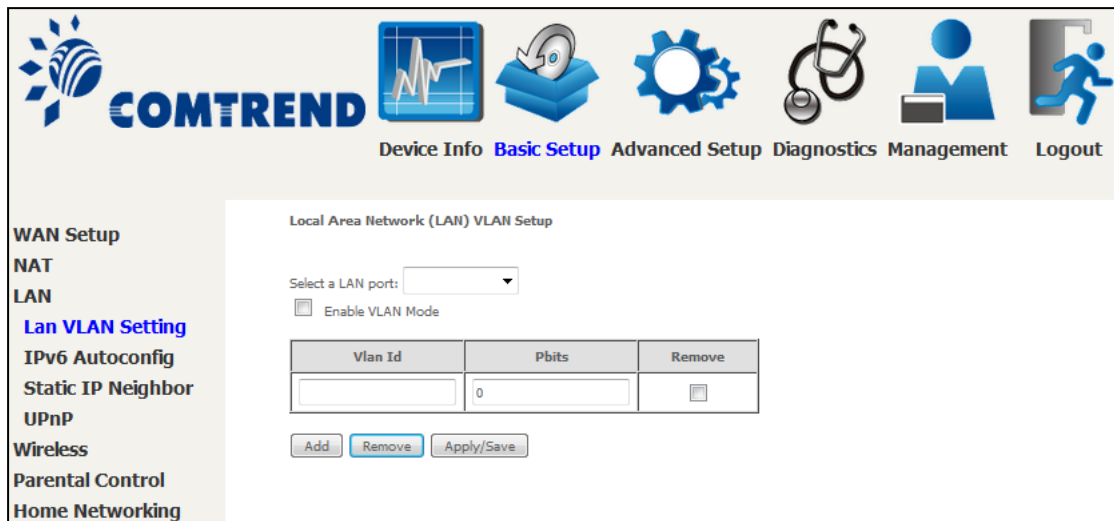
ETH1	Auto
ETH2	Auto
ETH3	10Mbps-Half
ETH4	10Mbps-Full
	100Mbps-Half
	100Mbps-Full

### 5.3.1 Lan VLAN Setting

The CPE will tag VLAN on a specific LAN port when this feature is used.



Click the Add button to display the following.



Heading	Description
Vlan Id	Define a specific VLAN ID for this LAN port
Pbits	Define priority bit for this LAN port

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

### 5.3.2 LAN IPv6 Autoconfig

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

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

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

**IPv6 LAN Auto Configuration**  
 Note: Stateless DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

**LAN IPv6 Link-Local Address Configuration**  
 EUI-64  
 User Setting  
 Interface Identifier: 0:0:0:1

**Static LAN IPv6 Address Configuration**  
 Interface Address (prefix length is required):

**IPv6 LAN Applications**  
 Enable DHCPv6 Server  
 Stateless  
 Refresh Time (sec): 14400  
 Stateful  
 Start interface ID: 0:0:0:2  
 End interface ID: 0:0:0:254  
 Leased Time (hour):  
 Static IP Lease List: (A maximum 32 entries can be configured)

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

Enable SLAAC (RADVD)  
 RA interval Min(sec): 3  
 RA interval Max(sec): 10  
 Reachable Time(ms): 0  
 Default Preference: Low  
 MTU (bytes): 1500  
 Enable Prefix Length Relay  
 Enable Configuration Mode  
 Enable ULA Prefix Advertisement  
 Randomly Generate  
 Statically Configure  
 Prefix:  
 Preferred Life Time (hour): -1  
 Valid Life Time (hour): -1  
 Enable MLD Snooping  
 Standard Mode  
 Blocking Mode  
 Enable MLD LAN to LAN Multicast: Disable  
 (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

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
<input type="button" value="Add Entries"/>		<input type="button" value="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"/>

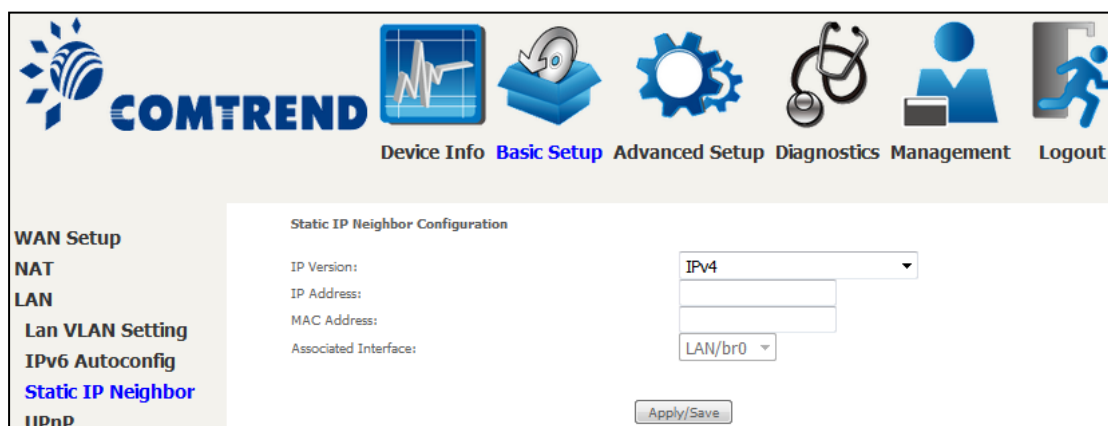
Heading	Description
<b>Enable RADVD</b>	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving 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 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

### 5.3.3 Static IP Neighbor

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



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



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

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

### 5.3.4 UPnP

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



The screenshot displays the COMTREND web interface. At the top left is the COMTREND logo. A navigation bar contains icons and labels for: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists: WAN Setup, NAT, LAN, Lan VLAN Setting, IPv6 Autoconfig, Static IP Neighbor, and UPnP (highlighted in blue). The main content area is titled "UPnP Configuration" and contains the following text: "NOTE: UPnP is activated only when there is a live WAN service with NAT enabled." Below this is a checkbox labeled "Enable UPnP" which is checked. At the bottom right of the configuration area is a button labeled "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.

**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

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMMF)

Enable WiFi Button

SSID:

BSSID:

Country:

Country RegRev:

Max Clients:



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

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMM	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.

Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (  or  ) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
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.
Enable WiFi Button	Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
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	Local regulations limit channel range: US/Canada = 1-11.
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.

The screenshot shows the Comtrend web interface for configuring wireless security. The navigation menu on the left includes: WAN Setup, NAT, LAN, Wireless (2.4GHz, Basic, Security, 5GHz), Parental Control, and Home Networking. The main content area is titled "Wireless -- Security" and contains the following configuration options:

- WPS Setup:**
  - Enable WPS: Disabled (dropdown menu)
- Manual Setup AP:**
  - Select SSID: ComtrendF613\_2.4GHz (dropdown menu)
  - Network Authentication: WPA2 -PSK (dropdown menu)
  - Protected Management Frames: Disabled (dropdown menu)
  - WPA/WAPI passphrase: [masked] (text input) [Click here to display](#)
  - WPA Group Rekey Interval: 3600 (text input)
  - WPA/WAPI Encryption: AES (dropdown menu)
  - WEP Encryption: Disabled (dropdown menu)

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

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

### 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

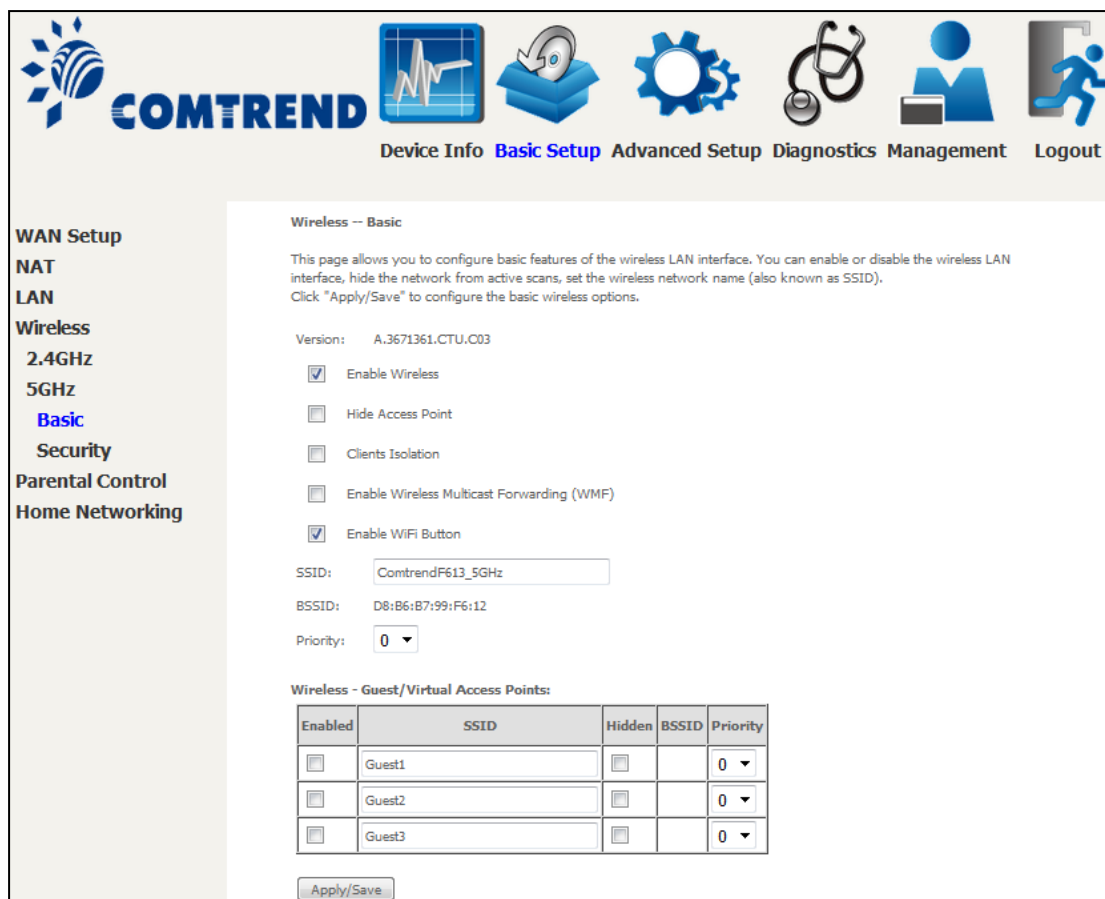
This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength 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.



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 view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (  or  ) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
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.

Option	Description
Enable Wireless Multicast Forwarding	Select the checkbox <input checked="" type="checkbox"/> to enable this function.
Enable WiFi Button	Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
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.
Priority	Sets priority level to SSID from 0-3. Packet flow with high priority SSID will be processed in advance if congestion occurs.
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, 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>

### 5.4.4 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.

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with icons and labels: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: WAN Setup, NAT, LAN, Wireless, 2.4GHz, 5GHz, Basic, Security (highlighted), Parental Control, and Home Networking. The main content area is titled "Wireless -- WPS Setup" and contains the following text and form elements:

Wireless -- WPS Setup

This page allows you to configure WPS features of the wireless LAN interface.

Enable WPS: Disabled

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: ComtrendF613\_5GHz

Encryption: WPA2-AES

Passphrase: [masked] [Click here to display](#)

Apply/Save

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.

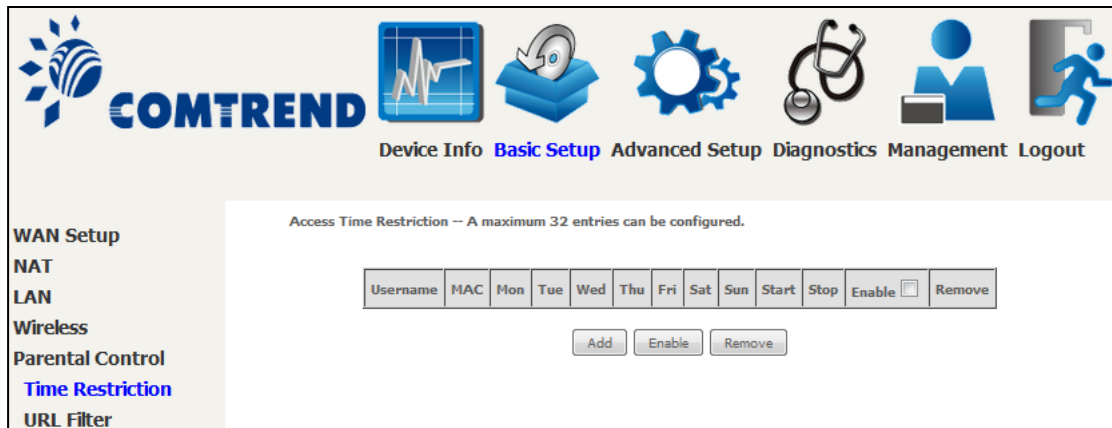
## 5.5 Parental Control

This selection provides WAN access control functionality.

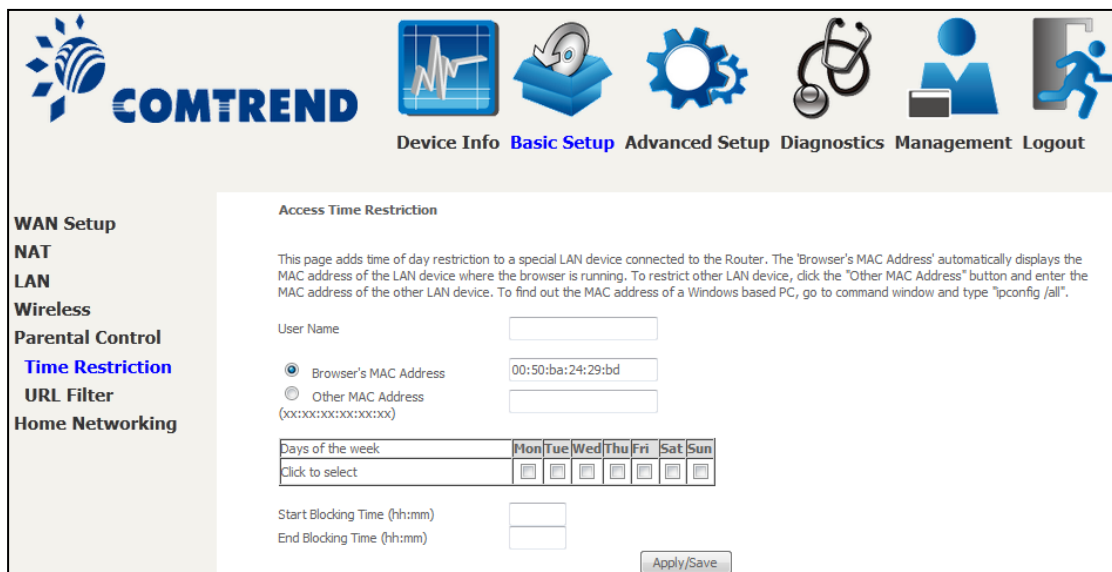
### 5.5.1 Time Restriction

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 8.5 Internet Time, so that the scheduled times match your local time.

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



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



See below for field descriptions. Click **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. At the top, there is a navigation bar with icons and labels: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various settings: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server (highlighted), DLNA, Storage Service, and USB Speed. The main content area is titled "Print Server settings" and contains the following text: "This page allows you to enable / disable printer support." Below this, there are three input fields labeled "Manufacturer", "Product", and "Serial Number". A checkbox labeled "Enable on-board print server." is present and unchecked. At the bottom right of the main content area, there is an "Apply/Save" button.

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. At the top, there is a navigation bar with icons and labels: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various settings: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA (highlighted), Storage Service, and USB Speed. The main content area is titled "Digital Media Server settings" and contains the following text: "This page allows you to enable / disable digital media server support." Below this, there is a checkbox labeled "Enable on-board digital media server." which is unchecked. At the bottom right of the main content area, there is an "Apply/Save" button.

### 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.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various settings: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA, Storage Service (highlighted), and USB Speed. The main content area is titled 'Samba Configuration for Storage Service' and contains three toggle switches: 'Samba Service' (set to Disable), 'Samba Security Mode' (set to Enable), and 'Samba Access from Internet' (set to Enable). Below these, a note states: 'Access to your USB storage devices via Samba is always active. You can access them in the following ways:' followed by a bullet point: 'Simply open your File Explorer and go to \\comtrend.' At the bottom, a table displays the details of attached USB storage devices.

Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	30517 MB	1492 MB	Safely remove

Display after storage device attached (for your reference).

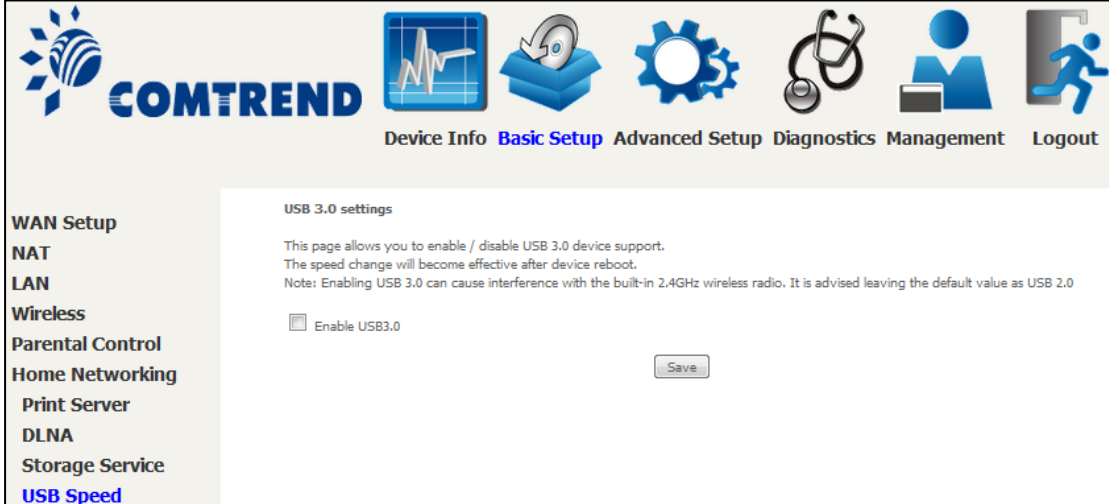
Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	30517 MB	1492 MB	Safely remove



## 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



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different settings: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA, Storage Service, and USB Speed (highlighted in blue). The main content area is titled "USB 3.0 settings" and contains the following text: "This page allows you to enable / disable USB 3.0 device support. The speed change will become effective after device reboot. 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". Below this text, there is a checkbox labeled "Enable USB3.0" which is currently unchecked. A "Save" button is located to the right of the checkbox.

## 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 screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the following items: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with the following items: **Auto-Detection** (highlighted), Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, and Interface Grouping. The main content area is titled 'Auto-detection setup' and contains the following text: '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.' Below this text is a checkbox labeled 'Enable auto-detect'. At the bottom right of the main content area, there are two buttons: 'Apply/Save' and 'Restart'.

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.

The screenshot shows the 'Advanced Setup' page for 'Auto-detection setup'. The navigation menu includes: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and 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:

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:

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

Buttons:

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 ▾

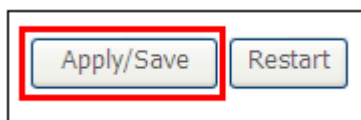
VPI[0-255]	VCI[32-65535]	Service
0	32	Disable ▾
0	32	PPPoE
0	32	PPPoA
0	32	IPoE
0	32	Disable
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Default Bridge ▾

**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.

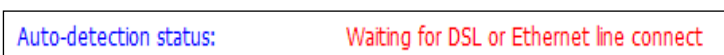
**Options for each WAN service:** These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

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

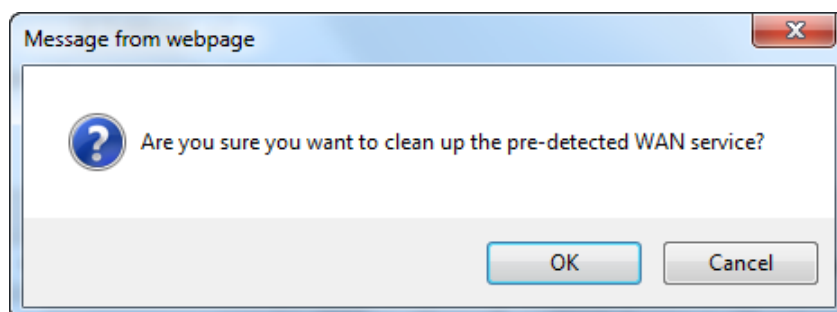
The Auto-detection status is used to display the real time status of the Auto-detection feature.



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.

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

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**.

**Add IP Filter -- Outgoing**

The screen allows you to create a filter rule to identify outgoing 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:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

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** Diagnostics Management Logout

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

**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

Add Remove

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** 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

Apply/Save

Consult the table below for field descriptions.



<b>Field</b>	<b>Description</b>
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** 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 3120 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.

**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	FORWARD	<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.

**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: LAN<=>WAN

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.

<b>Field</b>	<b>Description</b>
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.



The screenshot shows the COMTREND web interface for QoS configuration. The top navigation bar includes icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories, with **Quality of Service** selected. The main content area is titled 'QoS -- Queue Management Configuration' and contains the following text:

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note:** If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

**Note:** The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Select Default DSCP Mark:

### 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 un-checked will be disabled.  
 The enable-checkbox also shows status of the queue after page reload.

**Note: Ethernet LAN queue configuration only takes effect when all the queues of the interface have been configured.**

Name	Key	Interface	Qid	Prec/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"/>

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.

**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** Diagnostics Management Logout

**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:  [1-1000000 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 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

**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, w10)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in the Destination MAC Address.
<b>Classification Results</b>	
Specify Egress Interface	Choose the egress interface from the available list.
Specify Egress Queue	Choose the egress queue from the list of available for the specified egress interface.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. <ul style="list-style-type: none"> <li>- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.</li> <li>- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.</li> <li>- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.</li> <li>- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.</li> </ul>
Set Rate Limit	The data transmission rate limit in kbps.

### 6.3.3 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.

**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)
ETH1	LAN	-1	0
ETH2	LAN	-1	0
ETH3	LAN	-1	0
ETH4	LAN	-1	0

Apply/Save

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 displays the 'Default Gateway' configuration page in the COMTREND web interface. The page title is 'Routing -- Default Gateway'. A descriptive text explains that multiple WAN interfaces can be configured as default gateways, with priority order being important. The interface features two lists: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. Between these lists are two buttons: a right-pointing arrow (>) and a left-pointing arrow (<). Below the lists, there is a 'TODO: IPV6 \*\*\*\*\*' note and 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.

COMTREND

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

Routing -- Static Route (A maximum 32 entries can be configured)

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

Auto-Detection  
Security  
Quality of Service  
Routing  
Default Gateway  
**Static Route**  
Policy Routing  
RIP

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

COMTREND

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

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

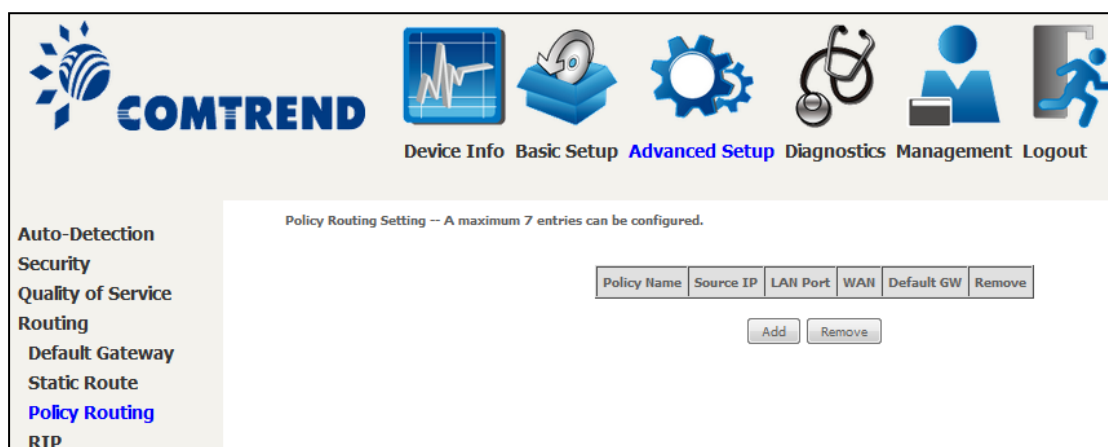
Auto-Detection  
Security  
Quality of Service  
Routing  
Default Gateway  
**Static Route**  
Policy Routing  
RIP  
DNS  
DSL  
DSL Bonding

- **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.

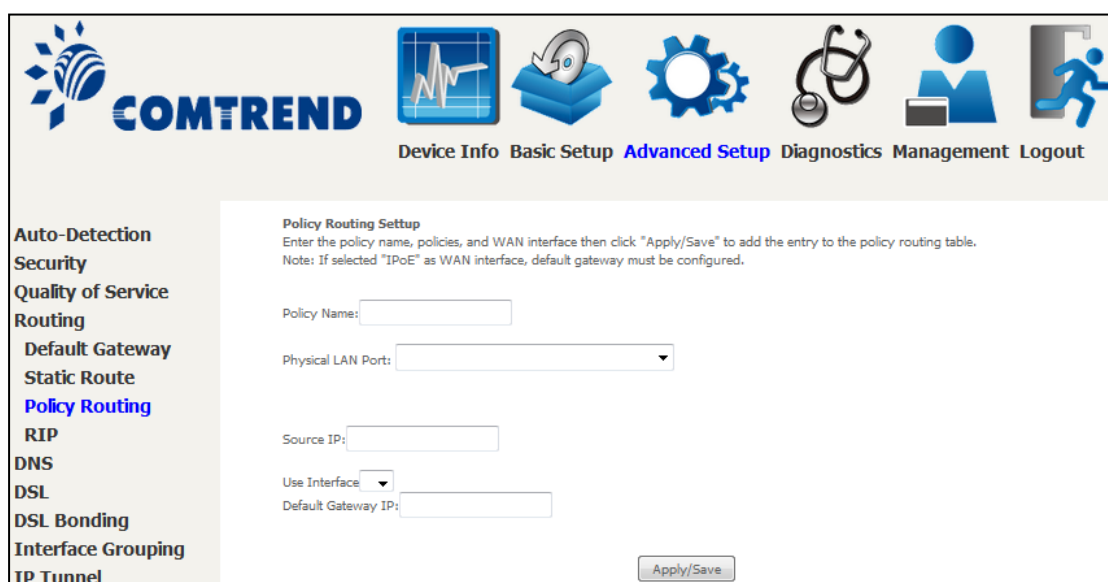
After completing the settings, click **Apply/Save** to add the entry to the routing table.

### 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 for RIP configuration. The navigation menu on the left includes: Auto-Detection, Security, Quality of Service, Routing (with sub-items: Default Gateway, Static Route, Policy Routing, and **RIP**), DNS, DSL, and DSL Bonding. The main content area is titled "Routing -- RIP Configuration" and contains the following text:

**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** Diagnostics Management Logout

**Auto-Detection**  
**Security**  
**Quality of Service**  
**Routing**  
**DNS**  
**DNS Server**  
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: [NO CONFIGURED INTERFACE]

Use the following Static IPv6 DNS address:

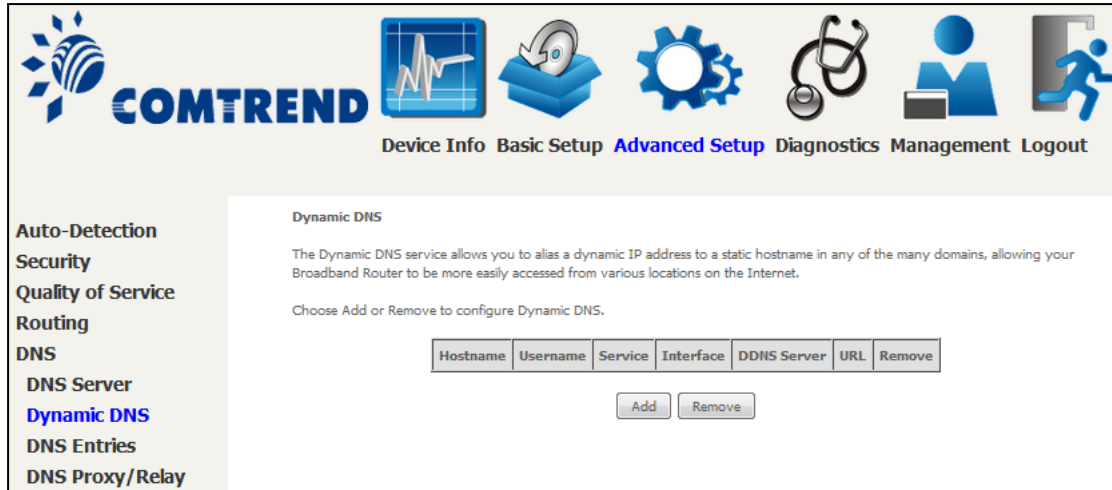
Primary IPv6 DNS server: [ ]  
Secondary IPv6 DNS server: [ ]

Apply/Save

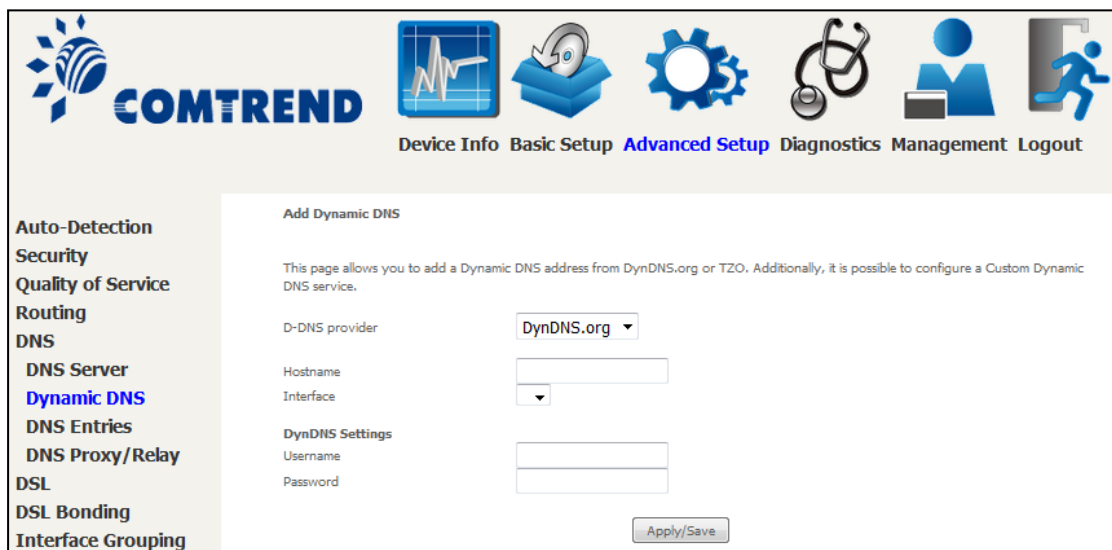
Click **Apply/Save** to save the new configuration.

## 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 3120 to be more easily accessed from various locations on the Internet.



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



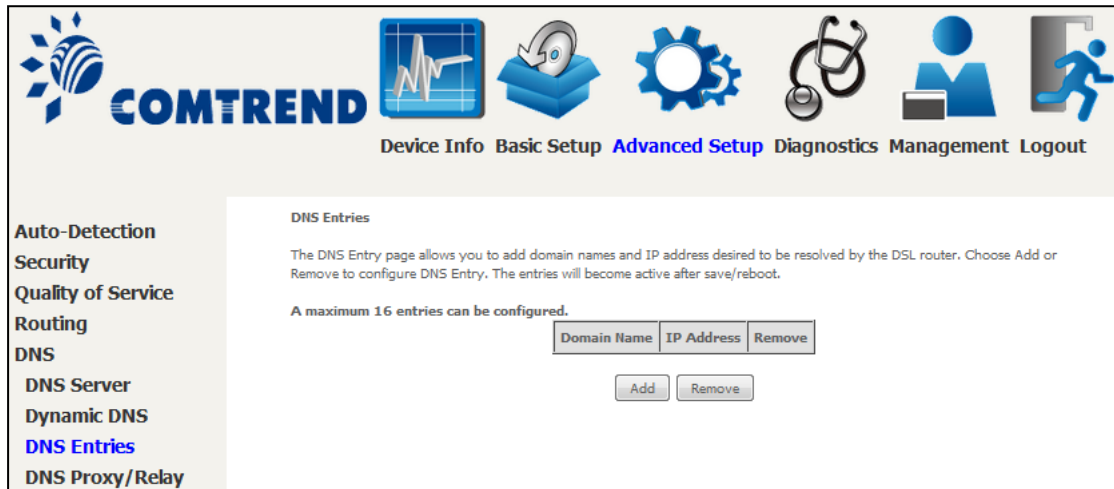
Click **Apply/Save** to save your settings.

Consult the table below for 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.



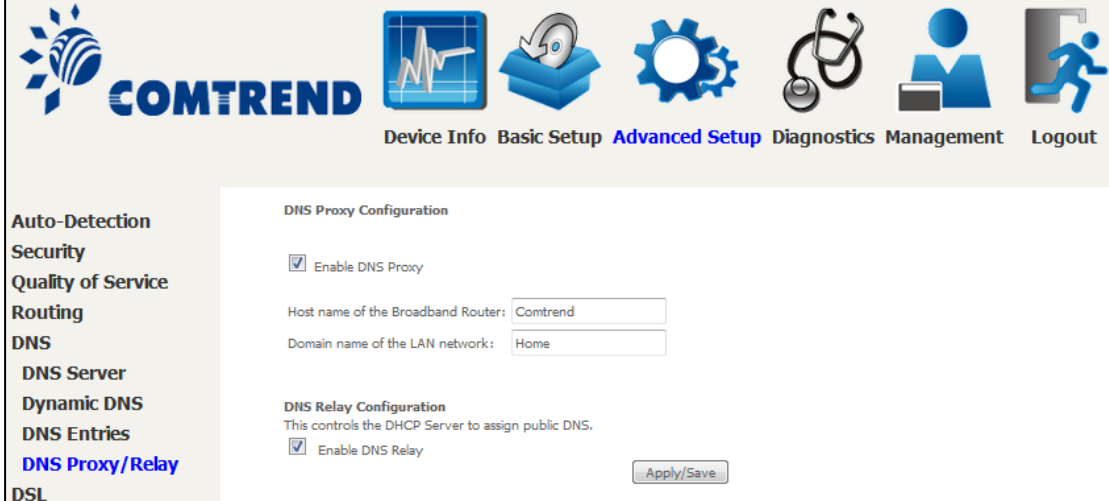
Choose Add or Remove to configure a DNS Entry. The entries will become active after save/reboot.



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

## 6.5.4 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".



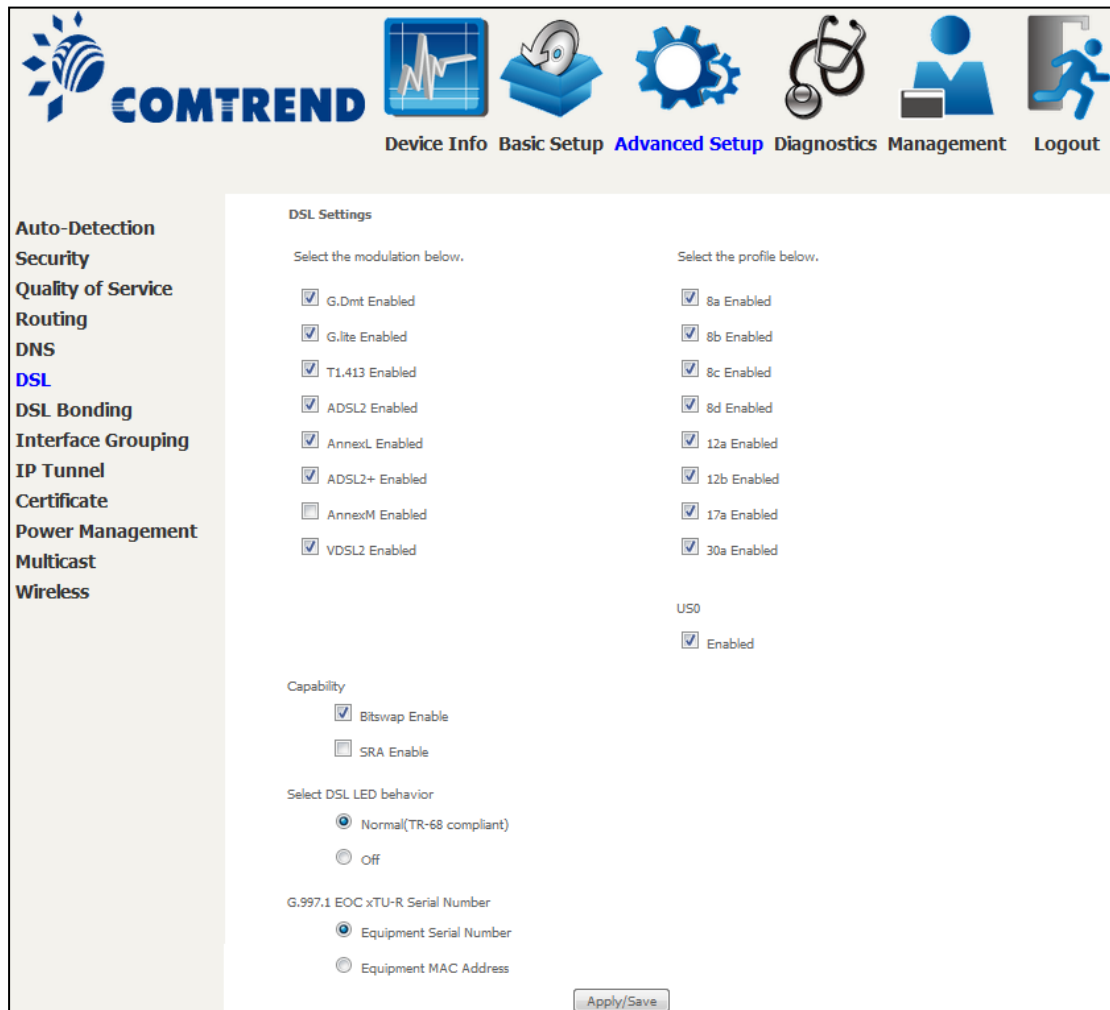
The screenshot displays the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several menu items: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. Below the navigation bar, a sidebar on the left lists various configuration categories: Auto-Detection, Security, Quality of Service, Routing, DNS, DNS Server, Dynamic DNS, DNS Entries, **DNS Proxy/Relay** (highlighted), and DSL. The main content area is titled "DNS Proxy Configuration" and contains the following settings:

- Enable DNS Proxy
- Host name of the Broadband Router:
- Domain name of the LAN network:
- DNS Relay Configuration**  
This controls the DHCP Server to assign public DNS.
- Enable DNS Relay
- 

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)
Select DSL LED behavior	Normal (TR-68 compliant): Select this option for DSL LED to operate normally (See menu 2.2 LED Indicator)  Off:DSL LED will always be OFF
G997.1 EOC xTU-R Serial Number	Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages

## 6.7 DSL Bonding

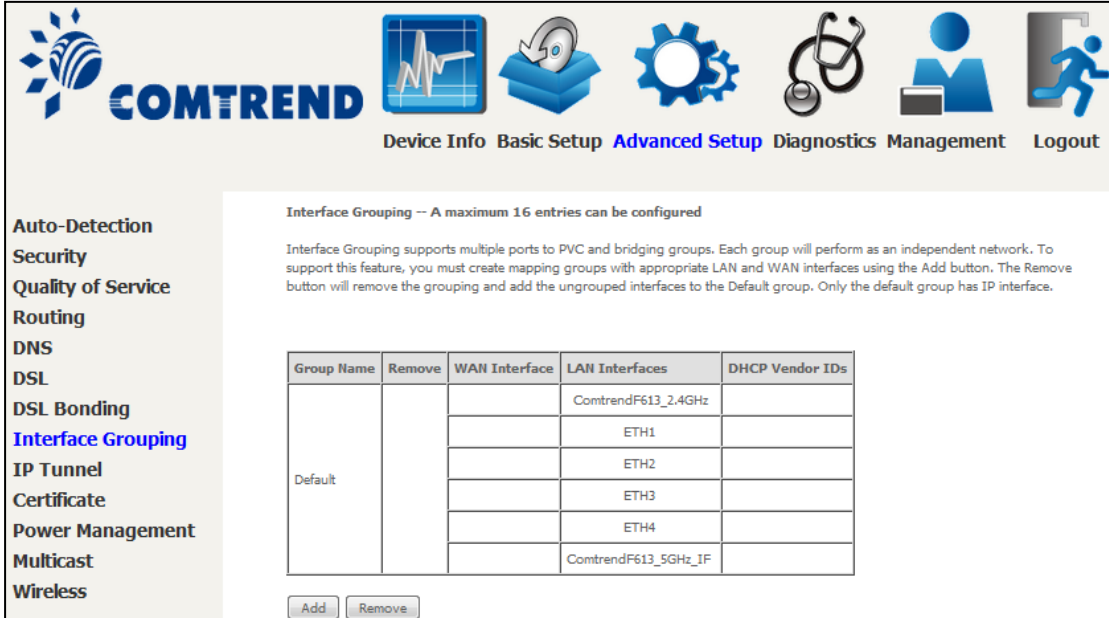
This page displays the bonding status of the connected xDSL line.

The screenshot shows the COMTREND web interface. At the top, there is a navigation menu with icons and labels: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. 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). The main content area displays the title 'xDSL Bonding Capability Configuration' and a status box indicating 'Current WAN xDSL Mode: Bonded'.

## 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. At the top, there is a navigation bar with icons and labels for: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left, a sidebar lists various settings 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, there is a descriptive paragraph: "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 row for the "Default" group, which has a "Remove" button, an empty "WAN Interface" field, and a "LAN Interfaces" field containing a list of interfaces: ComtrendF613\_2.4GHz, ETH1, ETH2, ETH3, ETH4, and ComtrendF613\_5GHz\_IF. The "DHCP Vendor IDs" field is empty.

At the bottom of the table, there are two buttons: "Add" and "Remove".

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



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' (which is highlighted), 'Diagnostics', 'Management', and 'Logout'. On the left side, there is a vertical menu with various configuration options: 'Auto-Detection', 'Security', 'Quality of Service', 'Routing', 'DNS', 'DSL', 'DSL Bonding', 'Interface Grouping' (highlighted in blue), 'IP Tunnel', 'Certificate', 'Power Management', 'Multicast', and 'Wireless'. The main content area is titled 'Interface grouping Configuration'. It contains instructions on how to create a new interface group, including steps for naming, selecting dynamic or static options, adding DHCP vendor IDs, and selecting interfaces. Below the instructions, there is a 'Group Name' input field. There are two sets of interface selection boxes: 'Grouped WAN Interfaces' and 'Available WAN Interfaces' (both empty), and 'Grouped LAN Interfaces' and 'Available LAN Interfaces'. The 'Available LAN Interfaces' list includes: ETHWAN, ETH1, ETH2, ETH3, ETH4, ComtrendF613\_5GHz\_IF, ComtrendF613\_2.4GHz, wl0\_Guest1, wl0\_Guest2, and wl0\_Guest3. At the bottom, there are three input fields for 'Automatically Add Clients With the following DHCP Vendor IDs' and an 'Apply/Save' button.

**Automatically Add Clients With Following DHCP Vendor IDs:**

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

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

The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and ETH4.
2. Video: nas\_0\_36, nas\_0\_37, and nas\_0\_38. The DHCP vendor ID is "Video".

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

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

1. Default: ETH2, ETH3, and ETH4
2. Video: nas\_0\_36, nas\_0\_37, nas\_0\_38, and ETH1.

## 6.9 IP Tunnel

### 6.9.1 IPv6inIPv4

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

COMTREND

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
**IPv6inIPv4**  
IPv4inIPv6

IP Tunneling -- 6in4 Tunnel Configuration

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

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

COMTREND

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
**IPv6inIPv4**  
IPv4inIPv6  
Certificate  
Power Management

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual  Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

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

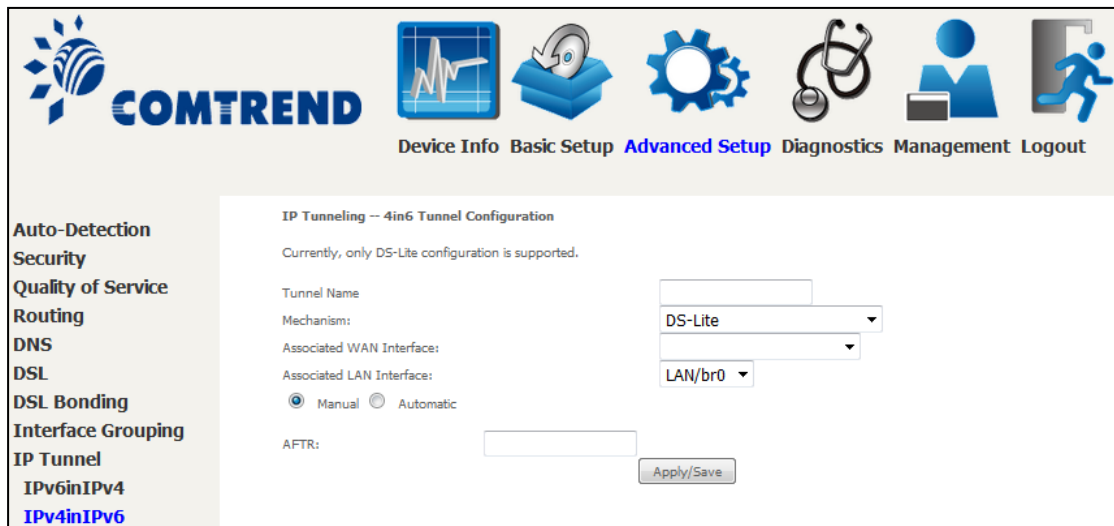
Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for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

### 6.9.2 IPv4inIPv6

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



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



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

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

## 6.10 Certificate

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

### 6.10.1 Local

### CREATE CERTIFICATE REQUEST

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

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.

The following table is provided for your reference.

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

### IMPORT CERTIFICATE

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

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

## 6.10.2 Trusted CA

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

COMTREN

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
Certificate  
Local  
**Trusted CA**

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action

Import Certificate

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

COMTREN

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

Auto-Detection  
Security  
Quality of Service  
Routing  
DNS  
DSL  
DSL Bonding  
Interface Grouping  
IP Tunnel  
Certificate  
Local  
**Trusted CA**  
Power Management  
Multicast

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Apply

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

## 6.11 Power Management

This screen allows for control of hardware modules to evaluate power consumption. Use the buttons to select the desired option, click **Apply** and check the response.

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

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

**Power Management**

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

**Host CPU Clock divider when Idle**  
 Enable Status: **Enabled**

**Wait instruction when Idle**  
 Enable Status: **Enabled**

**Energy Efficient Ethernet**  
 Enable Status: **Enabled**

**Ethernet Auto Power Down and Sleep**  
 Enable Status: **Enabled**

Apply refresh



## 6.12 Multicast

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

The screenshot shows the COMTREND web interface with a navigation bar at the top containing icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. A left sidebar lists various configuration categories, with **Multicast** highlighted in blue. The main content area is titled 'Multicast' and contains the following sections:

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

Group Address	Mask/Mask bits	Remove
224.0.0.0	255.255.255.0	<input type="checkbox"/>
239.255.255.250	255.255.255.255	<input type="checkbox"/>
224.0.255.135	255.255.255.255	<input type="checkbox"/>
- MLD Configuration:** A section with the instruction 'Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.' and several input fields:
  - Default Version: 2
  - Query Interval: 125
  - Query Response Interval: 10
  - Last Member Query Interval: 10
  - Robustness Value: 2
  - Maximum Multicast Groups: 10
  - Maximum Multicast Data Sources (for mldv2): 10
  - Maximum Multicast Group Members: 10
  - Fast Leave Enable:
- MLD Group Exception List:** A table with columns 'Group Address', 'Mask/Mask bits', and 'Remove'. It contains three rows of data and an 'Add' button at the bottom right.
 

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

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

### Multicast Precedence:

Select precedence of multicast packets.

**Multicast Strict Grouping Enforcement:**

Enable/Disable multicast strict grouping.

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

**IGMP Group Exception List**

Group addresses which are excluded from IGMP service.

## 6.13 Wireless

### 6.13.1 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.

**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

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMM)

Enable WiFi Button

SSID:

BSSID:

Country:

Country RegRev:



Max Clients:

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

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMM	Max Clients	BSSID
<input type="checkbox"/>	w10_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A
<input type="checkbox"/>	w10_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A
<input type="checkbox"/>	w10_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A

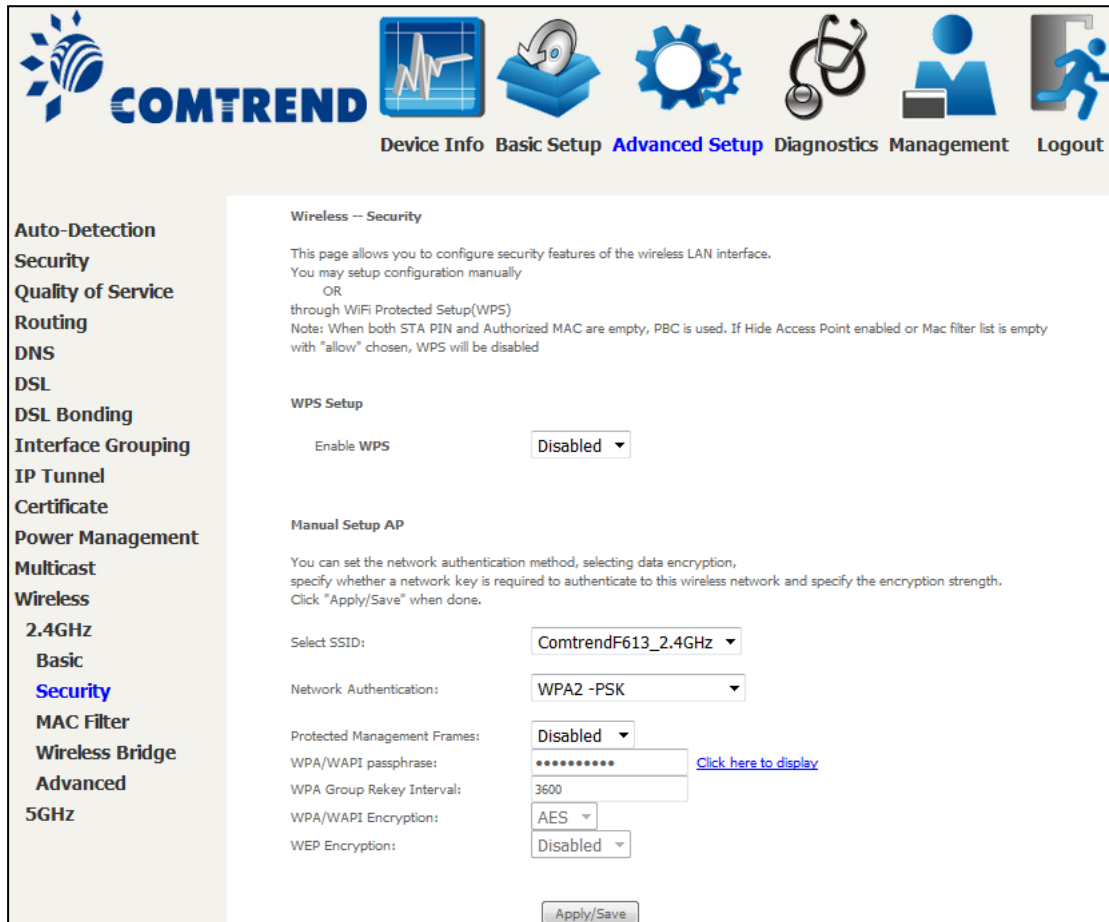
Click **Apply/Save** to configure the basic wireless options.

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 view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (  or  ) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
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.
Enable WiFi Button	Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
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: 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>

### 6.13.2 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.

Different authentication type pops up different settings requests.

Choosing **802.1X**, enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key.

Also, enable WEP Encryption and select Encryption Strength.

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

Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

### 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.

### 6.13.3 WPS 2.4GHz

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The NexusLink 3120 has a WPS button on the device.

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



**NOTE:** WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below.

#### I. Setup

**Step 1:** Enable WPS by selecting **Enabled** from the drop down list box shown.

 A screenshot of a web interface titled 'WPS Setup'. It features a label 'Enable WPS' followed by a dropdown menu currently displaying 'Enabled' with a downward arrow.

**Step 2:** Set the WPS AP Mode. **Configured** is used when the NexusLink 3120 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the NexusLink 3120.

 A screenshot of a web interface titled 'Set WPS AP Mode'. It features a dropdown menu currently displaying 'Configured' with a downward arrow.

**NOTES:** Your client may or may not have the ability to provide security settings to the NexusLink 3120. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

## IIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the front panel of the router can be used for this purpose.

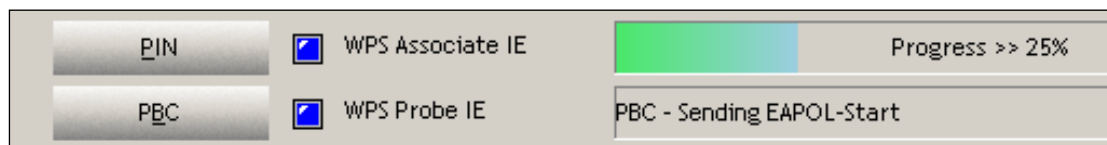
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

**NOTE:** The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 4, return to Step 3.

### Step 3: Press WPS button

Press the WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

**Step 4:** Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



Now go to Step 7 (part III. Check Connection) to check the WPS connection.

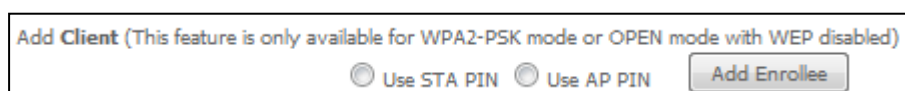
## IIb. WPS – PIN CONFIGURATION

Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

**Step 3:** Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

**A - For Configured mode, click the Add Enrollee button.**





**Enter STA PIN:** a Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be inputted at representing the network, usually the Access Point of the network.

Use STA PIN  Use AP PIN  Add Enrollee

12345678 [Help](#)

**B** - For **Unconfigured** mode, select Unconfigured from the Set WPS AP mode drop-down menu and click the **Apply/Save** button. Input the Device PIN displayed to your wireless client to initiate the PIN connection.

Set WPS AP Mode Unconfigured ▼

Setup AP (Configure all security settings with an external registrar)

Lock Device PIN Enable

Device PIN 38112034 [Help](#)

**Step 4:** Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

The figure below provides an example of a WPS client PIN function in-progress.

PIN  WPS Associate IE [Progress Bar]

PBC  WPS Probe IE PIN - Sending EAP-Rsp(ID)

**III. CHECK CONNECTION**

**Step 5:** If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.

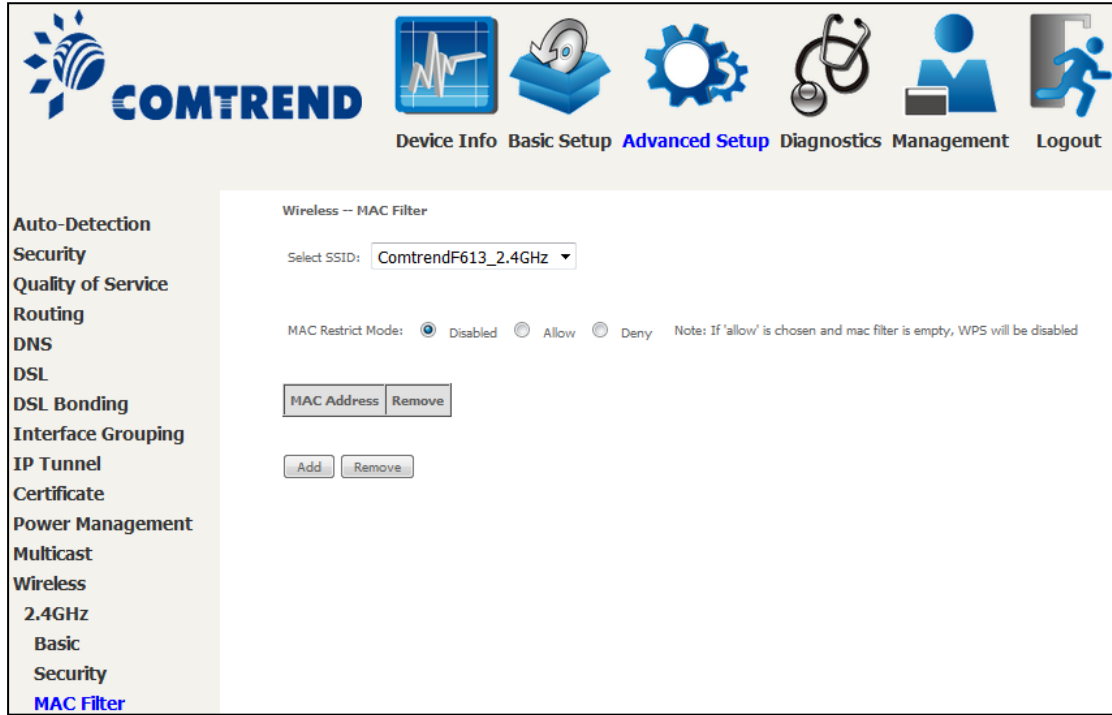
PIN  WPS Associate IE [Full Progress Bar]

PBC  WPS Probe IE WPS status is connected successfully

You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.


### 6.13.4 MAC Filter 2.4GHz

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.



Option	Description
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 user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.

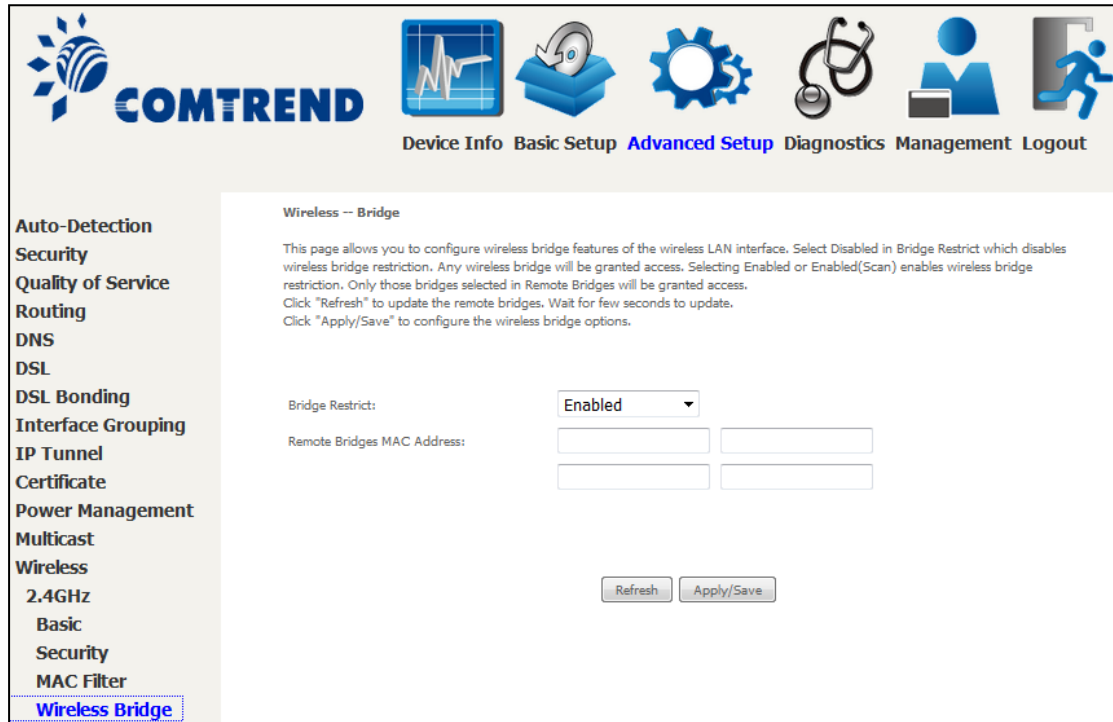


The screenshot displays the COMTREND web interface. At the top left is the COMTREND logo. To its right is a navigation bar with icons and labels: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, 2.4GHz, Basic, Security, and **MAC Filter**. The main content area is titled "Wireless -- MAC Filter" and contains the instruction: "Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters." Below this instruction is a text input field labeled "MAC Address:" and an "Apply/Save" button.

Enter the MAC address in the box provided and click **Apply/Save**.

### 6.13.5 Wireless Bridge 2.4GHz

This screen allows for the configuration of wireless bridge features of the WiFi interface. See the table below for detailed explanations of the various options.



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

Feature	Description
Bridge Restrict	Selecting <b>Disabled</b> disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting <b>Enabled</b> or <b>Enabled (Scan)</b> enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click <b>Refresh</b> to update the station list when Bridge Restrict is enabled.
Remote Bridges MAC Address	Enter the list of MAC addresses allowed to act as wireless bridge clients.

### 6.13.6 Advanced 2.4GHz

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Apply/Save** to set new advanced wireless options.

Field	Description
Band	Supports both 2.4GHz and 5GHz bands. NL-3120 adapts to all 802.11x series, up to the latest 802.11ac standard. Legacy client devices may support only 2.4GHz, 5GHz or both.
Channel	Drop-down menu that allows selection of a specific channel.

Field	Description
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20MHz or 40MHz bandwidth. 40MHz bandwidth uses two adjacent 20MHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40MHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g client's access to the router.
RIFS Advertisement	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in 802.11a or g.
OBSS Co-Existence	Co-existence between 20 MHz AND 40 MHz overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.

Field	Description
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.
Band Steering	Enable band steering for dual band traffic control if applicable.
Enable Traffic Scheduler	Enable traffic scheduler to ensure wireless traffic is shared based on scheduler scheme.
Airtime Fairness	Enable airtime fairness for varied wireless clients.

### 6.13.7 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 restrict the channel set based on country requirements.

Click **Apply/Save** to configure the basic 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.



Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (  or  ) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
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.
Enable Wireless Multicast Forwarding	Select the checkbox <input checked="" type="checkbox"/> to enable this function.
Enable WiFi Button	Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
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.
Priority	Sets priority level to SSID from 0-3. Packet flow with high priority SSID will be processed in advance if congestion occurs.
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, 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>

### 6.13.8 WPS 5GHz

Refer to [6.13.3](#) for WPS setup procedure.

WPS can be disabled / enabled by selecting the corresponding option and click **"Apply/Save"**

**Wireless -- WPS Setup**

This page allows you to configure WPS features of the wireless LAN interface.

Enable **WPS** Disabled ▼

- A. When enabled in configured mode, use Push button or PIN to allow client connection.

**Wireless -- WPS Setup**

This page allows you to configure WPS features of the wireless LAN interface.

Enable **WPS** Enabled ▼

Set **WPS AP Mode** Configured ▼

To activate Push button, click on the "Add Enrollee PBC" button or use the 5G Wifi On/Off & WPS button on the front panel.

**Add Client**

Push-Button

Enter STA PIN

\* Personal Identification Number (PIN) has to be read from either a sticker or the display on the client wireless device.

- B. When enabled in unconfigured mode, input the Device PIN displayed to your wireless client to initiate the PIN connection.

### Wireless -- WPS Setup

This page allows you to configure WPS features of the wireless LAN interface.

Enable WPS

Set WPS AP Mode

Add Client

Push-Button

Enter STA PIN

Setup AP (Configure all security settings with an external registrar)

Device PIN  [Help](#)

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Encryption:

Passphrase:  [Click here to display](#)

### 6.13.9 MAC Filter 5GHz

This page is used to set allowed MAC addresses, and click the associated button for each interface to enable/disable the MAC address control.

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**, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with various configuration options, including Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, 2.4GHz, 5GHz, Basic, Security, and **MAC Filter**. The main content area is titled "Wireless -- MAC Filter" and includes a "Select SSID:" dropdown menu set to "ComtrendF613\_5GHz". Below this, there are three radio buttons for "MAC Restrict Mode": Disabled (selected), Allow, and Deny. There is a table with one row containing a "MAC Address" and a "Remove" button. At the bottom of the table, there are "Add" and "Remove" buttons.

After clicking the **Add** button, the following screen appears.

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**, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with various configuration options, including Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, 2.4GHz, 5GHz, Basic, Security, and **MAC Filter**. The main content area is titled "Wireless -- MAC Filter" and includes a text input field for "MAC Address:" and an "Apply/Save" button. Above the input field, there is a message: "Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters."

Enter the MAC address in the box provided and click **Apply/Save**.

### 6.13.10 Wireless Bridge 2.4GHz

This page allows you to configure wireless bridge features of the wireless LAN interface.

Click the checkbox, enter the corresponding MAC address of the designated wireless devices and click **Apply/Save** to apply the wireless bridge settings.

Feature	Description
MAC Address	MAC address of the other wireless station
Passphrase	Passphrase of the other wireless station
VLAN	Assign VLAN Group to this bridge
RSSI	received signal strength of the other station

### 6.13.11 Advanced 5GHz

This page allows you to configure advanced features of the wireless LAN interface. Click **Apply/Save** to configure the basic wireless options.

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**, Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, Wireless, 2.4GHz, 5GHz, Basic, Security, MAC Filter, Wireless Bridge, and **Advanced**. The main content area is titled 'Wireless -- Advanced' and contains the following configuration options:

- Band:** 5GHz (dropdown menu)
- Channel:** (dropdown menu) Current Channel: 48 (interference: acceptable)
- Bandwidth:** 20MHz (dropdown menu)
- DTIM Interval:** (text input field)
- Beacon Interval:** (text input field)
- Beamforming Transmission:** Disabled (dropdown menu)
- Apply/Save** button

Field	Description
Band	Supports both 2.4GHz and 5GHz bands. NL-3120 adapts to all 802.11x series, up to the latest 802.11ac standard. Legacy client devices may support only 2.4GHz, 5GHz or both.
Channel	Drop-down menu that allows selection of a specific channel.
Bandwidth	Select the bandwidth used on the 5G interface. 80MHz is selected by default.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Field	Description
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Beamforming Transmission	Enable beamforming signal enhance for wireless transmission.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

## Chapter 7 Diagnostics

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



### 7.1 Diagnostics – Individual Tests

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

**LAN**

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:99:f6:13
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254

**Device**

Model	NexusLink 3120
Serial Number	15B3120UAXF-AA000213
Firmware Version	PJ11-416CTU-C07_R04-A2pvbH042u.d26q
Bootloader (CFE) Version	1.0.38-118.3-1
Up Time	1 hours:45 mins:59 secs
System Log	<a href="#">Show</a>

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

**Diagnostics**

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

Test the connection to your local network

Test your ETHWAN Connection:	FAIL	<a href="#">Help</a>
Test your ETH1 Connection:	PASS	<a href="#">Help</a>
Test your ETH2 Connection:	FAIL	<a href="#">Help</a>
Test your ETH3 Connection:	FAIL	<a href="#">Help</a>
Test your ETH4 Connection:	FAIL	<a href="#">Help</a>
Test your 2.4GHz Wireless Connection:	PASS	<a href="#">Help</a>
Test your 5GHz Wireless Connection:	PASS	<a href="#">Help</a>

[Rerun Diagnostic Tests](#)

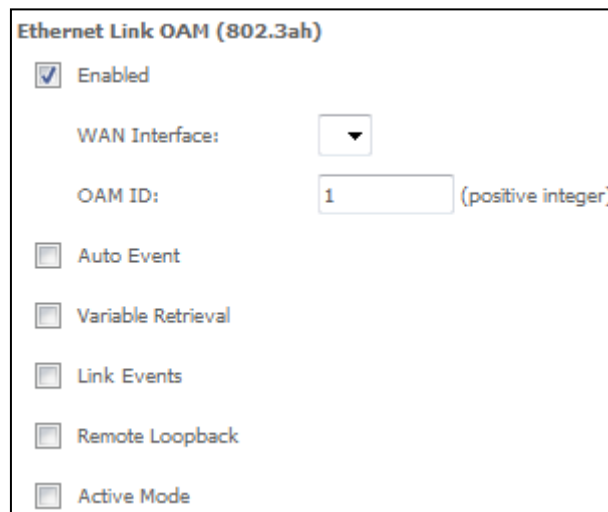


## 7.2 Ethernet OAM

The Ethernet OAM page provides settings to enable/disable 802.3ah, 802.1ag/Y1.731 OAM protocols.



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



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

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

Enabled  802.1ag  Y.1731

WAN Interface:

MD Level:  [0-7]

MD Name:  [e.g. Broadcom]

MA ID:  [e.g. BRCM]

Local MEP ID:  [1-8191]

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

CCM Transmission

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

**Loopback and Linktrace Test**

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

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

<b>Loopback Result:</b>	N/A			
<b>Linktrace Result:</b>	N/A			

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

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

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

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

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

## 7.3 Uptime Status

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

**COMTREND**

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

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

**Uptime Status**

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

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

System Up Time 13 mins:33 secs

DSL Group:

DSL Up Time Not Connected

ClearAll

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

## 7.4 Ping

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



**COMTREND**

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

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

**Ping**

Send ICMP ECHO\_REQUEST packets to network hosts.

Ping IP Address / Hostname:

PING 192.168.1.1 (192.168.1.1): 56 data bytes  
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.239 ms  
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.144 ms  
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.145 ms  
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.147 ms

--- 192.168.1.1 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max = 0.144/0.168/0.239 ms

## 7.5 Trace Route

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



The screenshot displays the COMTREND web interface. At the top, the COMTREND logo is on the left, and a navigation menu is on the right with icons for Device Info, Basic Setup, Advanced Setup, **Diagnostics**, Management, and Logout. The **Diagnostics** menu is expanded on the left side, listing options: Diagnostics, Ethernet OAM, Uptime Status, Ping, and **TraceRoute**. The main content area shows the TraceRoute tool interface. It includes the title "TraceRoute", a description "Trace the route ip packets follow going to 'host'", a text input field for "TraceRoute IP Address / Hostname:", and a "TraceRoute" button. Below the input field, the command "traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets" is shown, followed by the output "1 192.168.1.1 (192.168.1.1) 0.217 ms".

## Chapter 8 Management

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



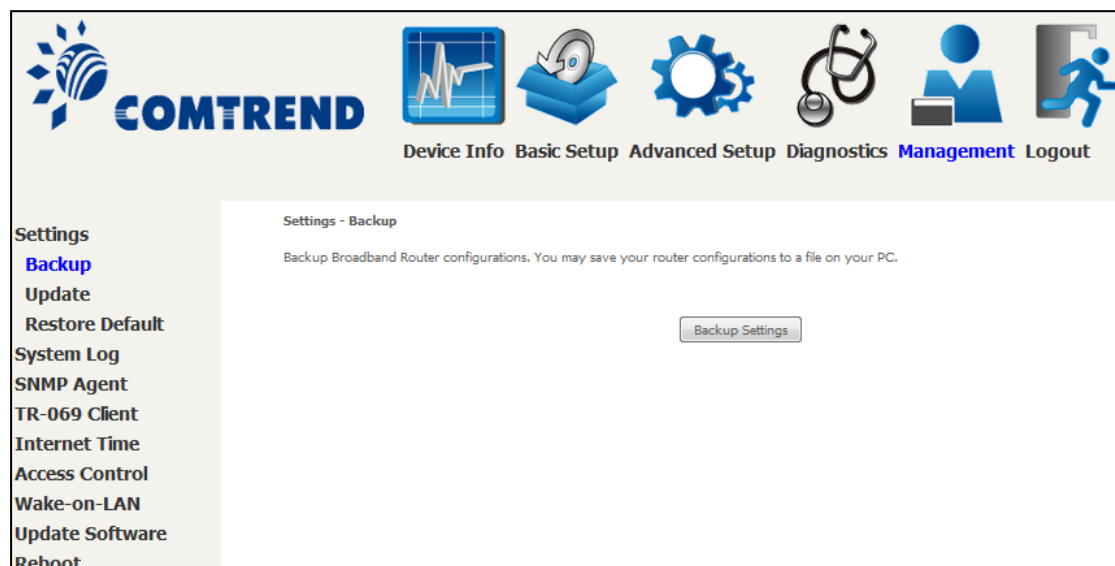
The Management menu has the following maintenance functions and processes:

### 8.1 Settings

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

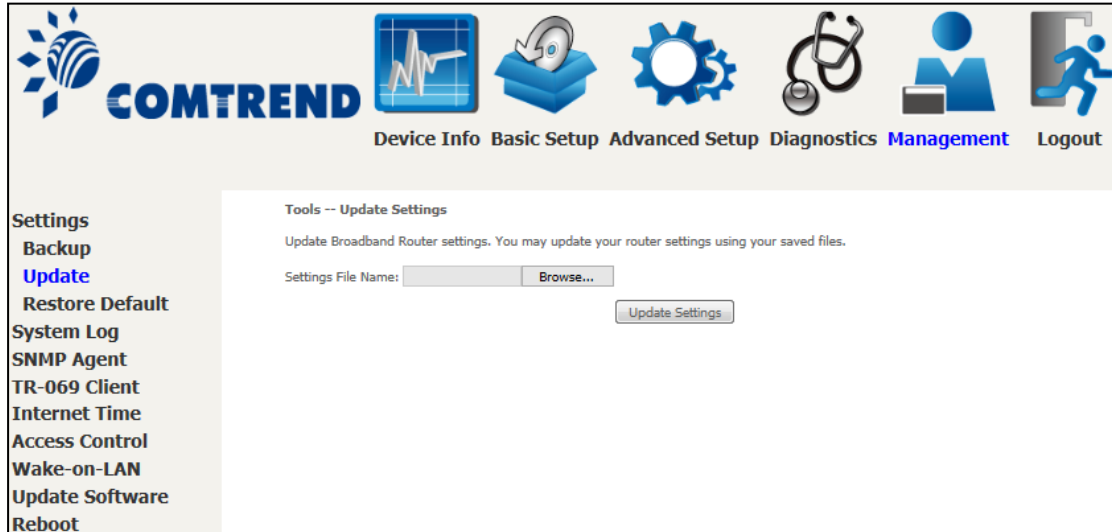
#### 8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



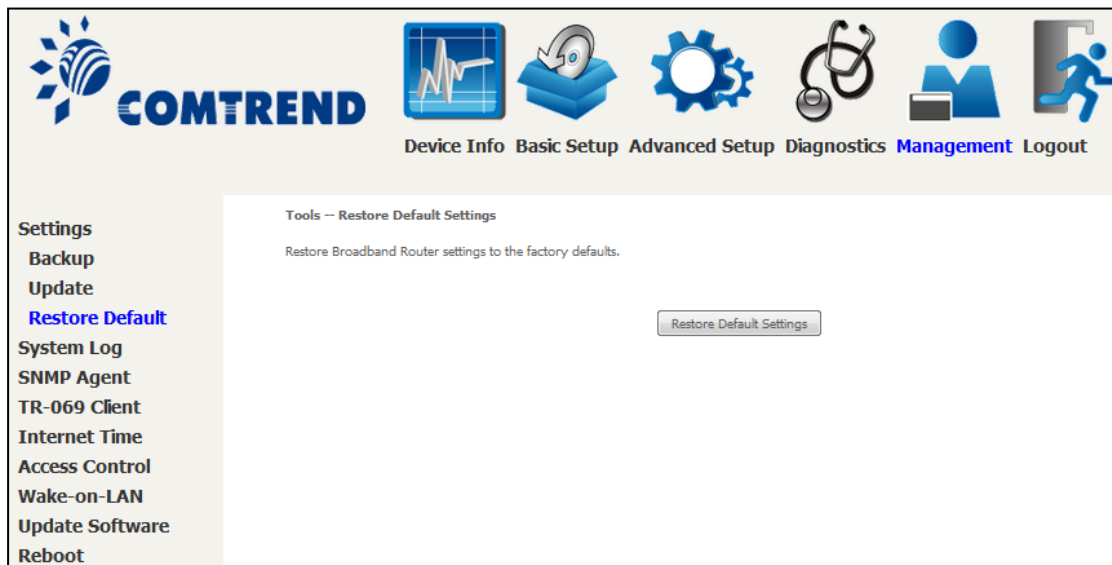
### 8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse...** to search for the file, then click **Update Settings** to recover settings.



### 8.1.3 Restore Default

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



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

#### DSL Router Restore

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

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

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

**NOTE:** This entry has the same effect as the **Reset** button. The NexusLink 3120 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase all configuration data saved in flash memory and enter bootloader mode.

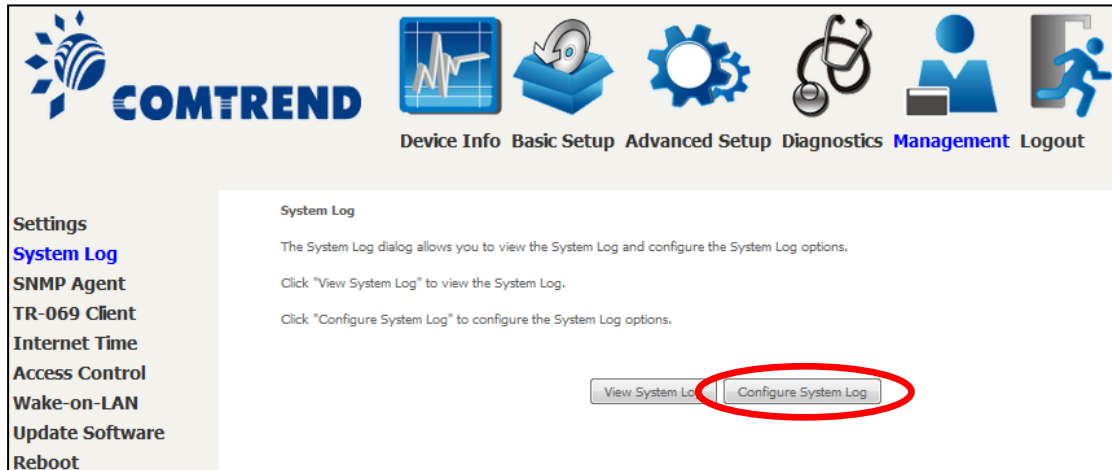


## 8.2 System Log

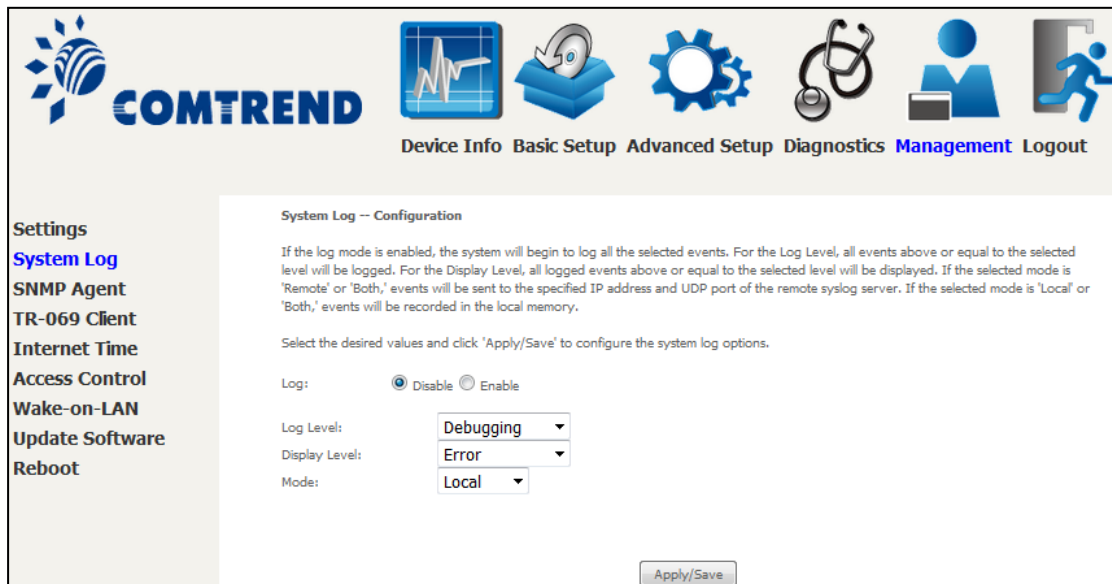
This function allows a system log to be kept and viewed upon request.

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

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



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



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

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

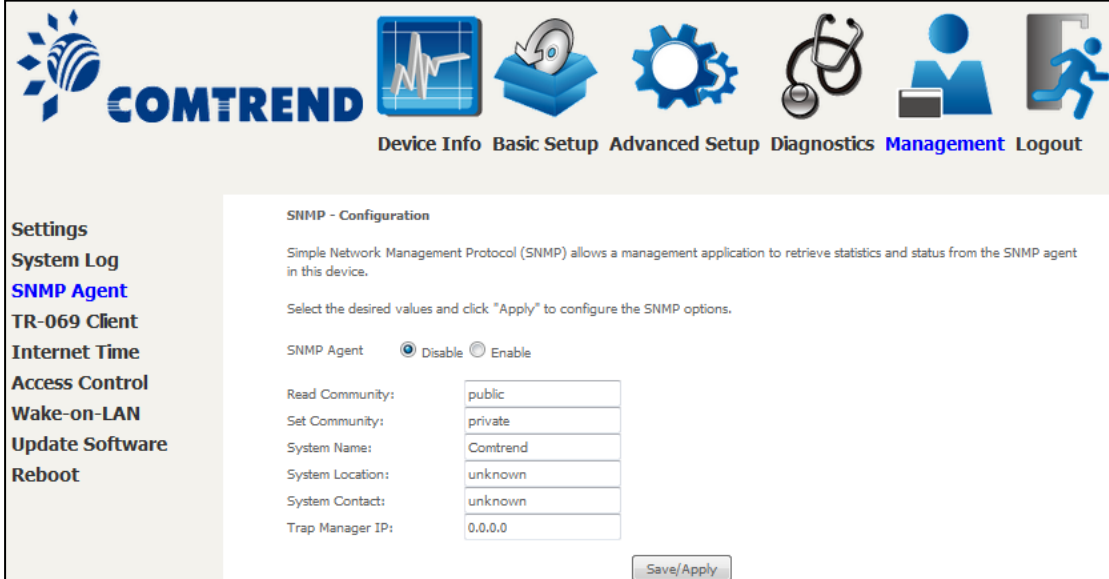
Option	Description
Log Level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the NexusLink 3120 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> <li>• Emergency = system is unusable</li> <li>• Alert = action must be taken immediately</li> <li>• Critical = critical conditions</li> <li>• Error = Error conditions</li> <li>• Warning = normal but significant condition</li> <li>• Notice= normal but insignificant condition</li> <li>• Informational= provides information for reference</li> <li>• Debugging = debug-level messages</li> </ul> <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	<p>Allows the user to select the logged events and displays on the <b>View System Log</b> window for events of this level and above to the highest Emergency level.</p>
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

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

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

## 8.3 SNMP Agent

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



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different sections: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (highlighted in blue), and Logout. Below the navigation bar, the main content area is titled "SNMP - Configuration". It contains a brief description of SNMP and instructions to select values and click "Apply". The configuration options are as follows:

SNMP Agent	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Read Community:	public
Set Community:	private
System Name:	Comtrend
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

A "Save/Apply" button is located at the bottom right of the configuration area. On the left side of the interface, there is a sidebar menu with the following items: Settings, System Log, **SNMP Agent** (highlighted in blue), TR-069 Client, Internet Time, Access Control, Wake-on-LAN, Update Software, and Reboot.

## 8.4 TR-069 Client

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

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

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

**TR-069 client - Configuration**

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

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

Enable TR-069

OUI-serial:  MAC  Serialnumber  
 Inform:  Disable  Enable

Inform Interval: 300  
 ACS URL:  
 ACS User Name: admin  
 ACS Password: \*\*\*\*\*

WAN Interface used by TR-069 client:  Any\_WAN  LAN  Loopback

Connection Request Authentication

Connection Request User Name: admin  
 Connection Request Password: \*\*\*\*\*  
 Connection Request URL:

Enable STUN Client

STUN Server Address:  
 STUN Server Port: 0  
 STUN Server User Name:  
 STUN Server Password:  
 STUN Server Maximum Keep Alive Period: 0  
 STUN Server Minimum Keep Alive Period: 0

Apply/Save Send Inform

The table below is provided for ease of reference.

Option	Description
Enable TR-069	Tick the checkbox <input checked="" type="checkbox"/> to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with ACS or select serial number to use router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.

Option	Description
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
<b>Connection Request</b>	
Authentication	Tick the checkbox <input checked="" type="checkbox"/> to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to router.
<b>Enable STUN Client</b>	
STUN Server Address	IP address of the STUN server.
STUN Server Port	Service port of the STUN server.
STUN Server User Name	Account to link to the STUN server.
STUN Server Password	Password of said account to link to the STUN server.
STUN Server Maximum Keep Alive Period	Maximum period to wait for a packet to be received from the STUN server to keep the link alive.
STUN Server Minimum Keep Alive Period	Minimum period to send a packet to the STUN server to keep the link alive.

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

## 8.5 Internet Time

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

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

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

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

Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov  
 Second NTP time server: ntp1.tummy.com  
 Third NTP time server: None  
 Fourth NTP time server: None  
 Fifth NTP time server: None

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

Apply/Save

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


## 8.6 Access Control







### 8.6.1 Accounts

This screen is used to configure the user account access passwords for the device. Access to the NexusLink 3120 is controlled through the following user accounts:

- The root account has unrestricted access to view and change the configuration of your Broadband router.
- The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.
- The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.
- The apuser account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure wireless settings.

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



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

**Settings**

System Log

SNMP Agent

TR-069 Client

Internet Time

Access Control

Accounts

Services

IP Address

Wake-on-LAN

Update Software

Reboot

**Access Control -- Accounts/Passwords**

By default, access to your Broadband router is controlled through three user accounts: root,support,and user.

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

The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.

The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.

Use the fields below to update passwords for the accounts, add/remove accounts (max of 5 accounts). Note: Passwords may be as long as 16 characters but must not contain a space.

Select an account:

Create an account:

Old Password:

New Password:

Confirm Password:

---

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

Feature	root	support	user	apuser
Account access	Both	None ▾	None ▾	None ▾
Add/Remove WAN	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wireless - Basic	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wireless - Advanced	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LAN Settings	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Port Mapping	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAT Settings	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Update Software	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Quality of Service	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management Settings	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced Setup	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Home Networking	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parental Control	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Note: Passwords may be as long as 16 characters but must not contain a space.

Click **Save/Apply** to continue.



### 8.6.2 Services

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

The screenshot shows the 'Service Access Control Configuration' page in the COMTREND web interface. The left sidebar contains a menu with items like Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Accounts, **Services**, IP Address, Wake-on-LAN, Update Software, and Reboot. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area features a table for configuring services and an 'Apply/Save' button.

Service	Current	New	Port
HTTP	Lan	LAN	80
SSH	Lan	LAN	22
TELNET	Lan	LAN	23
SNMP	Disable	Disable	161
HTTPS	Lan	LAN	443
FTP	Lan	LAN	21
TFTP	Lan	LAN	69
ICMP	Lan+Wan	LAN+WAN	0

Apply/Save

### 8.6.3 IP Address

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

The screenshot shows the 'Access Control -- IP Address' configuration page. The navigation menu includes Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (selected), and Logout. The sidebar lists Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Accounts, Services, and IP Address (selected). The main content area contains the following text:

**Access Control -- IP Address**

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

Access Control Mode:  Disable  Enable

IP Address	Subnet Mask	Interface	Remove

Buttons: Add, Remove

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

The screenshot shows the 'Access Control' configuration page. The navigation menu includes Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (selected), and Logout. The sidebar lists Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Accounts, Services, and IP Address (selected). The main content area contains the following text:

**Access Control**

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address	Subnet Mask	Interface
<input type="text"/>	<input type="text"/>	none

Button: Save/Apply

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

**IP Address** – IP address of the management station.

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

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

## 8.7 Wake-on-LAN

This tool allows you to wake up (power on) computers connected to the Broadband Router LAN interface by sending special "magic packets".

The network interface card in the computer or device that is going to be woken up must support Wake-on-LAN.

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, Diagnostics, Management (highlighted in blue), and Logout. Below the navigation bar, there is a sidebar menu on the left with options: Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, **Wake-on-LAN** (highlighted in blue), Update Software, and Reboot. The main content area is titled "Wake-on-LAN" and contains the following text: "This tool allows you to wake up (power on) computers connected to the Broadband Router LAN interface by sending special 'magic packets'. The network interface card in the computer or device that is going to be woken up must support Wake-on-LAN." Below this text, there is a prompt: "Enter the device MAC address in the format xxxxxxxx:xxxxxx:xxxxxx and then click 'Wake Up!'." There is a dropdown menu for "LAN Interface (default br0):" with "br0" selected. Below that is a text input field for "MAC Address:". There is a checkbox labeled "Send WoL magic packet to the Broadcast address." and a "Wake Up!" button at the bottom right.

LAN Interface – Select the LAN interface to send the Wake-on-LAN packet.

MAC Address – Specify the MAC address of the device that is going to be woken up.

Click "**Send WoL magic packet to the Broadcast address**" if the WoL packets should be sent to the broadcast address.

Click the **Wake Up!** button to send the magic packet out to the LAN interface.

## 8.8 Update Software

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (selected), and Logout. On the left, a sidebar lists various settings, with 'Update Software' highlighted in blue. The main content area is titled 'Tools -- Update Software' and contains the following instructions:

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

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

**NOTE:** The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

The form includes a 'Configuration' dropdown menu set to 'No Change', a 'Software File Name' input field with a 'Browse...' button, and an 'Update Software' button at the bottom right.

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

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

### Configuration options:

**No change** – upgrade software directly.

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

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

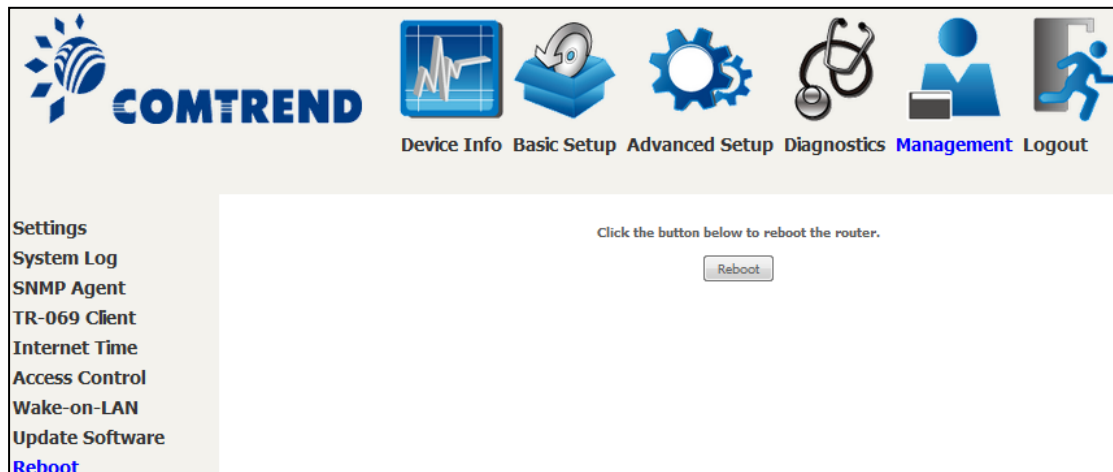
**STEP 3:** Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

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

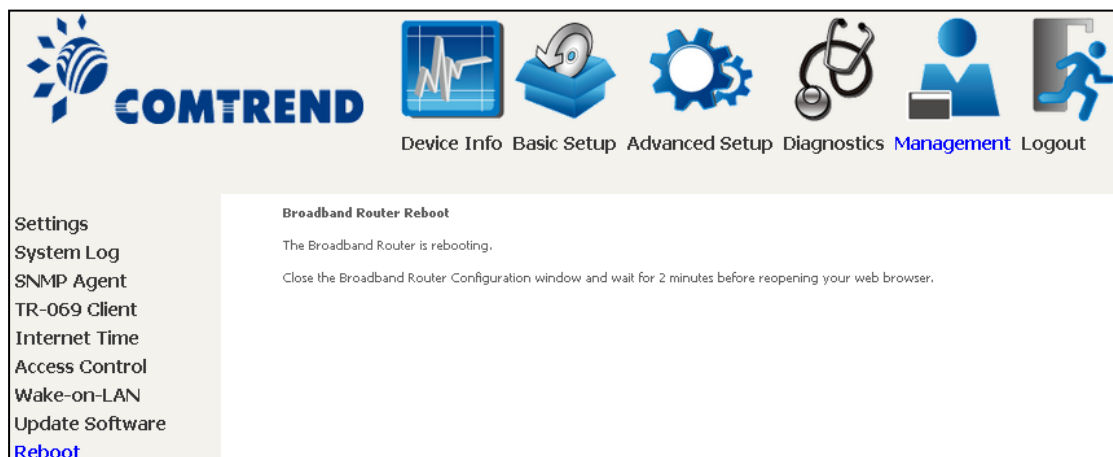
**NOTE:** The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Information](#) screen with the firmware version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

## 8.9 Reboot

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



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

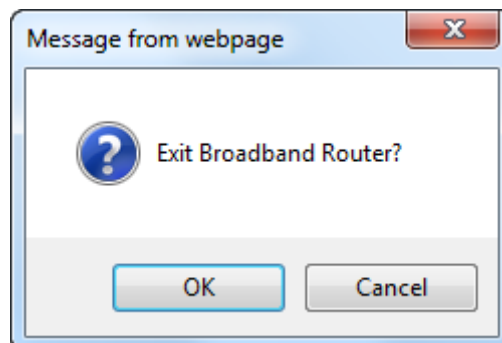


## Chapter 9 Logout

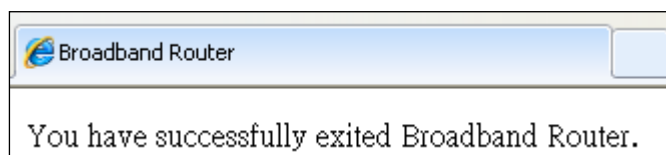
To log out from the device simply click the following icon located at the top of your screen.



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



Upon successful exit, the following message will be displayed.



## Appendix A - Firewall

### STATEFUL PACKET INSPECTION

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

### DENIAL OF SERVICE ATTACK

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

### TCP/IP/PORT/INTERFACE FILTER

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

### OUTGOING IP FILTER

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

**Example 1:**

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

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

**Example 2:**

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

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

### INCOMING IP FILTER

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

**Example 1:** Filter Name : In\_Filter1  
 Protocol : TCP  
 Policy : Allow  
 Source IP Address : 210.168.219.45  
 Source Subnet Mask : 255.255.0.0  
 Source Port : 80  
 Dest. IP Address : NA  
 Dest. Subnet Mask : NA  
 Dest. Port : NA  
 Selected WAN interface : br0

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

**Example 2:** Filter Name : In\_Filter2  
 Protocol : UDP  
 Policy : Allow  
 Source IP Address : 210.168.219.45  
 Source Subnet Mask : 255.255.0.0  
 Source Port : 5060:6060  
 Dest. IP Address : 192.168.1.45  
 Dest. Sub. Mask : 255.255.255.0  
 Dest. Port : 6060:7070  
 Selected WAN interface : br0

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

### MAC LAYER FILTER

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

**Example 1:** Global Policy : Forwarded  
 Protocol Type : PPPoE  
 Dest. MAC Address : 00:12:34:56:78:90  
 Source MAC Address : NA  
 Src. Interface : eth1  
 Dest. Interface : eth2

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

**Example 2:** Global Policy : Blocked  
 Protocol Type : PPPoE  
 Dest. MAC Address : 00:12:34:56:78:90  
 Source MAC Address : 00:34:12:78:90:56  
 Src. Interface : eth1  
 Dest. Interface : eth2

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



**DAYTIME PARENTAL CONTROL**

This feature restricts access of a selected LAN device to an outside Network through the NexusLink 3120, as per chosen days of the week and the chosen times.

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

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

## Appendix B - Pin Assignments

### Giga ETHERNET Ports (RJ45)

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

## Appendix C - Specifications

### Hardware Interface

RJ-14 X 1 for ADSL2+/VDSL2, RJ-45 X 4 for LAN, RJ-45 X 1 for WAN, Reset Button X 1, WPS/WiFi on/off button x2, Internal Wi-Fi Antennas X 2, External Wi-Fi Antennas X 2, Power Switch X 1, USB 3.0 Host X 1

### WAN Interface

ADSL2+: single line and bonding  
 VDSL2 17a, single line and bonding  
 10/100/1000 Base T, IEEE 802.3, IEEE 802.3u IEEE 802.3ab

### LAN Interface

Standard.....IEEE 802.3, IEEE 802.3u, IEEE 802.3ab  
 10/100/1000 BaseT .....Auto-sense  
 MDI/MDX support .....Yes

### WLAN Interface

Standard .....IEEE802.11b/g/n  
 Encryption..... 64/128-bit Wired Equivalent Privacy (WEP)  
 Channels..... 11 (US, Canada)/ 13 (Europe)/ 14 (Japan)  
 Data Rate.....Up to 300Mbps  
 WEP .....Yes  
 WPA .....Yes  
 IEEE 802.1x .....Yes  
 MAC Filtering .....Yes

### ATM Attributes

RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);  
 RFC 2364 (PPPoA); RFC 1577 (IPoA)

PVCs ..... 16  
 AAL type .....AAL5  
 ATM service class..... UBR/CBR/VBR  
 ATM UNI support ..... UNI 3.1/4.0  
 OAM F4/F5 .....Yes

### Management

Compliant with TR-069/TR-098/TR-104/TR-111 remote management protocols, SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

### Bridge Functions

Transparent bridging .....Yes  
 VLAN support.....Yes  
 Spanning Tree Algorithm .....Yes  
 IGMP Proxy .....Yes

**Routing Functions**

Static route, RIP v1/v2, NAT/PAT, DHCP Server/Relay, DNS Proxy, ARP,

**Security Functions**

Authentication protocols: PAP, CHAP  
TCP/IP/Port filtering rules, Packet and MAC address filtering, Access Control,

**QoS**

IP QoS, SP/WFQ/WRR for QoS, Per-PVC packet level QoS

**Environment Condition**

Operating temperature .....0 ~ 40 degrees Celsius  
Relative humidity.....5 ~ 95% (non-condensing)

**Dimensions** .....280 mm (W) x 35 mm (H) x 210 mm (D)

**Kit Weight**

(1\* NexusLink 3120, 1\*RJ11 cable, 1\*RJ45 cable, 1\*power adapter) = 1.2 kg

<b>NOTE:</b> Specifications are subject to change without notice.
---

## Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

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

For WAN access, type: `ssh -l support WAN IP address`

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

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

For WAN access, type: `putty -ssh -l support WAN IP address`

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

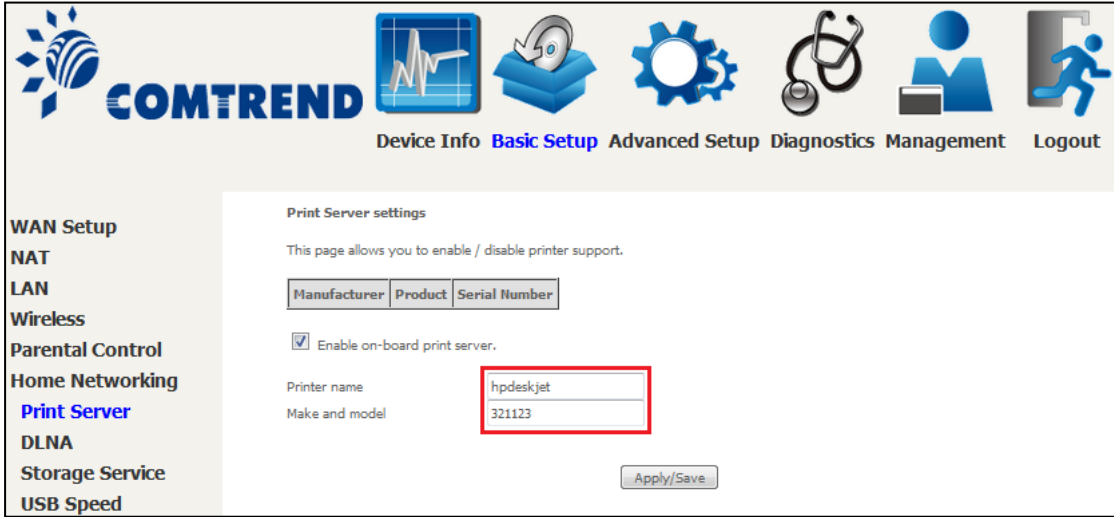
## Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

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

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

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



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with icons and labels for Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists various settings: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server (highlighted), DLNA, Storage Service, and USB Speed. The main content area is titled "Print Server settings" and contains the following text and form elements:

Print Server settings  
This page allows you to enable / disable printer support.

Manufacturer Product Serial Number

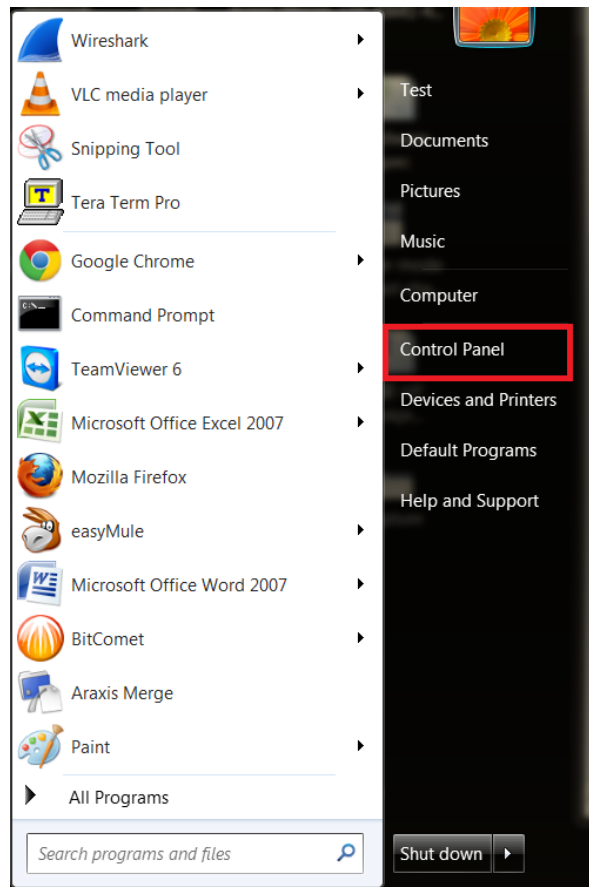
Enable on-board print server.

Printer name hpdeskjet

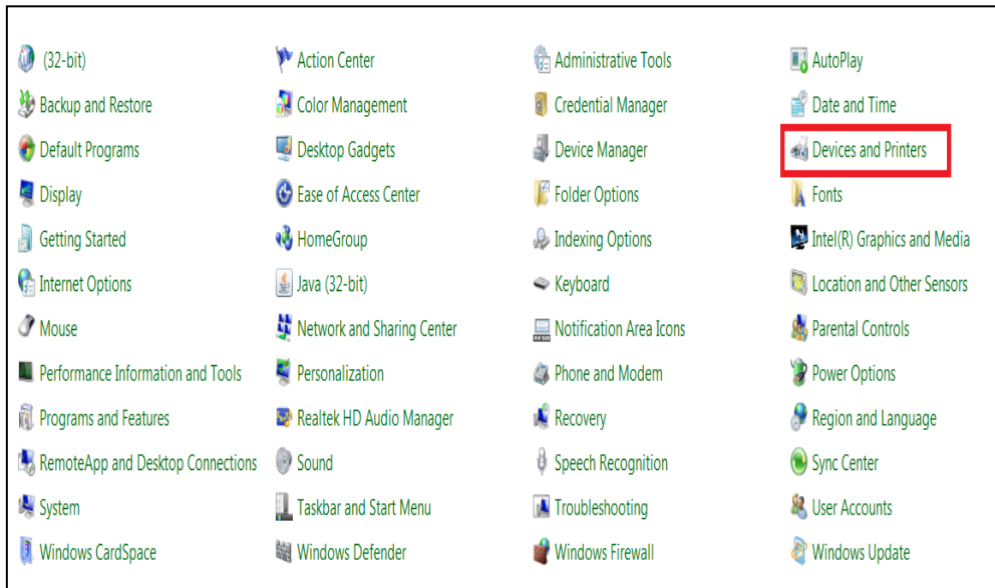
Make and model 321123

Apply/Save

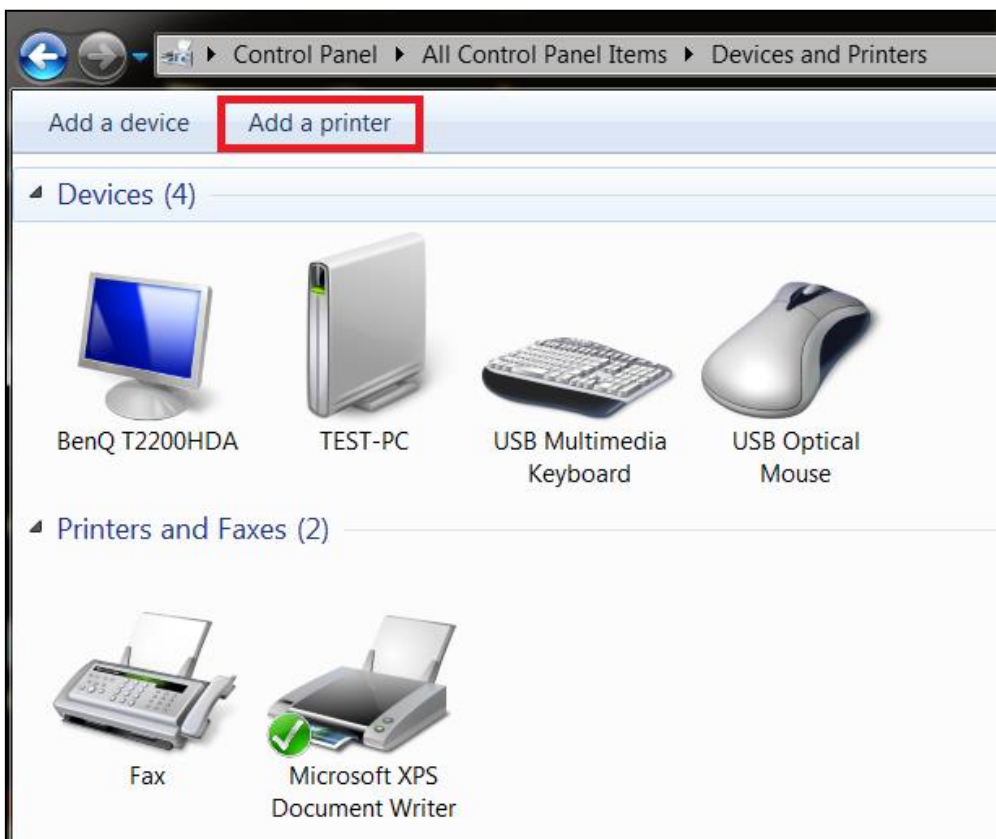
**STEP 2:** Click the Windows start button. → Then select **Control Panel**.



**STEP 3: Select Devices and Printers.**

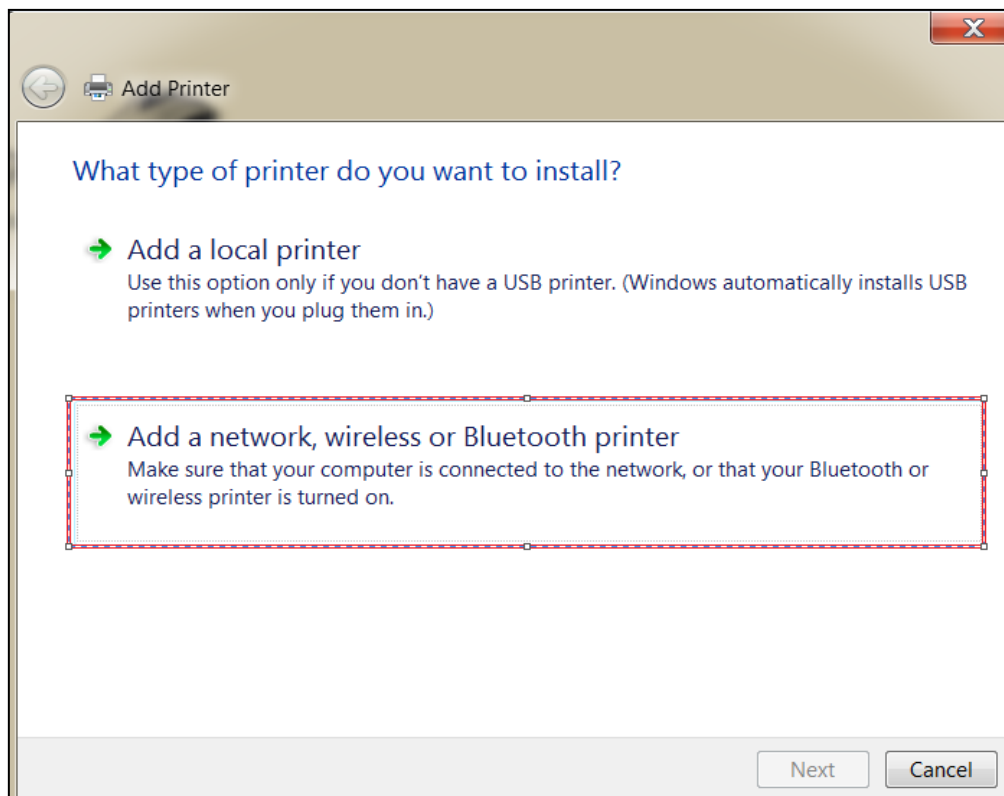


**STEP 4: Select Add a printer.**

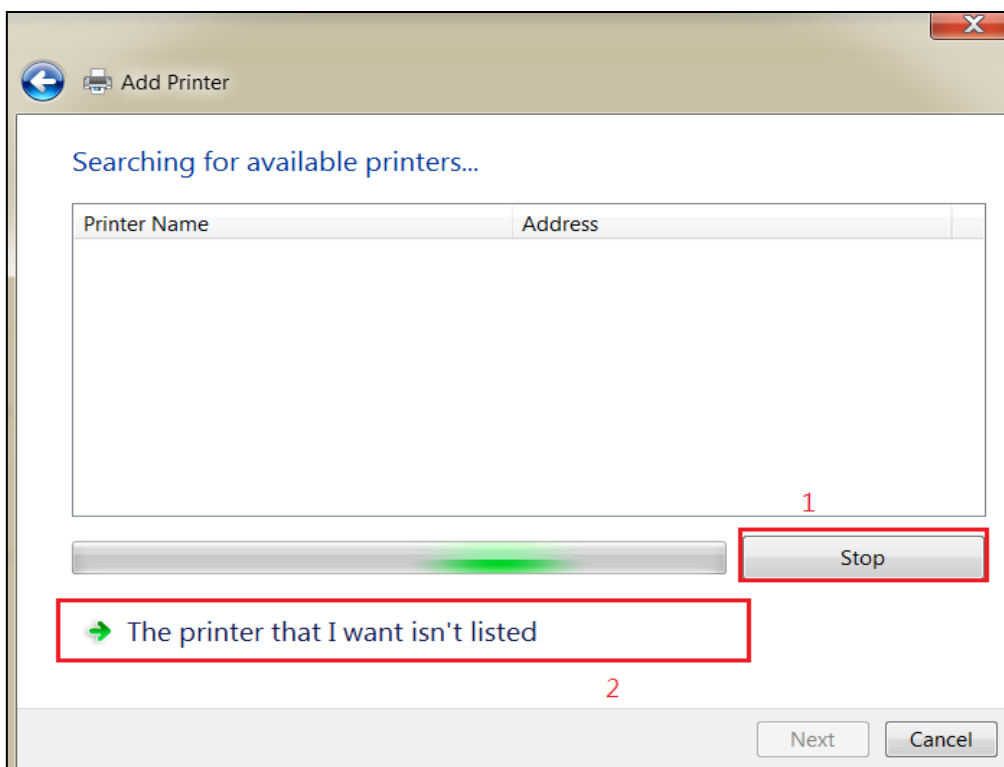




**STEP 5:** Select **Add a network, wireless or Bluetooth printer**.



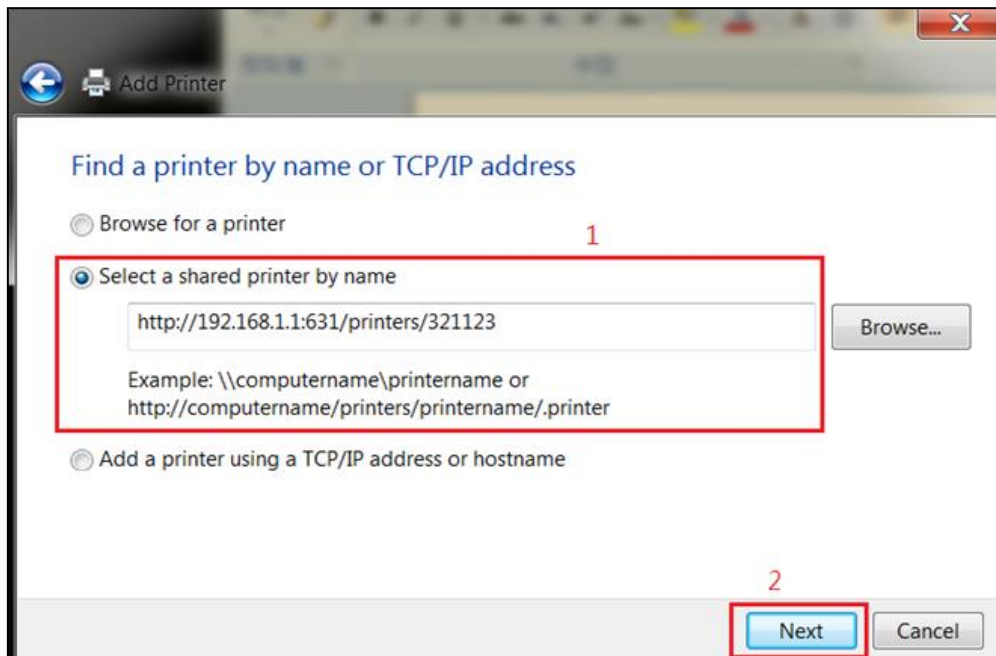
**STEP 6:** Click the **Stop** button. → Select **The printer that I want isn't listed**.



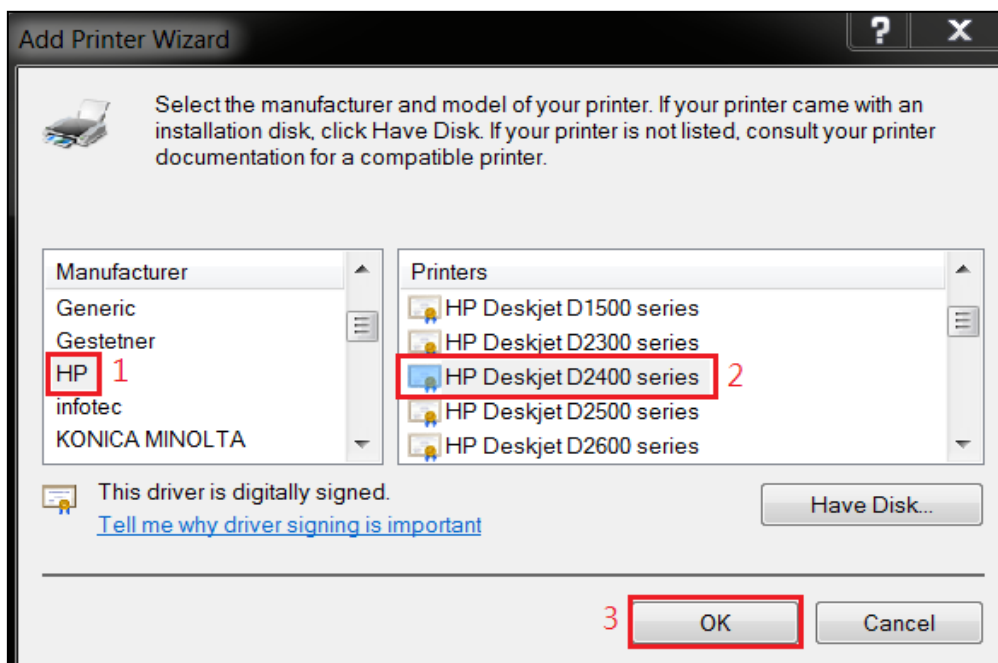
**STEP 7:** Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

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

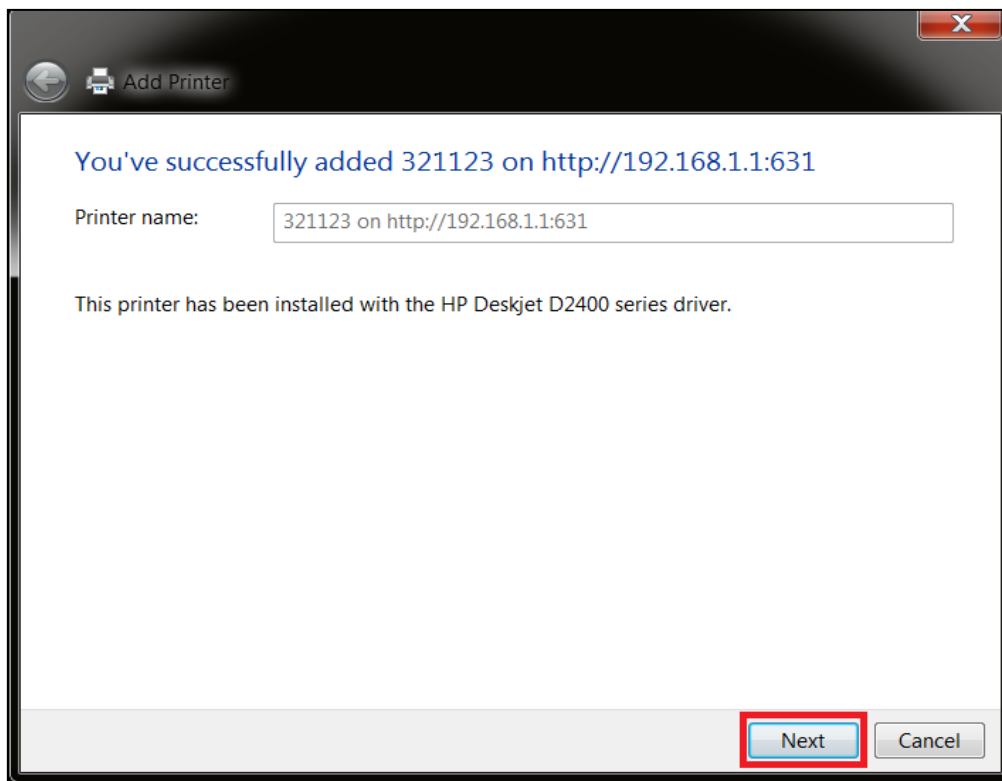
**NOTE:** The printer name must be the same name inputted in the WEB UI "printer server settings" as in step 1.



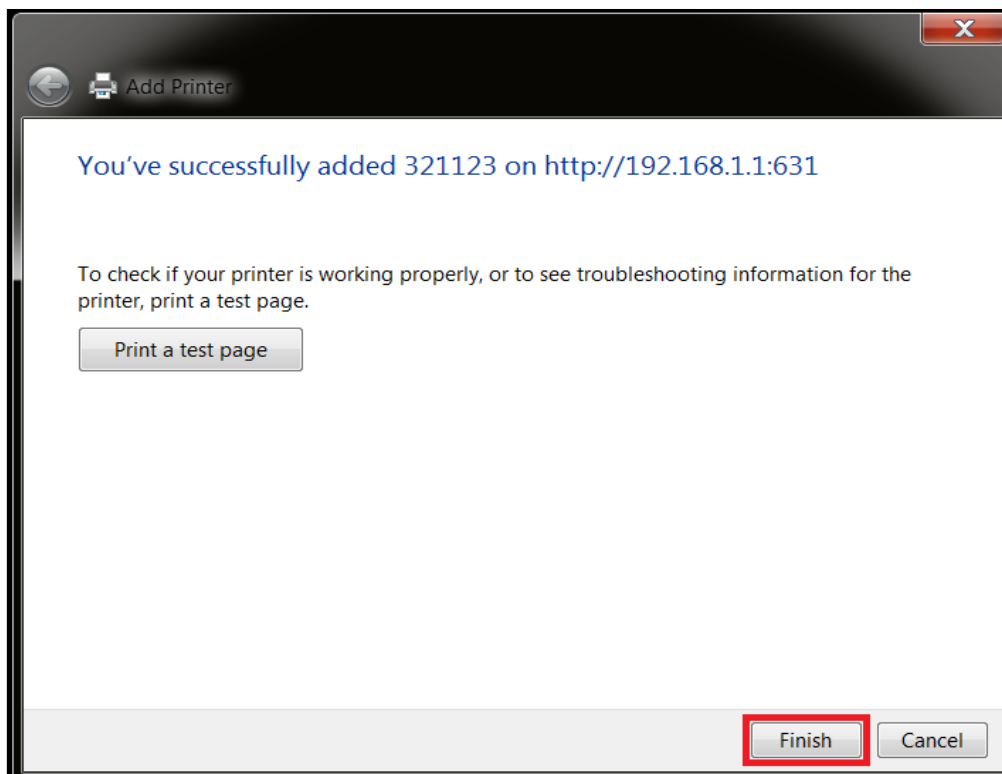
**STEP 8:** Select the **manufacturer** → and **model** of your printer → then, click **OK**.



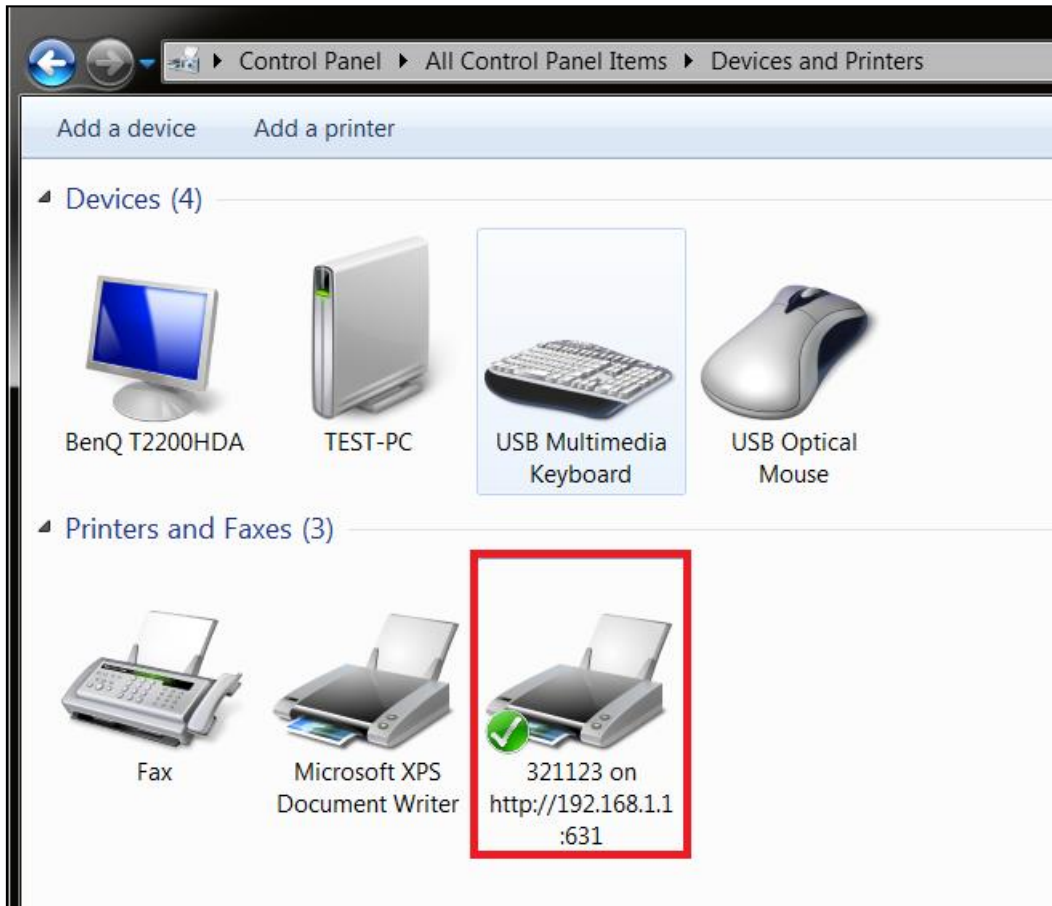
**STEP 9:** The printer has been successfully installed. Click the **Next** button.



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



**STEP 11:** Go to → **Control Panel** → **All Control Panel Items** → **Devices and Printers** to confirm that the printer has been configured.



## Appendix F - Connection Setup

Creating a WAN connection is a two-stage process.

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

The following sections describe each stage in turn.

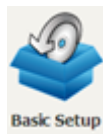
### F1 ~ Layer 2 Interfaces

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

#### F1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

**NOTE:** The NexusLink 3120 supports up to 16 ATM interfaces.



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

COMTREND

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

WAN Setup  
NAT  
LAN  
Wireless  
Parental Control  
Home Networking

Step 1: Layer 2 Interface

Select new interface to add: **ATM Interface** Add

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

This table is provided here for ease of reference.

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

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

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

**ATM PVC Configuration**

This screen allows you to configure a ATM PVC.

VPI:  [0-255]  
VCI:  [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA  
 PPPoA  
 IPoA

Encapsulation Mode:  ▾

Service Category:  ▾

Minimum Cell Rate:  [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

Default Queue Weight:  [1-63]  
Default Queue Precedence:  [1-8] (lower value, higher priority)

VC WRR Weight:  [1-63]  
VC Precedence:  [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.  
For single queue VC, the default queue precedence and weight will be used for arbitration.  
For multi-queue VC, its VC precedence and weight will be used for arbitration.

There are many settings here including: VPI/VCI, DSL Link Type, Encapsulation Mode, Service Category and Queue Weight.

Here are the available encapsulations for each xDSL Link Type:

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

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

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

Select new interface to add: **ATM Interface**

**DSL ATM Interface Configuration**

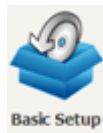
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	<input type="button" value="Remove"/>

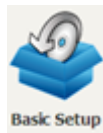
To add a WAN connection go to [Section F2 ~ WAN Connections](#).


### F1.2 PTM Interfaces







Follow these procedures to configure a PTM interface.

**NOTE:** The NexusLink 3120 supports up to four PTM interfaces.



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



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

**WAN Setup**

NAT

LAN

Wireless

Parental Control

Home Networking

Step 1: Layer 2 Interface

Select new interface to add: **PTM 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
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	<input type="button" value="Remove"/>

**DSL PTM Interface Configuration**

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
					<input type="button" value="Remove"/>

**ETH WAN Interface Configuration**

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

This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0
PTM Priority	Normal or High Priority (Preemption).



Heading	Description
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface.
IP QoS	Quality of Service (QoS) status.
Remove	Select interfaces to remove.

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

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

**PTM Configuration**

This screen allows you to configure a PTM flow.

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

Default Queue Weight:  [1-63]  
 Default Queue Precedence:  [1-8] (lower value, higher priority)  
 Default Queue Minimum Rate:  [1-0 Kbps] (-1 indicates no shaping)  
 Default Queue Shaping Rate:  [1-0 Kbps] (-1 indicates no shaping)  
 Default Queue Shaping Burst Size:  [bytes] (shall be >=1600)

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

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

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

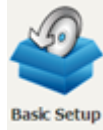
For example, a PTM interface in Default Mode is shown below.

DSL PTM Interface Configuration					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="button" value="Remove"/>

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

### F1.3 Ethernet WAN Interface

The NexusLink 3120 supports a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet interface.



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

The screenshot shows the COMTREND web interface. The top navigation bar includes 'Device Info', 'Basic Setup' (highlighted), 'Advanced Setup', 'Diagnostics', 'Management', and 'Logout'. The left sidebar lists 'WAN Setup' (highlighted), 'NAT', 'LAN', 'Wireless', 'Parental Control', and 'Home Networking'. The main content area is titled 'Step 1: Layer 2 Interface'. It features a dropdown menu for 'Select new interface to add' set to 'ETHERNET Interface' with an 'Add' button. Below this are three configuration tables:

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
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	Remove

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	Remove

Interface/(Name)	Connection Mode	Remove

This table is provided here for ease of reference.

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

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

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

Select a ETH port:

eth0/ETHWAN ▾

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

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

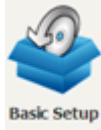
ETH WAN Interface Configuration		
Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	<input type="button" value="Remove"/>

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

## F2 ~ WAN Connections

The NexusLink 3120 supports one WAN connection for each interface, up to a maximum of 16 connections.

To setup a WAN connection follow these instructions.



**STEP 1:** Go to Basic Setup → WAN Setup.

Step 2: Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
<div style="display: flex; justify-content: center; gap: 10px;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>														

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

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)  
 For PTM interface, the descriptor string is (portId\_high\_low)  
 Where portId=0 --> DSL Latency PATH0  
 portId=1 --> DSL Latency PATH1  
 portId=4 --> DSL Latency PATH0&1  
 low =0 --> Low PTM Priority not set  
 low =1 --> Low PTM Priority set  
 high =0 --> High PTM Priority not set  
 high =1 --> High PTM Priority set

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

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

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

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

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

- (1) For [F2.1 PPP over ETHERNET \(PPPoE\) – IPv4](#)
- (2) For [F2.2 IP over ETHERNET \(IPoE\) – IPv4](#)
- (3) For [F2.3 Bridging – IPv4](#)
- (4) For [F2.4 PPP over ATM \(PPPoA\) – IPv4](#)
- (5) For [F2.5 IP over ATM \(IPoA\) – IPv4](#)
- (6) For [F2.6 PPP over ETHERNET \(PPPoE\) – IPv6](#)
- (7) For [F2.7 IP over ETHERNET \(IPoE\) – IPv6](#)
- (8) Bridging – IPv6 (Not Supported)
- (9) For [F2.8 PPP over ATM \(PPPoA\) – IPv6](#)
- (10) IPoA – IPv6 (Not Supported)

The subsections that follow continue the WAN service setup procedure.

## F2.1 PPP over ETHERNET (PPPoE) – IPv4

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet (DHCP/ Static IP)  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

\*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

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

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

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

### PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO** ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

### IGMP Multicast Proxy

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

### WAN interface with base MAC.

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

Enable WAN interface with base MAC

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

The settings shown above are described below.

### PPP SETTINGS

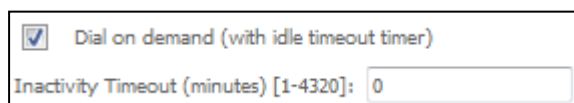
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

### ENABLE FULLCONE NAT

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

### DIAL ON DEMAND

The NexusLink 3120 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]: 0

### PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

### ENABLE NAT

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

### ENABLE FIREWALL

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



**USE STATIC IPv4 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv4 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).

**FIXED MTU**

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

**ENABLE PPP DEBUG MODE**

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

**BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS**

*(This option is hidden when PPP IP Extension is enabled)*

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The NexusLink 3120 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

**ENABLE IGMP MULTICAST PROXY**

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

**ENABLE IGMP MULTICAST SOURCE**

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

**Enable WAN interface with base MAC**

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

---

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

**Routing -- Default Gateway**

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	<input type="button" value="→"/> <input type="button" value="←"/>	
<input type="button" value="Back"/> <input type="button" value="Next"/>		

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

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

### 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
ppp0.1	

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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

## F2.2 IP over ETHERNET (IPoE) – IPv4

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet (DHCP/ Static IP)

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

\*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

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

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

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

### WAN IP Settings

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

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 77 User ID:

Option 125:  Disable  Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

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

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

**Network Address Translation Settings**

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

Enable NAT

Enable Fullcone NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

### ENABLE NAT

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

### ENABLE FULLCONE NAT

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

### ENABLE FIREWALL

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

### ENABLE IGMP MULTICAST PROXY

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

### ENABLE IGMP MULTICAST SOURCE

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

**Enable WAN interface with base MAC**

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

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

**Routing -- Default Gateway**

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

<b>Selected Default Gateway Interfaces</b>		<b>Available Routed WAN Interfaces</b>
atm0.1	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	
	<input type="button" value="Back"/> <input type="button" value="Next"/>	

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

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

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. 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
atm0.1	

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

Primary DNS server:

Secondary DNS server:

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



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

**WAN Setup - Summary**

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

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

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

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

## F2.3 Bridging – IPv4

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet (DHCP/ Static IP)  
 Bridging  
 Allow as IGMP Multicast Source  
 Allow as MLD Multicast Source

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

### Allow as IGMP Multicast Source

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

### Allow as MLD Multicast Source

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

\*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

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

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

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

**WAN Setup - Summary**

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

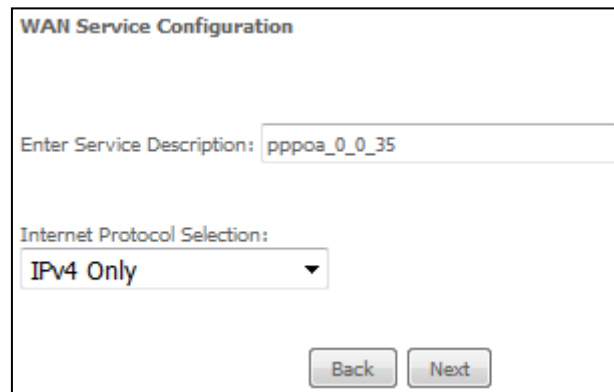
Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

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

**NOTE:** If this bridge connection is your only WAN service, the NexusLink 3120 will be inaccessible for remote management or technical support from the WAN.

## F2.4 PPP over ATM (PPPoA) – IPv4



The image shows a 'WAN Service Configuration' dialog box. It contains a text input field for 'Enter Service Description' with the value 'pppoa\_0\_0\_35'. Below it is a dropdown menu for 'Internet Protocol Selection' currently set to 'IPv4 Only'. At the bottom right are 'Back' and 'Next' buttons.

WAN Service Configuration

Enter Service Description:

Internet Protocol Selection:

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

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

**PPP Username and Password**

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

PPP Username:

PPP Password:

Authentication Method: AUTO ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU:

Enable PPP Debug Mode

**IGMP Multicast Proxy**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

### PPP SETTINGS

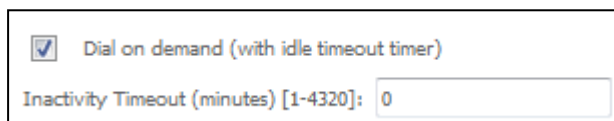
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

**ENABLE FULLCONE NAT**

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

**DIAL ON DEMAND**

The NexusLink 3120 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]: 0

**PPP IP EXTENSION**

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

**ENABLE NAT**

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

**ENABLE FIREWALL**

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

**USE STATIC IPv4 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in [Section 3.2](#).

**Fixed MTU**

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

**ENABLE PPP DEBUG MODE**

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

**ENABLE IGMP MULTICAST PROXY**

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

**ENABLE IGMP MULTICAST SOURCE**

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

**Enable WAN interface with base MAC**

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

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

**Routing -- Default Gateway**

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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
pppoa0	
<div style="display: flex; justify-content: center; gap: 10px;"> <div style="border: 1px solid gray; padding: 2px 10px;">-&gt;</div> <div style="border: 1px solid gray; padding: 2px 10px;">&lt;-</div> </div>	
<div style="display: flex; justify-content: center; gap: 20px;"> <div style="border: 1px solid gray; padding: 2px 10px;">Back</div> <div style="border: 1px solid gray; padding: 2px 10px;">Next</div> </div>	

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

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

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. 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
<div style="border: 1px solid gray; padding: 5px; min-height: 100px;">pppoa0</div>	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;"></div>

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

Primary DNS server:

Secondary DNS server:

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



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

**WAN Setup - Summary**

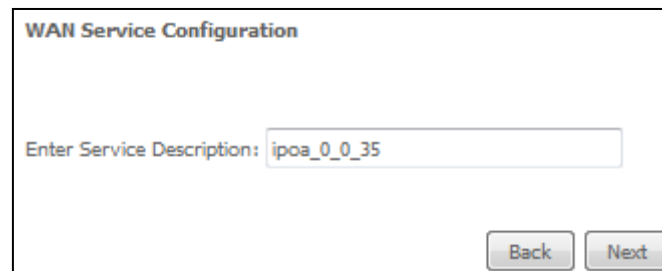
Make sure that the settings below match the settings provided by your ISP.

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

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

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

## F2.5 IP over ATM (IPoA) – IPv4

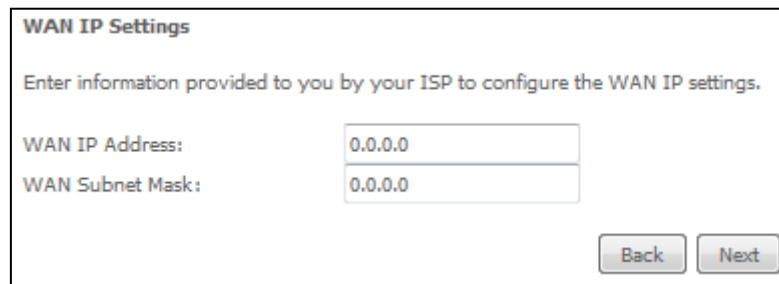


**WAN Service Configuration**

Enter Service Description:

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

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



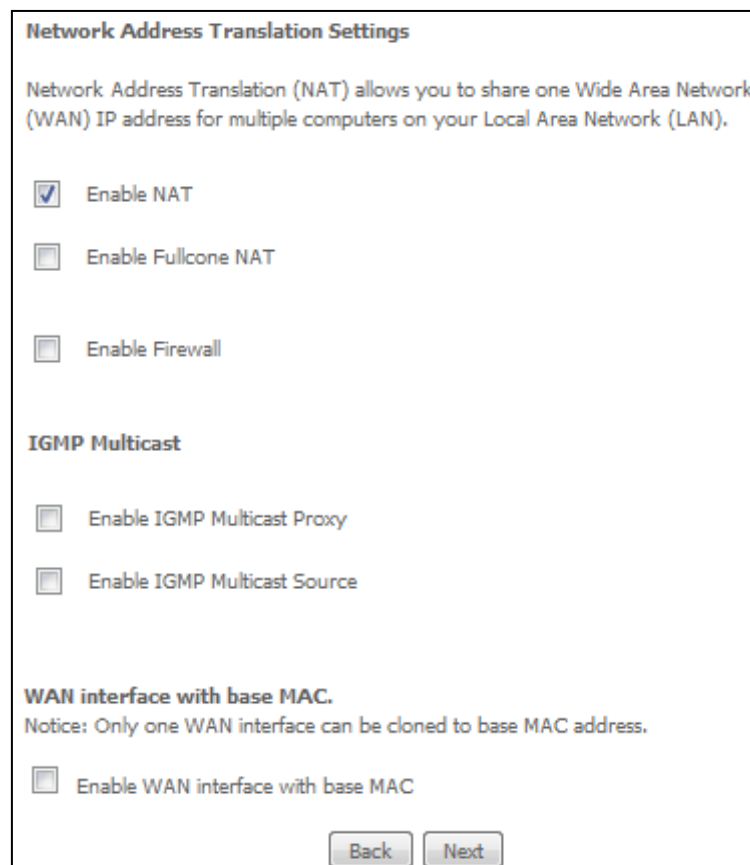
**WAN IP Settings**

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

WAN IP Address:

WAN Subnet Mask:

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



**Network Address Translation Settings**

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

Enable NAT

Enable Fullcone NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

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

Enable WAN interface with base MAC

**ENABLE NAT**

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

**ENABLE FULLCONE NAT**

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

**ENABLE FIREWALL**

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

**ENABLE IGMP MULTICAST PROXY**

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

**ENABLE IGMP MULTICAST SOURCE**

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

**Enable WAN interface with base MAC**

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

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

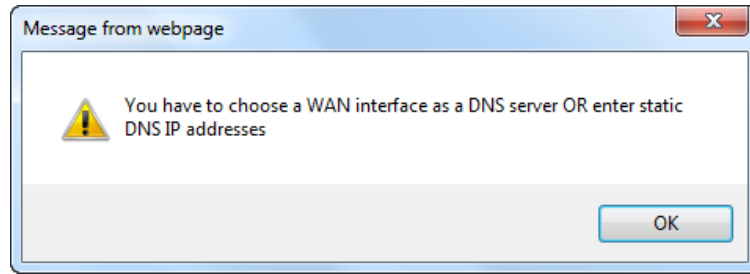
**Routing -- Default Gateway**

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ipoa0	<input type="button" value="→"/> <input type="button" value="←"/>	
<input type="button" value="Back"/> <input type="button" value="Next"/>		

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

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



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

**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	<input type="button" value="-&gt;"/>  <input type="button" value="&lt;-"/>	Available WAN Interfaces
<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>		<div style="border: 1px solid gray; width: 100%; height: 100%;"></div>

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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

## F2.6 PPP over ETHERNET (PPPoE) – IPv6

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet (DHCP/ Static IP)  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

\*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

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

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

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

### PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO** ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable Firewall

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Launch Dhcp6c for Rapid Commit

Fixed MTU

MTU:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Enable MLD Multicast Proxy

Enable MLD Multicast Source

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

Enable WAN interface with base MAC

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

The settings shown above are described below.

### PPP SETTINGS

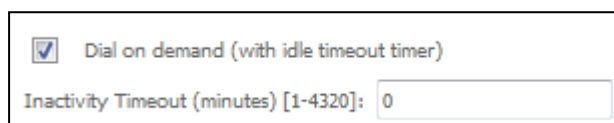
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

### ENABLE FULLCONE NAT

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

### DIAL ON DEMAND

The NexusLink 3120 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



### PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

### ENABLE FIREWALL

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

### USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv4 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).



**USE STATIC IPv6 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv6 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).

**ENABLE IPv6 UNNUMBERED MODEL**

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

**LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)**

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

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

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

**LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)**

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

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

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

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

**LAUNCH DHCP6C FOR RAPID COMMIT**

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

**FIXED MTU**

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

**ENABLE PPP DEBUG MODE**

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

**BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS**

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The NexusLink 3120 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

**ENABLE MLD MULTICAST PROXY**

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

**ENABLE MLD MULTICAST SOURCE**

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

**Enable WAN interface with base MAC**

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

---

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

**Routing -- Default Gateway**

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

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

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

Selected WAN Interface

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

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

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

**DNS Server Configuration**

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. 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
ppp0.1	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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

## F2.7 IP over ETHERNET (IPoE) – IPv6

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet (DHCP/ Static IP)  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

\*

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

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

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

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

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

Notice: If "Obtain an IPv6 address automatically" is chosen, DHCP client will be enabled on this WAN interface.

If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

**WAN IP Settings**

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

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 77 User ID:

Option 125:  Disable  Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.  
 Notice:  
 If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.  
 If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address.  
 If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Dhcpv6 Rapid Commit

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

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

WAN Next-Hop IPv6 Address:

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



### **DHCP6C FOR ADDRESS ASSIGNMENT (IANA)**

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

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

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

### **DHCP6C FOR PREFIX DELEGATION (IAPD)**

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

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

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

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

### **DHCP6C FOR RAPID COMMIT**

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

### **WAN NEXT-HOP IPv6 ADDRESS**

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

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

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

**Network Address Translation Settings**

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

Enable NAT

Enable Firewall

Enable MLD Multicast Proxy

Enable MLD Multicast Source

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

Enable WAN interface with base MAC

Back Next

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

#### **ENABLE NAT**

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

#### **ENABLE FIREWALL**

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

#### **ENABLE MLD MULTICAST PROXY**

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

#### **ENABLE MLD MULTICAST SOURCE**

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

#### **Enable WAN interface with base MAC**

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

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

### Routing -- Default Gateway

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
atm0.1	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Selected WAN Interface

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

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

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

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. 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
atm0.1	
<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

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

**WAN Setup - Summary**

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

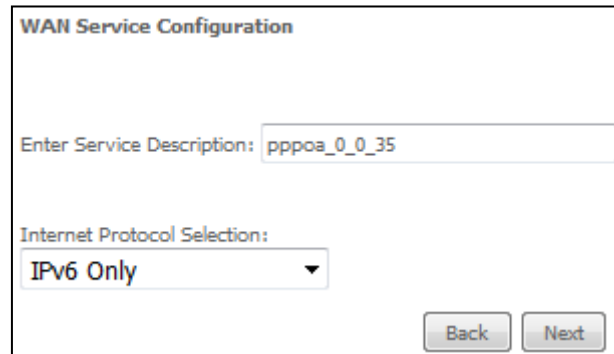
Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

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

## F2.8 PPP over ATM (PPPoA) – IPv6

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



The image shows a screenshot of a web-based configuration interface titled "WAN Service Configuration". It contains the following elements:

- A text input field labeled "Enter Service Description:" with the value "pppoa\_0\_0\_35".
- A dropdown menu labeled "Internet Protocol Selection:" with "IPv6 Only" selected.
- Two buttons at the bottom right: "Back" and "Next".

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

**PPP Username and Password**

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

PPP Username:

PPP Password:

Authentication Method: **AUTO** ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable Firewall

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Launch Dhcp6c for Rapid Commit

Fixed MTU

MTU:

Enable PPP Debug Mode

Enable MLD Multicast Proxy

Enable MLD Multicast Source

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

### PPP SETTINGS

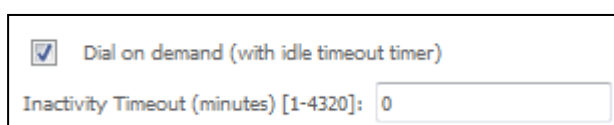
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

### ENABLE FULLCONE NAT

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

### DIAL ON DEMAND

The NexusLink 3120 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

### PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

### ENABLE FIREWALL

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

### USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in [3.2 IP Configuration](#).

### USE STATIC IPv6 ADDRESS

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



**ENABLE IPv6 UNNUMBERED MODEL**

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

**LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)**

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

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

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

**LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)**

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

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

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

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

**LAUNCH DHCP6C FOR RAPID COMMIT**

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

**FIXED MTU**

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

**ENABLE PPP DEBUG MODE**

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

**ENABLE MLD MULTICAST PROXY**

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

**ENABLE MLD MULTICAST SOURCE**

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

**Enable WAN interface with base MAC**

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

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

**Routing -- Default Gateway**

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
pppoa0	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	
IPv6: Select a preferred wan interface as the system default IPv6 gateway.		
Selected WAN Interface <input style="width: 150px;" type="text" value="pppoa_0_0_35/pppoa0"/>		
<input type="button" value="Back"/> <input type="button" value="Next"/>		

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

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

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

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. 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
pppoa0	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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