

NexusLink 3130

Home Gateway

User Manual



Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

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:

- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.
- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
- If you experience trouble with this equipment, disconnect it from the network until the problem has been corrected or until you are sure that equipment is not malfunctioning.

**WARNING**

- Disconnect the power line from the device before servicing.
- For indoor use only
- Do NOT open the casing
- Do NOT use near water
- Do NOT insert sharp objects into the RJ-11 jack
- Keep away from the fire
- For use in ventilated environment / space
- Use 26 AWG or larger cable connect to RJ-11 port

- Débranchez l'alimentation électrique avant l'entretien
- Cet appareil est conçu pour l'usage intérieur seulement
- N'ouvrez pas le boîtier
- N'utilisez pas cet appareil près de l'eau
- N'insérez pas d'objets tranchants dans la prise RJ-11
- N'approchez pas du feu
- Veuillez utiliser dans un environnement aéré
- Veuillez utiliser fil électrique de 26AWG pour port RJ-11

Power Specifications (Alimentation) :
 Input : 12Vdc, 1.0A 

**User Information**

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

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

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

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

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

This Class B digital apparatus complies with Canadian ICES-003.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.
This device complies with Part 15 of the FCC Rules and Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada.
Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s).

Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

Certification

- FCC / IC standard
 - Part 15B / ICES-003
 - TIA-968 / IC-CS03
 - UL 62368-1 / CSA 62368-1

Copyright

Copyright©2020 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

NOTE: This document is subject to change without notice.

Protect Our Environment

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

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

Table of Contents

CHAPTER 1 INTRODUCTION.....	7
CHAPTER 2 INSTALLATION.....	8
2.1 HARDWARE SETUP.....	8
2.2 LED INDICATORS.....	10
CHAPTER 3 WEB USER INTERFACE.....	11
3.1 DEFAULT SETTINGS	11
3.2 IP CONFIGURATION.....	12
3.3 LOGIN PROCEDURE.....	14
CHAPTER 4 DEVICE INFORMATION.....	16
4.1 WAN	17
4.2 STATISTICS.....	19
4.2.1 LAN Statistics	19
4.2.2 WAN Service	20
4.2.3 XTM Statistics.....	21
4.2.4 xDSL Statistics.....	22
4.3 ROUTE	27
4.4 ARP.....	28
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
CHAPTER 5 BASIC SETUP.....	38
5.1 WAN SETUP	39
5.1.1 WAN Service Setup	40
5.2 NAT	42
5.2.1 Virtual Servers.....	42
5.2.2 Port Triggering.....	44
5.2.3 DMZ Host.....	46
5.2.4 IP Address Map	47
5.2.5 ALG/Pass-Through.....	49
5.3 LAN	50
5.3.1 Lan VLAN Setting	53
5.3.2 LAN IPv6 Autoconfig.....	54
5.3.3 Static IP Neighbor	58
5.3.4 UPnP	59
5.4 ROUTER LIMITS	60
5.5 PARENTAL CONTROL.....	62
5.5.1 Time Restriction.....	62
5.5.2 WhiteList Time	63
5.5.3 URL Filter	64
5.6 HOME NETWORKING.....	66
5.6.1 Print Server	66
5.6.2 DLNA.....	67
CHAPTER 6 ADVANCED SETUP.....	68
6.1 AUTO-DETECTION SETUP	68
6.2 SECURITY	73
6.2.1 IP Filtering	73
6.2.2 MAC Filtering	77
6.3 QUALITY OF SERVICE (QoS).....	79

6.3.1 QoS Queue.....	80
6.3.1.1 QoS Queue Configuration	80
6.3.2 QoS Classification.....	82
6.3.3 QoS Port Shaping.....	84
6.4 ROUTING	85
6.4.1 Default Gateway.....	85
6.4.2 Static Route.....	86
6.4.3 Policy Routing	87
6.4.4 RIP.....	88
6.5 DNS	89
6.5.1 DNS Server.....	89
6.5.2 Dynamic DNS.....	90
6.5.3 DNS Entries.....	92
6.5.4 DNS Proxy/Relay.....	93
6.6 DSL.....	94
6.7 DSL BONDING.....	96
6.8 INTERFACE GROUPING.....	97
6.9 IPTUNNEL.....	100
6.9.1 IPv6inIPv4.....	100
6.9.2 IPv4inIPv6.....	102
6.10 CERTIFICATE.....	103
6.10.1 Local.....	103
6.10.2 Trusted CA.....	106
6.11 MULTICAST.....	107
CHAPTER 7 DIAGNOSTICS.....	110
7.1 DIAGNOSTICS – INDIVIDUAL TESTS	110
7.2 ETHERNET OAM	111
7.3 UPTIME STATUS	113
7.4 PING	114
7.5 TRACE ROUTE	115
CHAPTER 8 MANAGEMENT	116
8.1 SETTINGS.....	116
8.1.1 Backup Settings	116
8.1.2 Update Settings.....	117
8.1.3 Restore Default.....	117
8.2 SYSTEM LOG	118
8.3 SNMP AGENT	120
8.4 TR-069 CLIENT	121
8.5 INTERNET TIME	124
8.6 ACCESS CONTROL	125
8.6.1 Accounts	125
8.6.2 Services.....	127
8.6.3 IP Address.....	128
8.7 WAKE-ON-LAN.....	129
8.8 UPDATE SOFTWARE	130
8.9 REBOOT.....	131
CHAPTER 9 LOGOUT	132
APPENDIX A - FIREWALL	133
APPENDIX B - PIN ASSIGNMENTS	136
APPENDIX C - SPECIFICATIONS.....	137
APPENDIX D - SSH CLIENT	139
APPENDIX E - PRINTER SERVER.....	140
APPENDIX F - CONNECTION SETUP.....	147

Chapter 1 Introduction

NexusLink 3130 is a Multi-DSL bonding router using the updated silicon platform. It not only provides both ADSL and VDSL but also supports xDSL bonding for extend WAN access bandwidth. Support VDSL 35b profile on single line. NexusLink 3130 is designed for high speed applications and is suitable for triple play services.

Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.



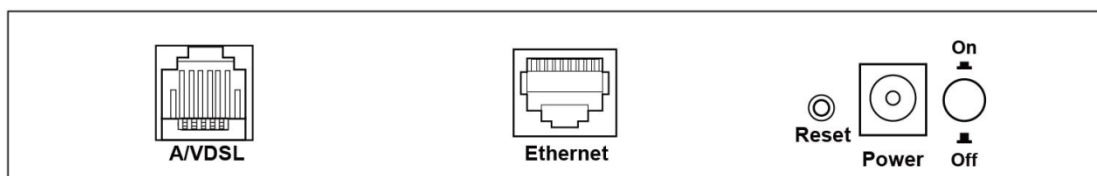
DO NOT STACK

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 3130 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.

Giga Ethernet (LAN) Port

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.

DSL Port

Connect to an ADSL2/2+ or VDSL with this RJ14 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.

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.
GE	GREEN	On	Giga Ethernet connected
		Off	Giga Ethernet not connected
		Blink	Giga Ethernet is transmitting/receiving
DSL 1	GREEN	On	xDSL Link is established.
		Off	xDSL Link is not established.
		Blink	The xDSL link is training or some traffic is passing through xDSL.
DSL 2	GREEN	On	xDSL Link is established.
		Off	xDSL Link is not established.
		Blink	The xDSL link is training or some traffic is passing through xDSL.
INTERNET	GREEN	On	WAN connected.
		Off	Modem power off, modem in bridged mode or WAN connection not present.
		Blink	WAN Traffic is passing thru the device (either direction).
	RED	On	Device attempted to become WAN connected but 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 3130 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

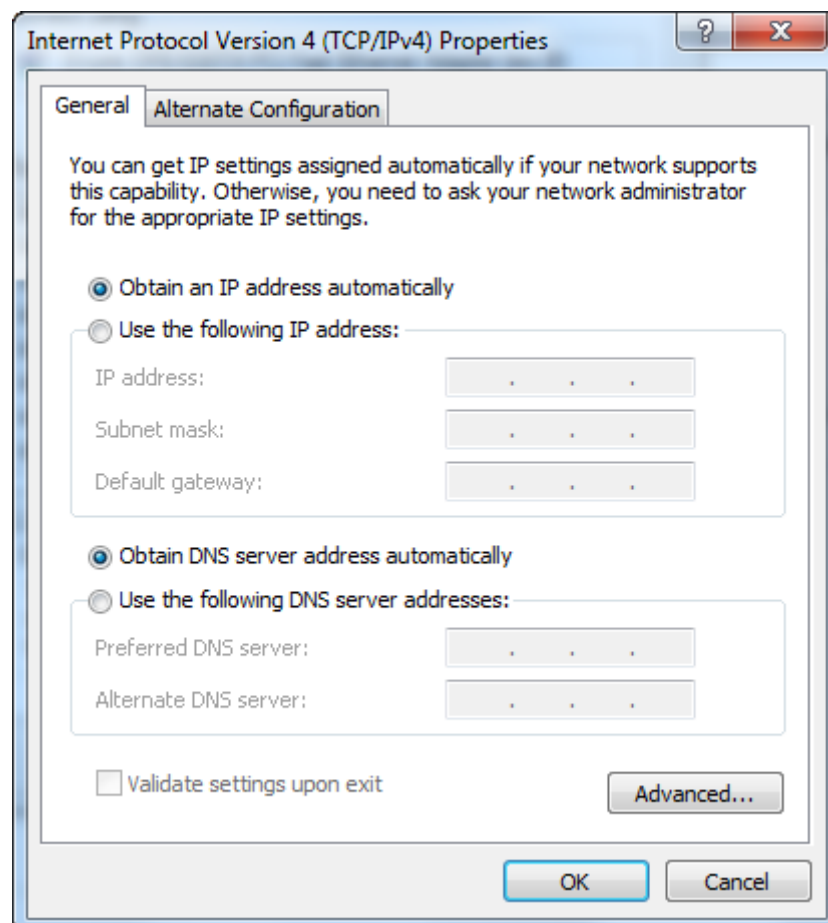
To obtain an IP address from the DHCP server, follow the steps provided below.

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

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

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

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



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

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

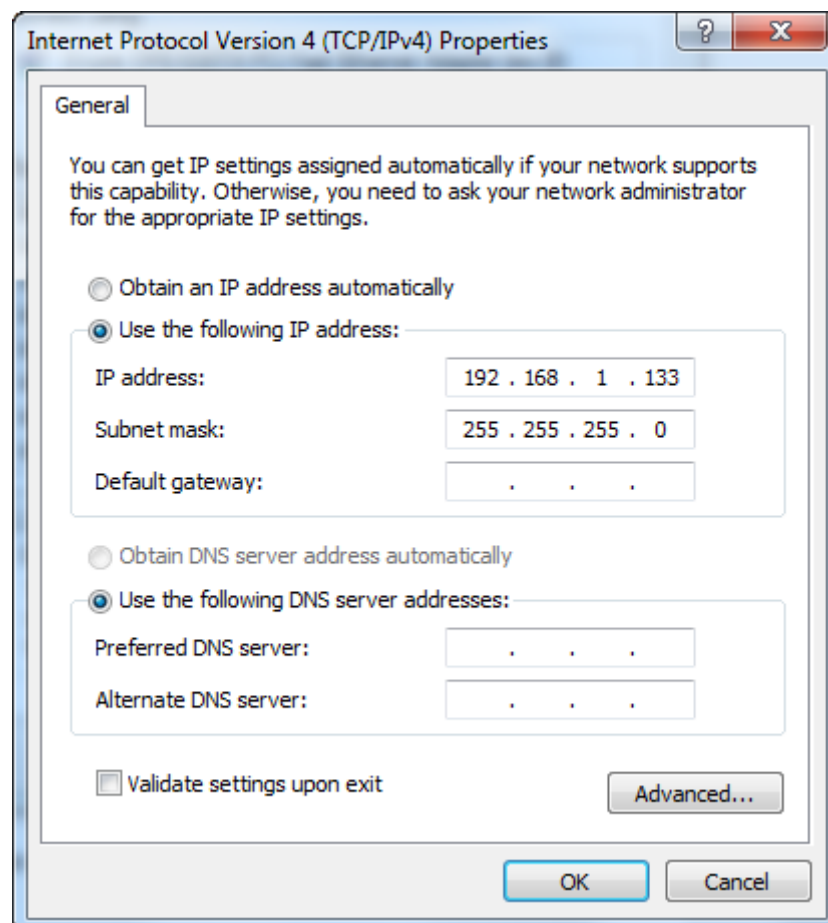
STATIC IP MODE

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

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

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

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



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

3.3 Login Procedure

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

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

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

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

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



Click **OK** to continue.

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

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

The screenshot displays the COMTREND web interface. At the top, there are six navigation icons: Device Info (a line graph), Basic Setup (a floppy disk), Advanced Setup (gears), Diagnostics (a stethoscope), Management (a person at a computer), and Logout (a person walking). Below these icons is a sidebar menu with the following items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, CPU & Memory, and Network Map.

The main content area is divided into three sections:

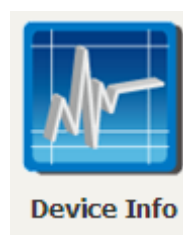
- Device:** A table with the following data:

Model	NexusLink 3130
Board ID	63138MB-186AC7
Serial Number	0
Firmware Version	V011-416CTU-C01_R01.A2pvhH042x5.d27i
Bootloader (CFE) Version	1.0.38-118.8-14
Up Time	6 mins:59 secs
- LAN:** A table with the following data:

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:00:00:55:55:55
DHCP Server	Enabled
- WAN:** A table with the following data:

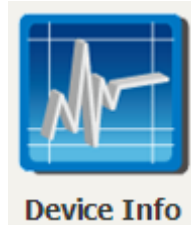
DSL 1 Status	Down
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
DSL 2 Status	Down
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

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



Chapter 4 Device Information

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



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

NOTE: The menu items shown are based upon the configured connection(s) and user account privileges. For example, user account has limited access to configuration modification.

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

The Device Info Summary screen displays at startup.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Info
IPv6
CPU & Memory
Network Map

Device	
Model	NexusLink 3130
Board ID	63138MB-186AC7
Serial Number	0
Firmware Version	V011-416CTU-C01_R01.A2pvbH042x5.d27i
Bootloader (CFE) Version	1.0.38-118.8-14
Up Time	6 mins:59 secs

LAN
GE

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:00:00:55:55:55
DHCP Server	Enabled

WAN
DOWN

DSL 1 Status	Down
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
DSL 2 Status	Down
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

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

4.1 WAN

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

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

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

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

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		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	558969	4662	0	0	0	627	3818	217	3491469	4873	0	5	0	249	4620	4		
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		

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

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
 Statistics
 LAN
[WAN Service](#)
 xTM
 xDSL

Statistics -- WAN

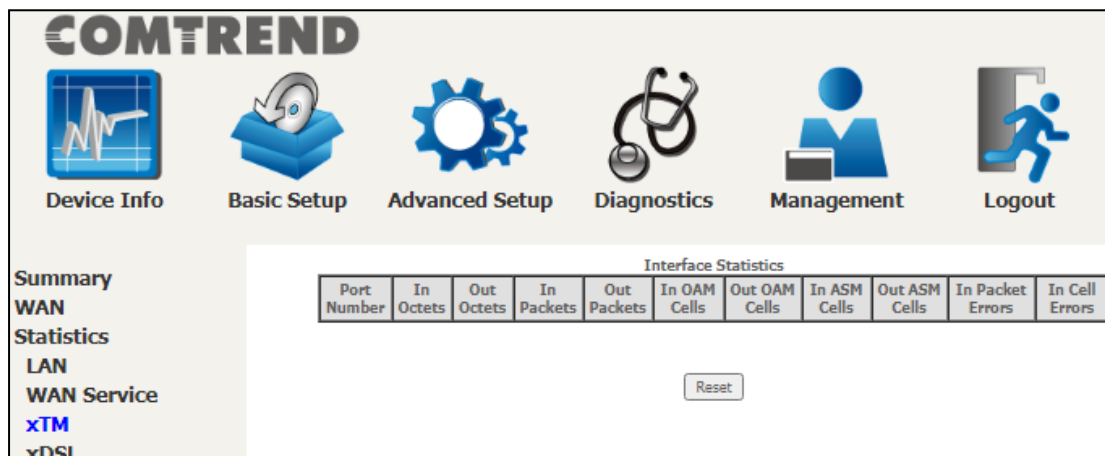
Interface	Description	Received						Transmitted									
		Total		Multicast	Unicast	Broadcast	Total		Multicast	Unicast	Broadcast						
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts

Reset Statistics

Item	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

Statistics -- xDSL

Bonding Line Selection

	Downstream	Upstream
Mode:	vDSL2	
Traffic Type:	PTM	
Status:	Up	
Link Power State:	L0	
	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	163	60
Attenuation (0.1 dB):	53	0
Output Power (0.1 dBm):	145	85
Attainable Rate (Kbps):	147821	62767
	Path 0	
	Downstream	Upstream
Rate (Kbps):	99999	59969
B (# of bytes in Mux Data Frame):	79	237
M (# of Mux Data Frames in an RS codeword):	1	1
T (# of Mux Data Frames in an OH sub-frame):	59	64
R (# of redundancy bytes in the RS codeword):	16	16
S (# of data symbols over which the RS code word spans):	0.0255	0.1263
L (# of bits transmitted in each data symbol):	30168	16086
D (interleaver depth):	631	253
I (interleaver block size in bytes):	96	127
N (RS codeword size):	96	254
Delay (msec):	4	4
INP (DMT symbol):	1.00	0.50
OH Frames:	23870	13282
OH Frame Errors:	0	0
RS Words:	4069341	855619
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	0	0
Data Cells:	0	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	39	39

xDSL BER Test Reset Statistics Draw Graph

ADSL

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

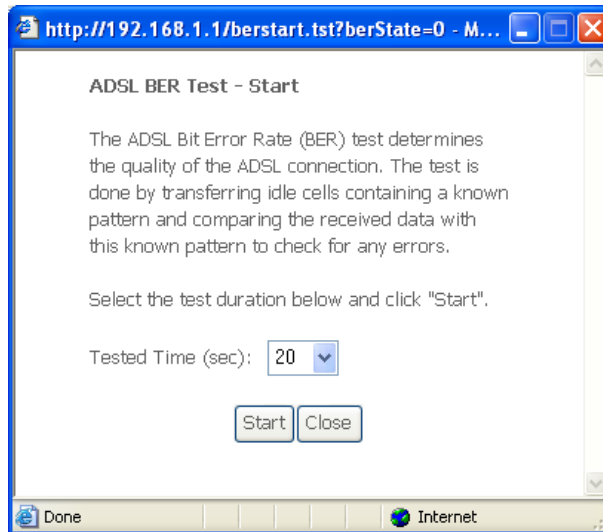
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)

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

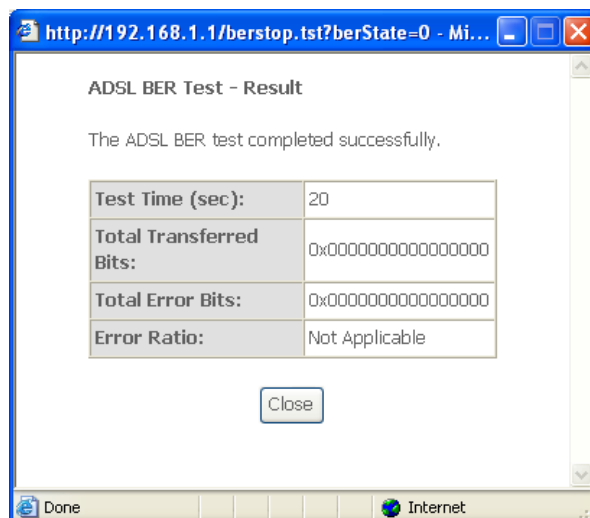
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

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.

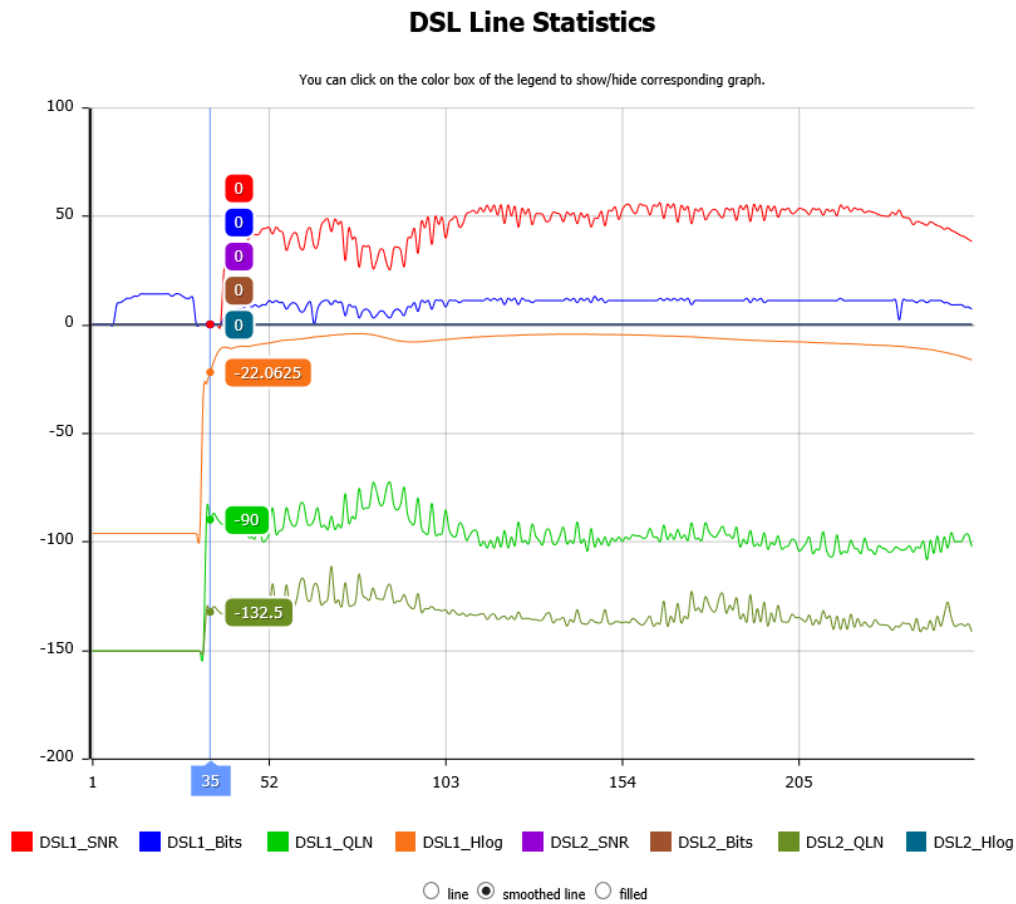


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



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 3130 has found.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP

Device Info -- Route

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

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

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

4.4 ARP

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

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 the navigation bar, there is a sidebar menu with links for Summary, WAN, Statistics, Route, and ARP. The main content area displays the title "Device Info -- ARP" and a table with the following data:

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

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

4.5 DHCP

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

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
DHCPv4
DHCPv6

Device Info -- DHCPv6 Leases

IPv6 Address	MAC Address	Duration	Expires In
--------------	-------------	----------	------------

Item	Description
IPv6 Address	Shows IP address of device/host/PC
MAC Address	Shows the MAC address of the device/host/PC
Duration	Shows the device duration of being active
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.

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.3	51042	192.168.1.1	80	tcp	86399
127.0.0.1	45000	127.0.0.1	45032	udp	25

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

4.7 IGMP Info

Click **IGMP Info** to display the list of IGMP entries broadcasting through 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	Last Report Time	Total Time(sec)	Total Joins	Total Leaves
-----------	-----	--------	--------	---------	------------------	-----------------	-------------	--------------

Item	Description
Interface	The Source interface from which the IGMP report was received
WAN	The WAN interface from which the multicast traffic is received
Groups	The destination IGMP group address
Member	The Source IP from which the IGMP report was received
Timeout	The time remaining before the IGMP report expires
Last Report Time	The time of the last received IGMP report
Total Time(sec)	Total time that the IGMP stream has been played
Total Joins	Total IGMP join packets received for this IGMP address for this client
Total Leaves	Total IGMP leave packets received for this IGMP address for this client

4.8 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. Below this, a sidebar on the left contains a list of menu items: 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 two tables. The first table, 'General Info', has columns for Interface, Status, Address, and Prefix. The second table, 'General Info', lists device settings: Device Link-local Address (fe80::200:ff:fe55:5555/64), Default IPv6 Gateway, and IPv6 DNS Server.

Item	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 for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below this, a sidebar menu lists various system information sections: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, IPv6 Info, **IPv6 Neighbor**, and IPv6 Route. The main content area displays the 'Device Info -- IPv6 Neighbor Discovery table' with the following data:

IPv6 address	Flags	HW Address	Device
fe80::200:ff:fe55:5555	STALE	00:00:00:55:55:55	br0

Item	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

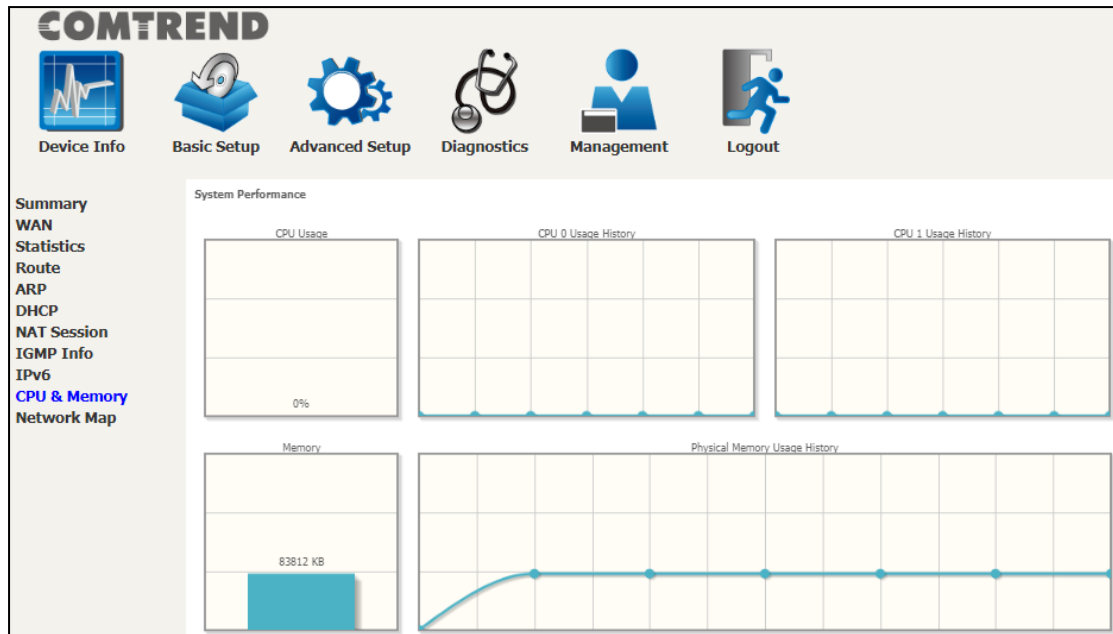
Click **IPv6 Route** to display the IPv6 route info.

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 system functions, with 'IPv6 Route' highlighted in blue. The main content area is titled 'Device Info -- IPv6 Route' and displays a table with the following columns: Destination, Gateway, Metric, and Interface.

Item	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.



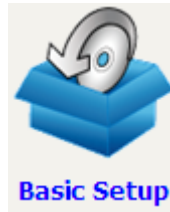
4.10 Network Map

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

The screenshot displays the COMTREND web interface. At the top, the COMTREND logo is visible. Below it is a navigation bar with six 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: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Info, IPv6, CPU & Memory, and Network Map (highlighted in blue). The main content area features a 'Device Scan' button at the top. The network map shows a central router icon connected to a computer icon on the right, which is labeled '192.168.1.3 (you)'. A vertical line labeled 'WAN Cable' extends upwards from the router, ending in a red 'X' symbol, indicating a disconnected WAN connection.

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

Router Limits

Parental Control

Home Networking

LAN

GE

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:00:00:55:55:55
DHCP Server	Enabled

WAN

DOWN

DSL 1 Status	Down
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
DSL 2 Status	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

38

Leading the **Communication Trend**

5.1 Wan Setup

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
 NAT
 LAN
 Router Limits
 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
------------------	-----------------	--------

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
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

Add Remove

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

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

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

5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

Step 2: Wide Area Network (WAN) Service Setup

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

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

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

Step 2: Wide Area Network (WAN) Service Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	<input checked="" type="radio"/>	<input type="button" value="Edit"/>
<input type="button" value="Add"/> <input type="button" value="Remove"/>														

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

Item	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
VlanTpid	VLAN Tag Protocol Identifier
IGMP Proxy	Shows Internet Group Management Protocol (IGMP) Proxy status
IGMP Source	Shows the status of WAN interface used as IGMP source
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD Proxy	Shows Multicast Listener Discovery (MLD) Proxy status
Mld Source	Shows the status of WAN interface used as MLD source

Remove	Select interfaces to remove
Edit	Click the Edit button to make changes to the WAN interface

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.

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

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.

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
 Router Limits
 Parental Control
 Home Networking

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: pppoe_0_0_35/ppp0.1

Service Name: Select One

Custom Service:

Server IP Address: 192.168.1.

Enable NAT Loopback

Apply/Save

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

Apply/Save

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

Consult the table below for field and header descriptions.

Item	Description
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 Or Custom Service	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
Enable NAT Loopback	Allows local machines to access virtual server via WAN IP Address
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

5.2.2 Port Triggering

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

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.

Buttons: 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: pppoe_0_0_35/ppp0.1

Application Name:

- Select an Application: Select One
- Custom Application:

Buttons: Save/Apply

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

Buttons: Save/Apply

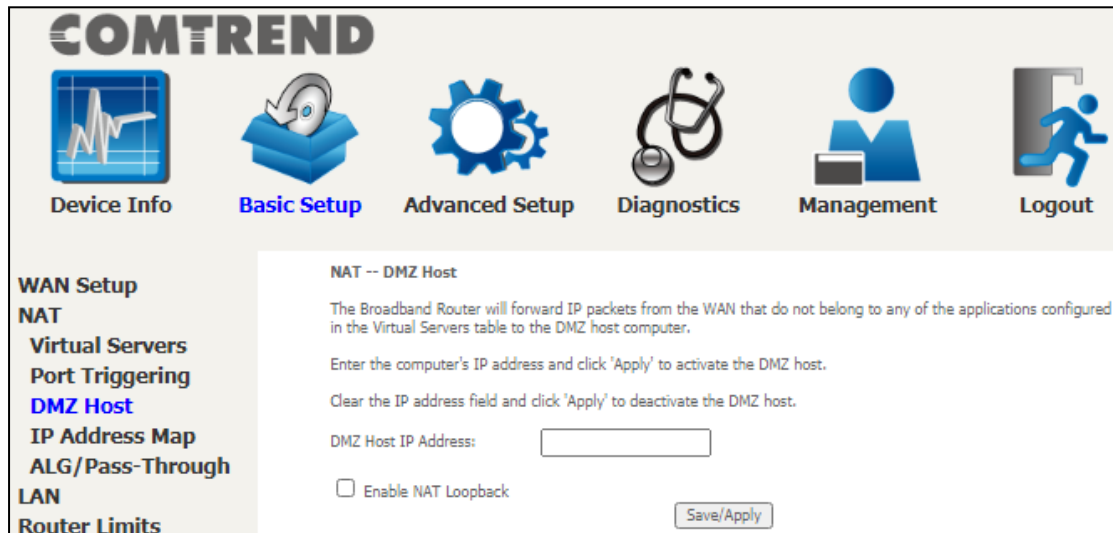
Click **Save/Apply** to save and apply the settings.

Consult the table below for field and header descriptions.

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

5.2.3 DMZ Host

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



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

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

Enable NAT Loopback 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).

Item	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

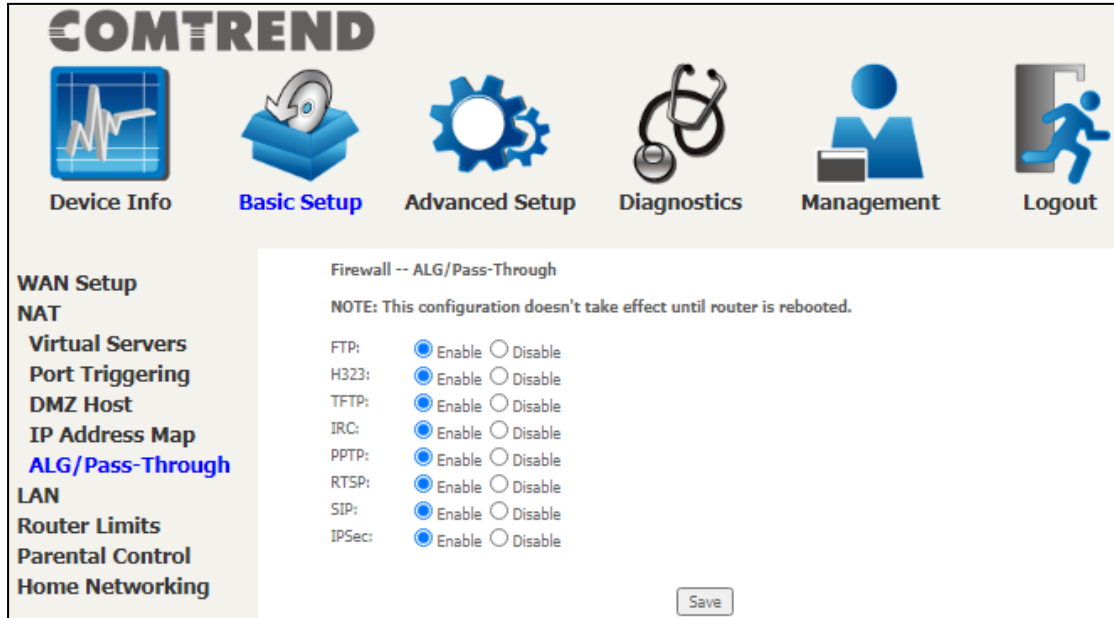
Many to one: mapping a range of local IP to a specific public IP

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.



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

5.3 LAN

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

The screenshot shows the 'Local Area Network (LAN) Setup' page in the COMTREND web interface. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with the following items: WAN Setup, NAT, LAN (highlighted), Lan VLAN Setting, IPv6 Autoconfig, Static IP Neighbor, UPnP, Router Limits, Parental Control, and Home Networking. The main content area is titled 'Local Area Network (LAN) Setup' and contains the following configuration options:

- Local Area Network (LAN) Setup**: Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName: **Default** (dropdown)
- IP Address: **192.168.1.1** (text box)
- Subnet Mask: **255.255.255.0** (text box)
- Enable IGMP Snooping
 - Standard Mode
 - Blocking Mode
- Enable IGMP LAN to LAN Multicast: **Disable** (dropdown)

(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: **192.168.1.2** (text box)
 - End IP Address: **192.168.1.254** (text box)
 - Leased Time (hour): **24** (text box)
- Setting TFTP Server
- Enable Automatic Static IP Reservation

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

MAC Address	IP Address	Remove

Add Entries | **Remove Entries**
- Enable DHCP Server Relay

DHCP Server IP Address:
- Configure the second IP Address and Subnet Mask for LAN interface
- Enable Spanning Tree
- Enable Ethernet@wirespeed on LAN ports (This feature enables LAN port connectivity over 2 pair Cat5 Ethernet cables)
- Ethernet Media Type**

GE: **Auto** (dropdown)

At the bottom right of the main content area, there is an **Apply/Save** button.

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

Enable IGMP Snooping:

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

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

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

Enable LAN side firewall: Enable by ticking the checkbox .

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

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

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

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

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

2ND LAN INTERFACE

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

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

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

Enable Spanning Tree:

Spanning Tree Protocol is a protocol that builds a loop-free logical topology for Ethernet networks. To enable, tick the checkbox .

Enable Ethernet@wirespeed on LAN ports:

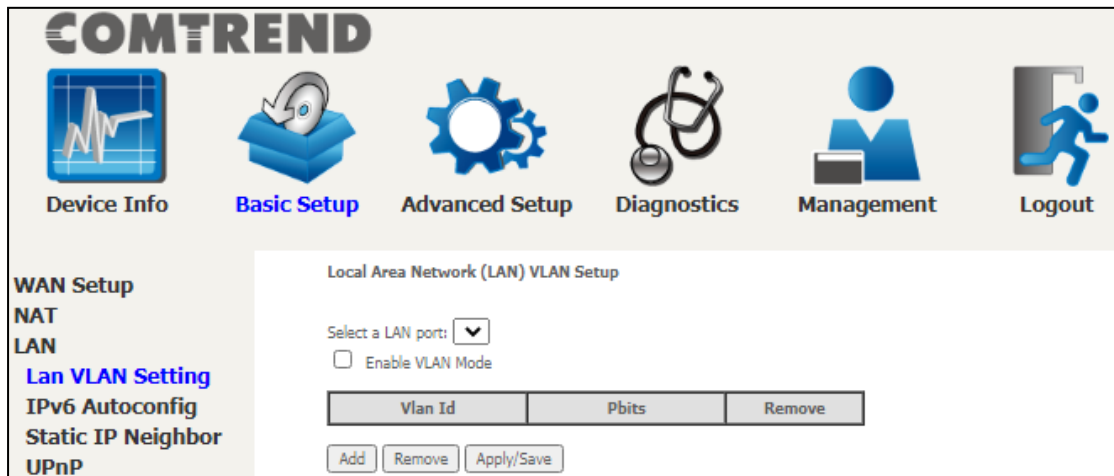
Enable to support 2 pair Cat5 Ethernet cables.

Ethernet Media Type:

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

5.3.1 Lan VLAN Setting

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



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

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

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

5.3.2 LAN IPv6 Autoconfig

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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

IPv6 LAN Auto Configuration
 Note: Stateful 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:

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

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

MAC Address	Interface ID	Remove

Enable SLAAC (RADVD)
 RA interval Min(sec):
 RA interval Max(sec):
 Reachable Time(ms):
 Default Preference:
 MTU (bytes):
 Enable Prefix Length Relay
 Enable Configuration Mode

Enable ULA Prefix Advertisement
 Randomly Generate
 Statically Configure
 Prefix:
 Preferred Life Time (hour):
 Valid Life Time (hour):

Enable MLD Snooping
 Standard Mode
 Blocking Mode

Enable MLD LAN to LAN Multicast:
 (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

Item	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

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

IPv6 LAN Applications

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

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

MAC Address	IP Address	Remove
Add Entries		Remove Entries

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

DHCP Static IP Lease

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

MAC Address:

Interface ID:

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

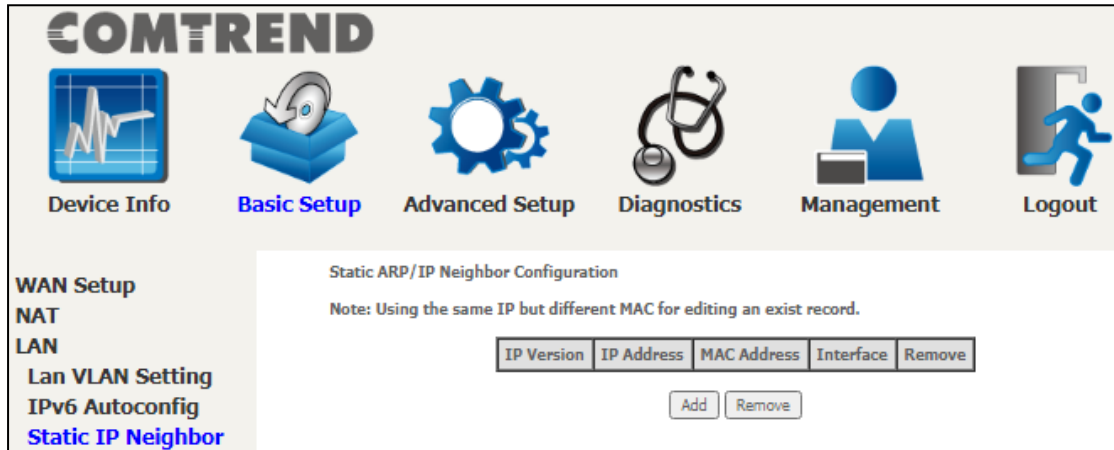
MAC Address	Interface ID	Remove
00:11:22:33:44:55	0:0:0:2	<input checked="" type="checkbox"/>
Add Entries		Remove Entries

Item	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix

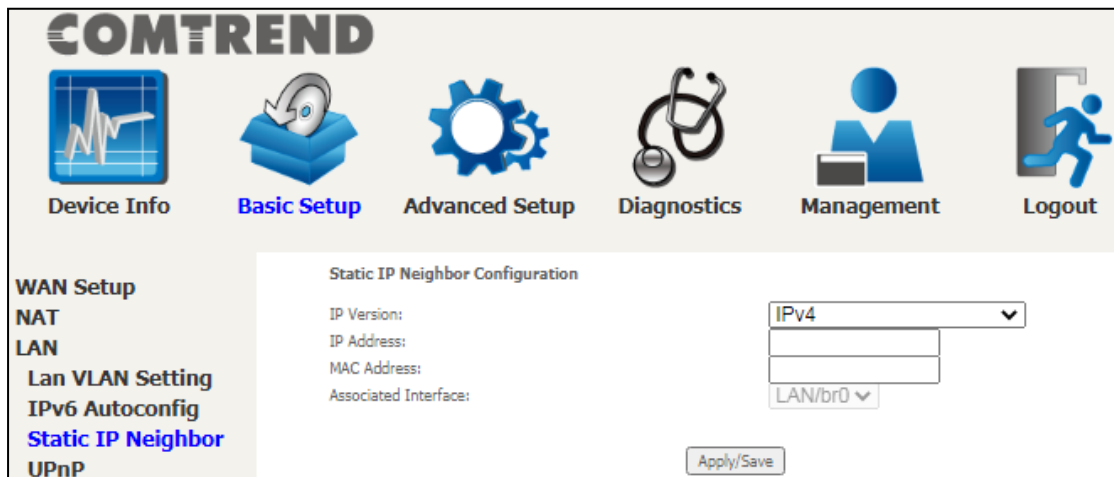
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure	Specify the prefix to be used
Prefix	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports
Standard Mode Blocking Mode	In standard mode, IPv6 multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if MLD snooping is enabled In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group
Enable MLD LAN To LAN Multicast	Enable/disable IPv6 multicast between LAN ports

5.3.3 Static IP Neighbor

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



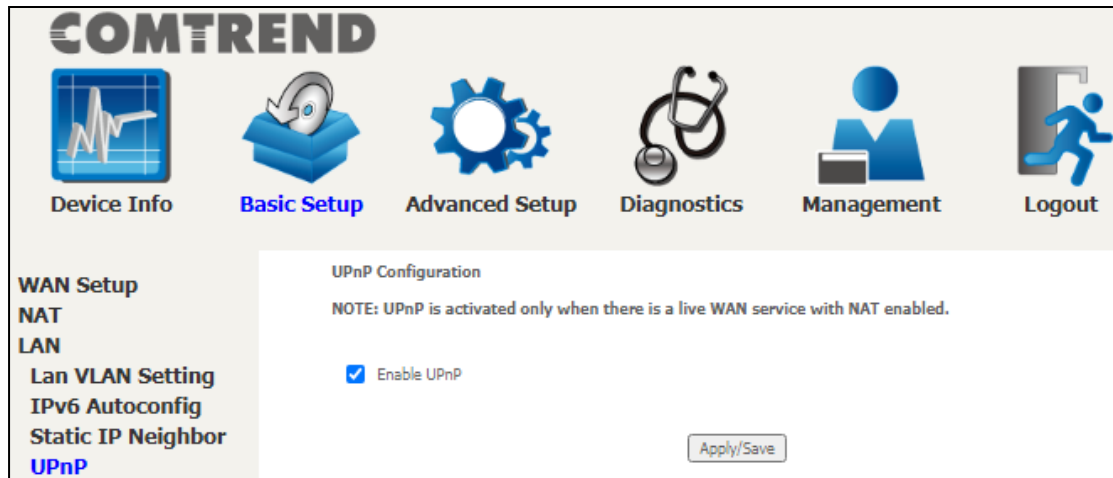
Click the **Add** button to display the following.



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

Item	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

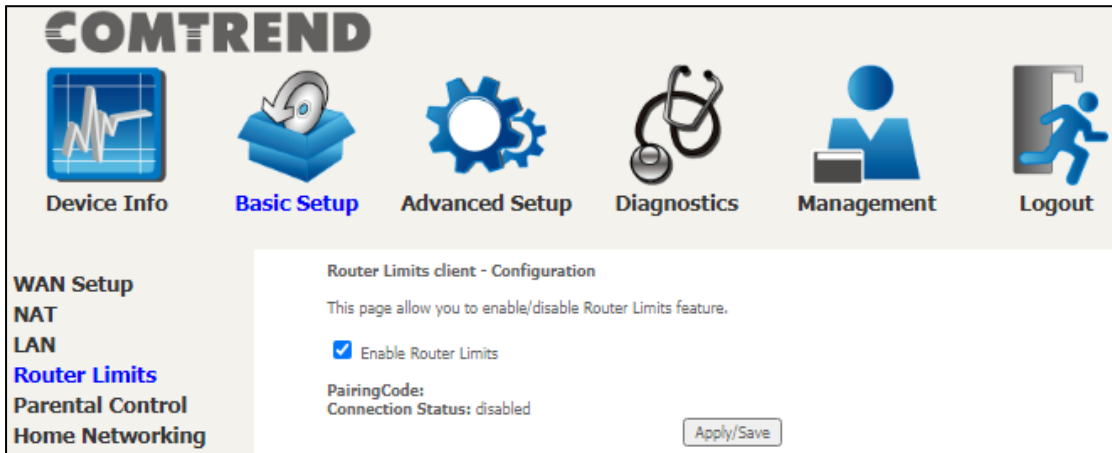
5.3.4 UPnP



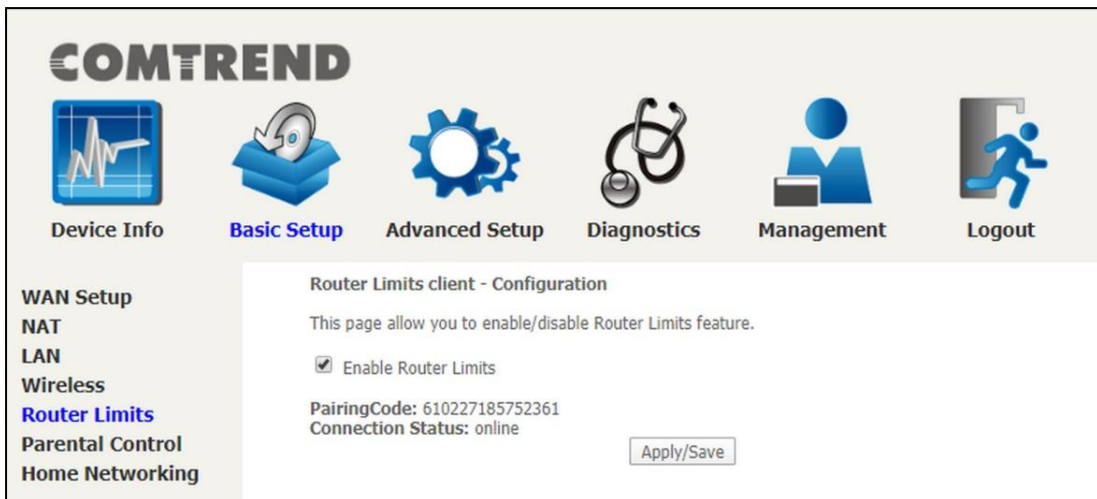
Select the checkbox provided and click **Apply/Save** to enable UPnP protocol.

5.4 Router Limits

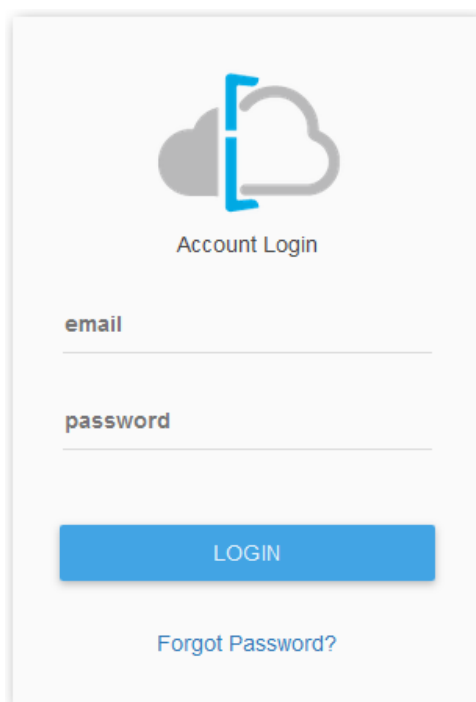
This page allows you to enable/disable the Router Limits feature.



Tick the checkbox and click **Apply/Save** to enable this feature. After Router Limits is enabled, PairingCode will be acquired.



Go to <https://portal.routerlimits.com/user>, the PairingCode will be needed to pair CPE device with Router Limits service after login.



The image shows a login form for an account. At the top, there is a logo consisting of a grey cloud with a blue bracket-like shape on its right side. Below the logo, the text "Account Login" is centered. The form contains two input fields: the first is labeled "email" and the second is labeled "password". Below these fields is a blue button with the text "LOGIN" in white. At the bottom of the form, there is a link that says "Forgot Password?".

For more details, please refer to www.routerlimits.com

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 WhiteList Time

This page provides time of day restriction blocking with white list. Only devices within the MAC address list can access the internet during the specified period. All other devices will be blocked from internet access.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
LAN
Router Limits
Parental Control
Time Restriction
WhiteList Time
URL Filter
Home Networking

Access Time Restriction - Whitelist

This page provides time of day restriction blocking with white list. Only devices within the MAC address list can access internet during the specified period. All other devices will be blocked from internet access.

Enable White List Time Restriction

MAC Address List: (Use comma to separate MAC addresses)

Days of the week

Mon	Tue	Wed	Thu	Fri	Sat	Sun
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

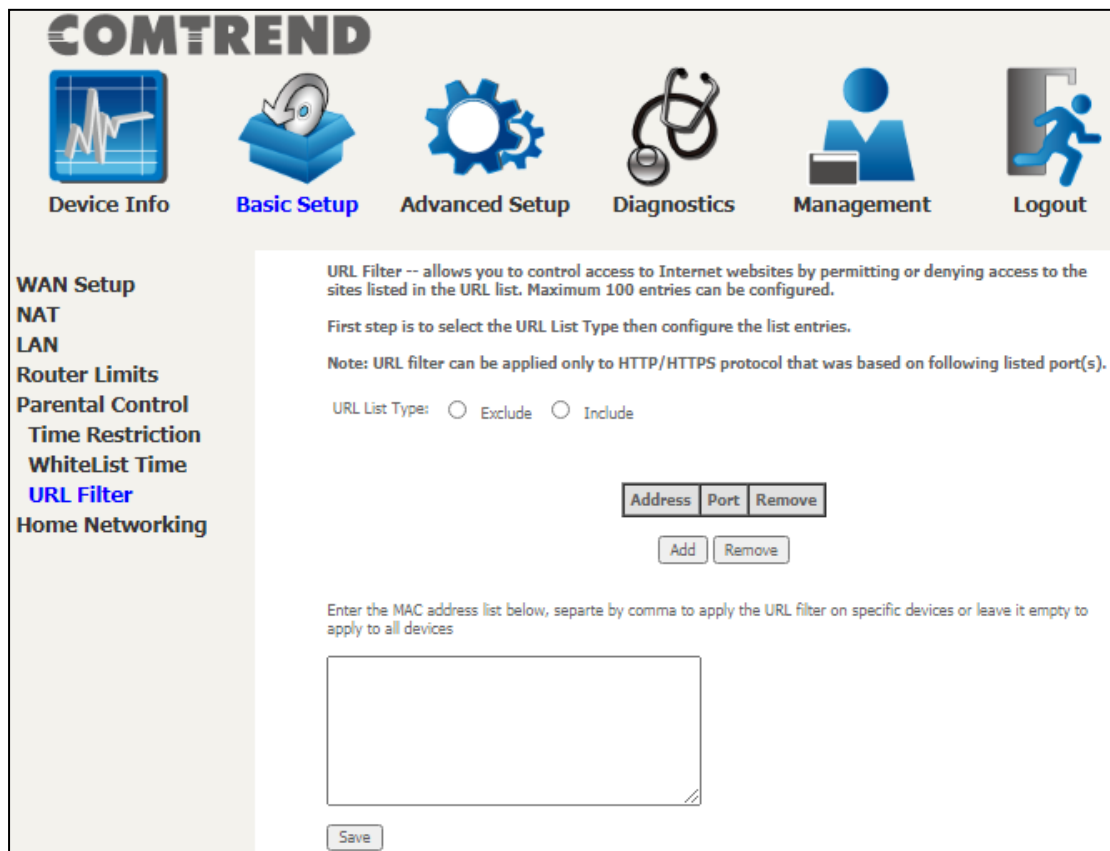
End Blocking Time (hh:mm)

Apply/Save

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

5.5.3 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.

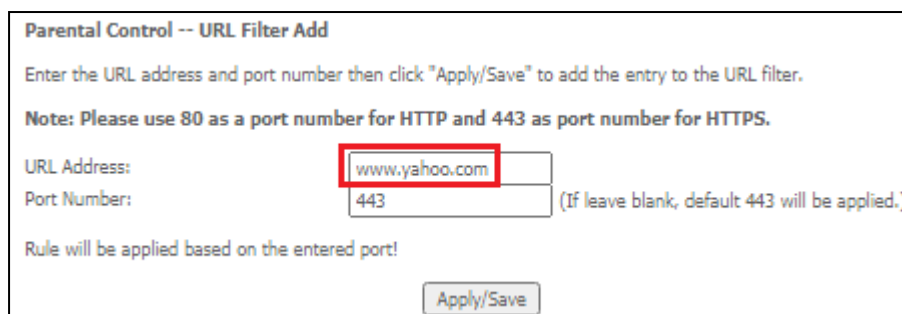


Select URL List Type: Exclude or Include.

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 -- allows you to control access to Internet websites by permitting or denying access to the sites listed in the URL list. Maximum 100 entries can be configured.

First step is to select the URL List Type then configure the list entries.

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

URL List Type: Exclude Include

Address	Port	Remove
www.yahoo.com	443	<input type="checkbox"/>

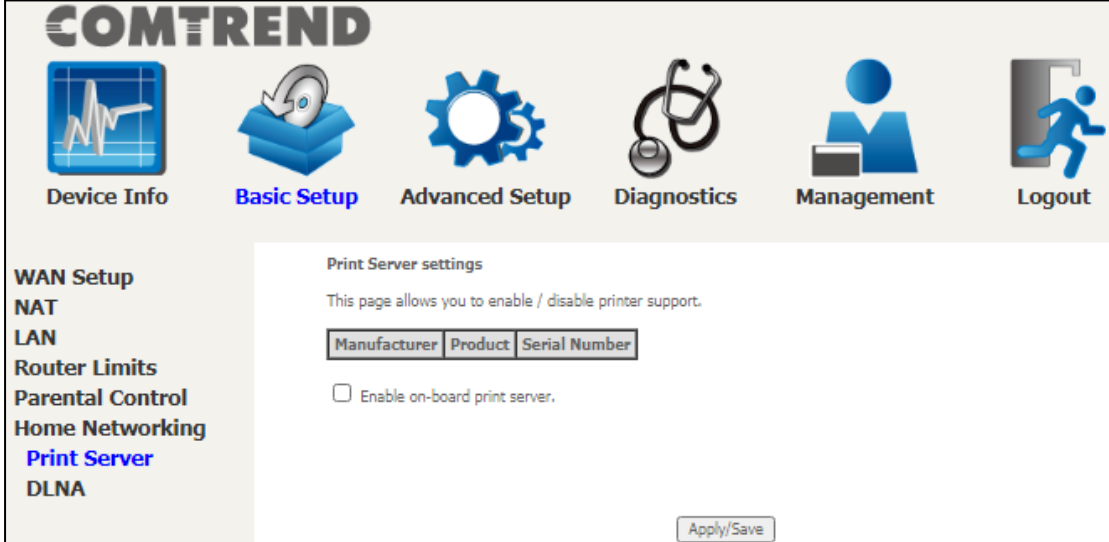
A maximum of 100 entries can be added to the URL Filter list.

5.6 Home networking

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

5.6.1 Print Server

This page allows you to enable or disable printer support.



The screenshot displays the COMTREND web interface. At the top, the COMTREND logo is visible. Below the logo, there are six navigation icons: Device Info (line graph), Basic Setup (CD/DVD), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). The left sidebar contains a list of menu items: WAN Setup, NAT, LAN, Router Limits, Parental Control, Home Networking, **Print Server** (highlighted in blue), and DLNA. The main content area is titled "Print Server settings" and contains the text: "This page allows you to enable / disable printer support." Below this text are three input fields labeled "Manufacturer", "Product", and "Serial Number". A checkbox labeled "Enable on-board print server." is present and is currently unchecked. An "Apply/Save" button is located at the bottom right of the settings area.

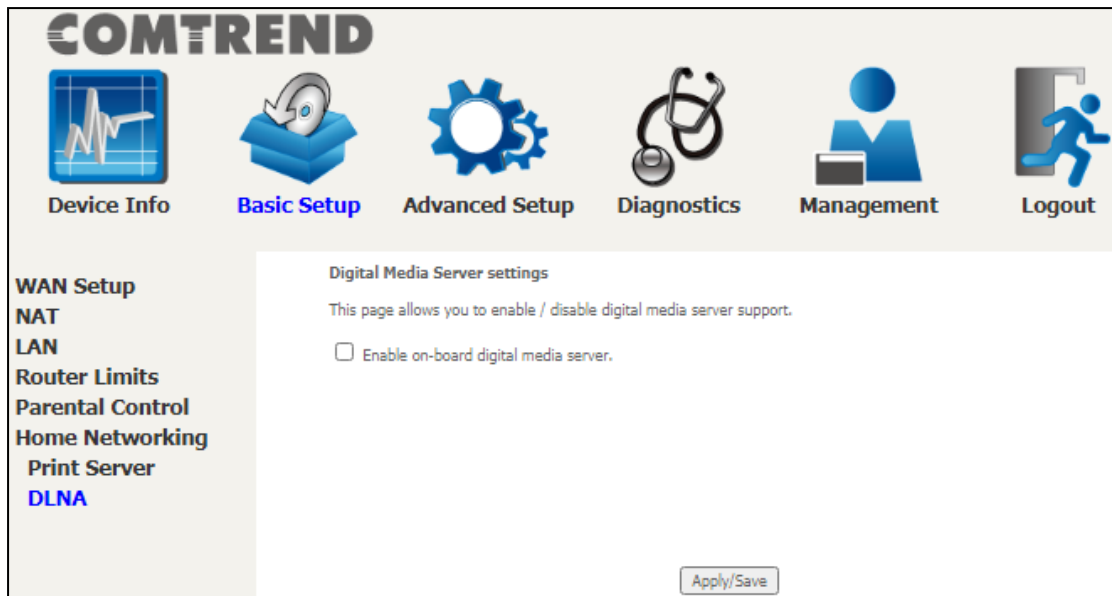
Please reference [Appendix E](#) to see the procedure for enabling the Printer Server.

5.6.2 DLNA

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

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.



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 icons and labels: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu with the following items: **Auto-Detection**, Security, Quality of Service, Routing, DNS, DSL, DSL Bonding, Interface Grouping, and IP Tunnel. 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 interfaces 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 the text, there is a checkbox labeled 'Enable auto-detect' which is currently unchecked. 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.

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

Multicast

Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interfaces 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:

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

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

PPP Username:

PPP Password:

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

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

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

69

Leading the Communication Trend

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	PPPoE
-1	IPoE
-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.

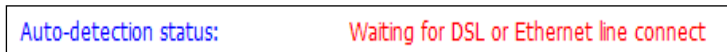
Options for each WAN service: These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

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

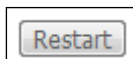
VLAN ID[0-4094]	Service	Option
-1	PPPoE ▾	<input type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input checked="" type="checkbox"/> IP extension

Auto Detection status and Restart

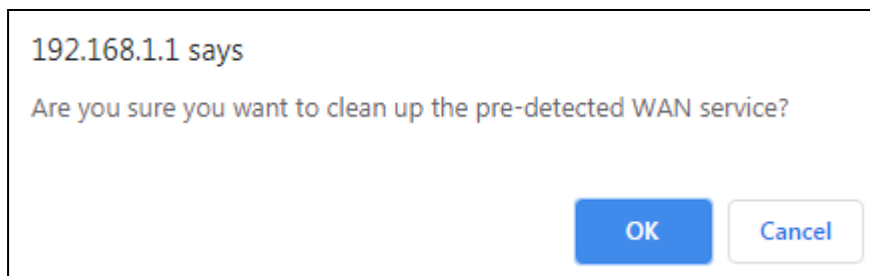
The Auto-detection status is used to display the real time status of the Auto-detection feature.



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 4th LAN port by default and allows it to be configured for any LAN port as well.
- 3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
- 4) If none of the pre-configured services are detected, a Bridge service will be created.

6.2 Security

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

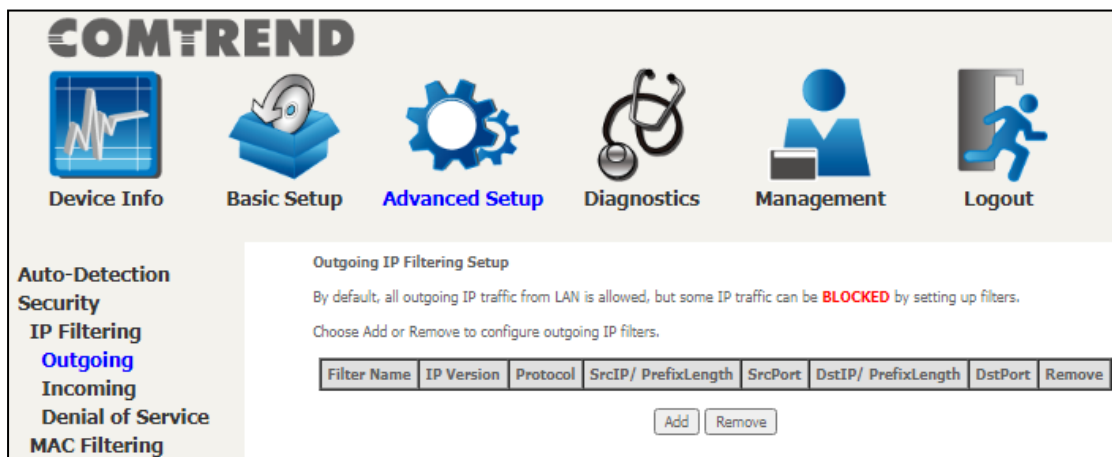
6.2.1 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead, [MAC Filtering](#) performs a similar function.

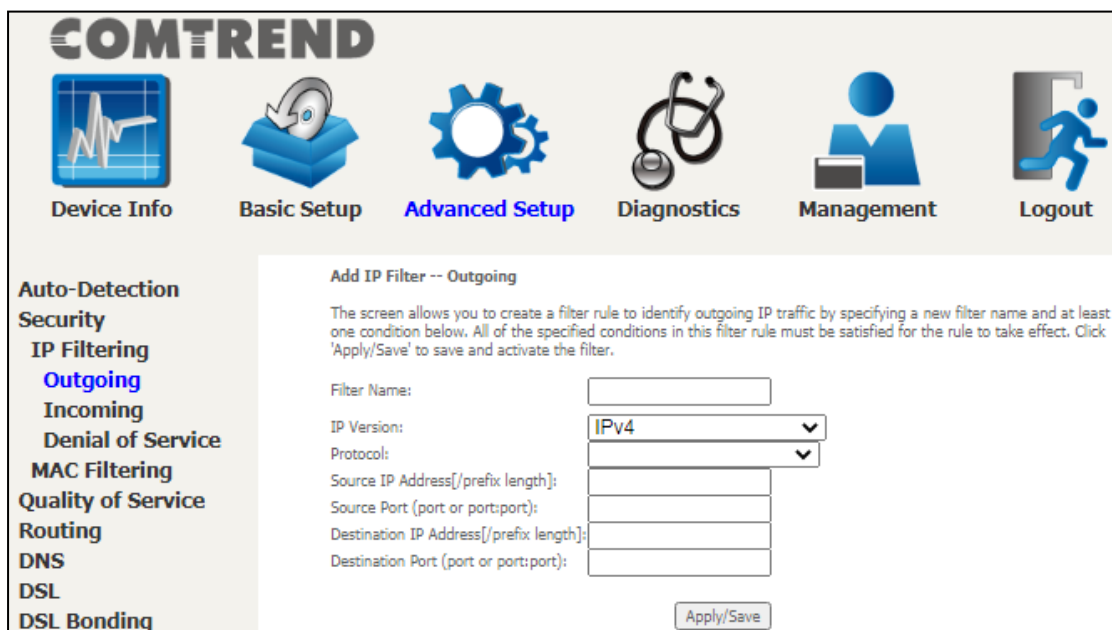
OUTGOING IP FILTER

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



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

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



Consult the table below for field descriptions.

Item	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.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options: Auto-Detection, Security, IP Filtering (Outgoing, **Incoming**), Denial of Service, MAC Filtering, and Quality of Service. The main content area is titled 'Incoming IP Filtering Setup'. It contains the following text: '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.' Below this text is a table with the following columns: Filter Name, Interfaces, IP Version, Protocol, Action, ICMP Type, SrcIP/PrefixLength, SrcPort, DstIP/PrefixLength, DstPort, and Remove. At the bottom of the table are 'Add' and 'Remove' buttons.

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

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

Consult the table below for field descriptions.

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

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

Denial of Service

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

COMTREND

Device Info Basic Setup **Advanced Setup** 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
 Multicast

Defend Against Denial of Service Attacks

This page allows you to activate/de-activate and set values for syn-flood protection, furtive port scan protection and ping of death protection. You can set the maximum average limit (packet per second) and the maximum burst (packet amount) for each protection. Please note that enabling the firewall will provide DoS protection. The DoS settings on this page are added traffic protections over the firewall to maximize Internet security, if needed. Click Apply/Save to save and activate/de-activate these protections.

DoS Protection	Enable	Maximum Average	Maximum Burst
Syn-Flood	<input type="checkbox"/>	3	10
Interfaces: <input type="checkbox"/> br0/br0			

DoS Protection	Enable	Maximum Average	Maximum Burst
Furtive Port Scan	<input type="checkbox"/>	3	10
Interfaces: <input type="checkbox"/> br0/br0			

DoS Protection	Enable	Maximum Average	Maximum Burst
Ping of Death	<input type="checkbox"/>	3	10
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 3130 can be set according to the following procedure.

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

COMTREND

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

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

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.

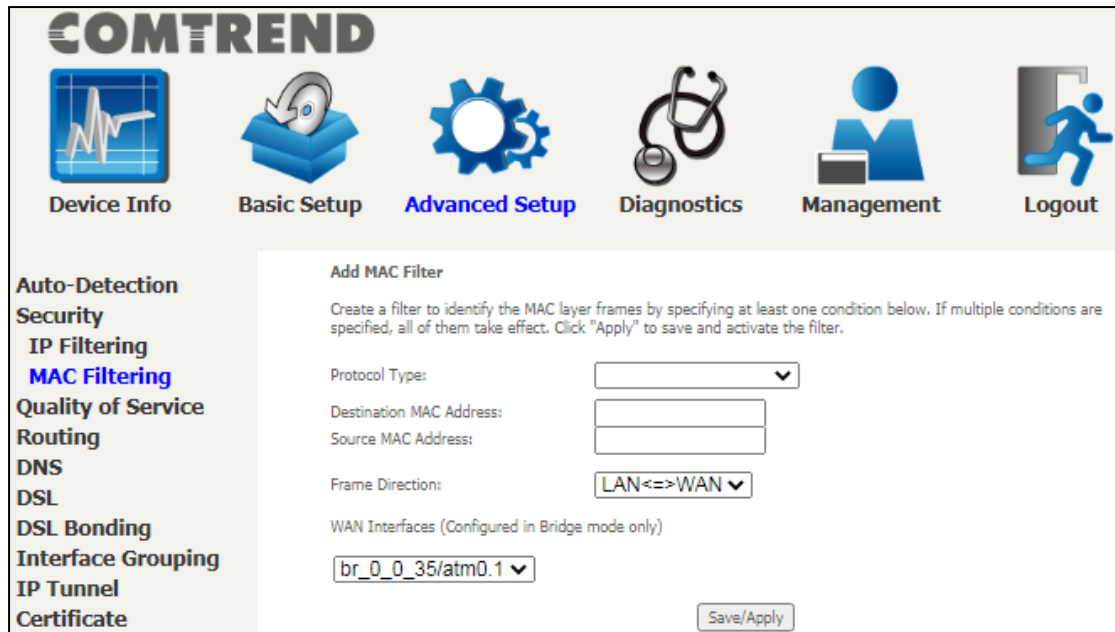
Interface	Policy	Change
atm0.1	FORWARD	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
Add Remove					

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



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

Consult the table below for detailed field descriptions.

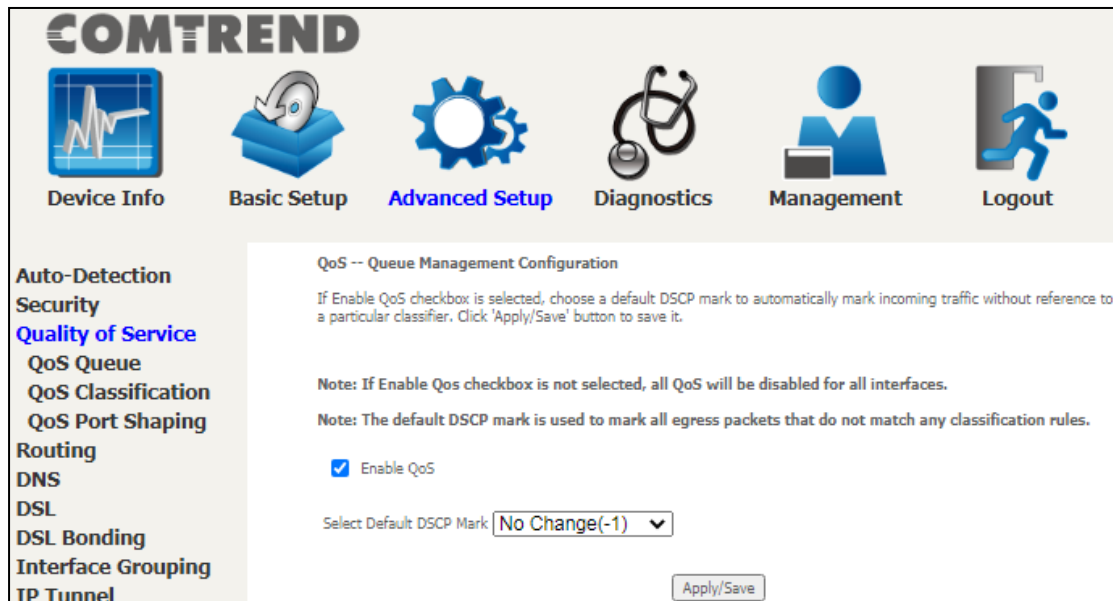
Item	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface

6.3 Quality of Service (QoS)

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

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

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



QoS and DSCP Mark are defined as follows:

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

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

6.3.1 QoS Queue

6.3.1.1 QoS Queue Configuration

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

In ATM mode, a maximum of 16 queues can be configured.

In PTM mode, a maximum of 8 queues can be configured.

For each Ethernet interface, a maximum of 8 queues can be configured.

For each Ethernet interface, a maximum of 8 queues can be configured.

(Please see the screen on the following page).

COMTREND

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

Auto-Detection
Security
Quality of Service
 QoS Queue
 Queue Configuration
 QoS Classification
 QoS Port Shaping
Routing
DNS
DSL
DSL Bonding
Interface Grouping
IP Tunnel
Certificate
Multicast

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 queue 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	eth0	8	1/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q7	2	eth0	7	2/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q6	3	eth0	6	3/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q5	4	eth0	5	4/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q4	5	eth0	4	5/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q3	6	eth0	3	6/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q2	7	eth0	2	7/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q1	8	eth0	1	8/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
Default Queue	9	atm0	1	8/WRR/1	Path0					<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Enable Remove

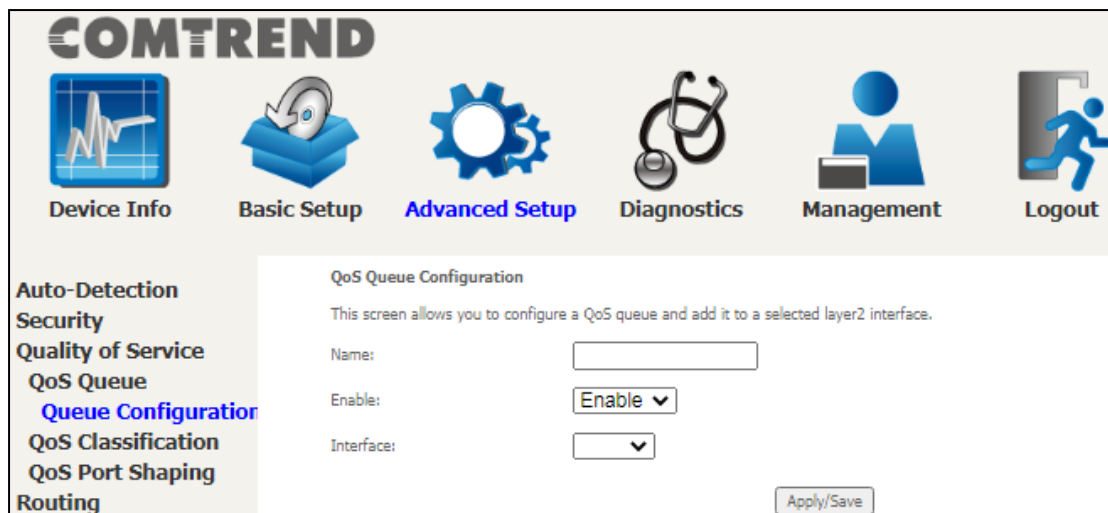
To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

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

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

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

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

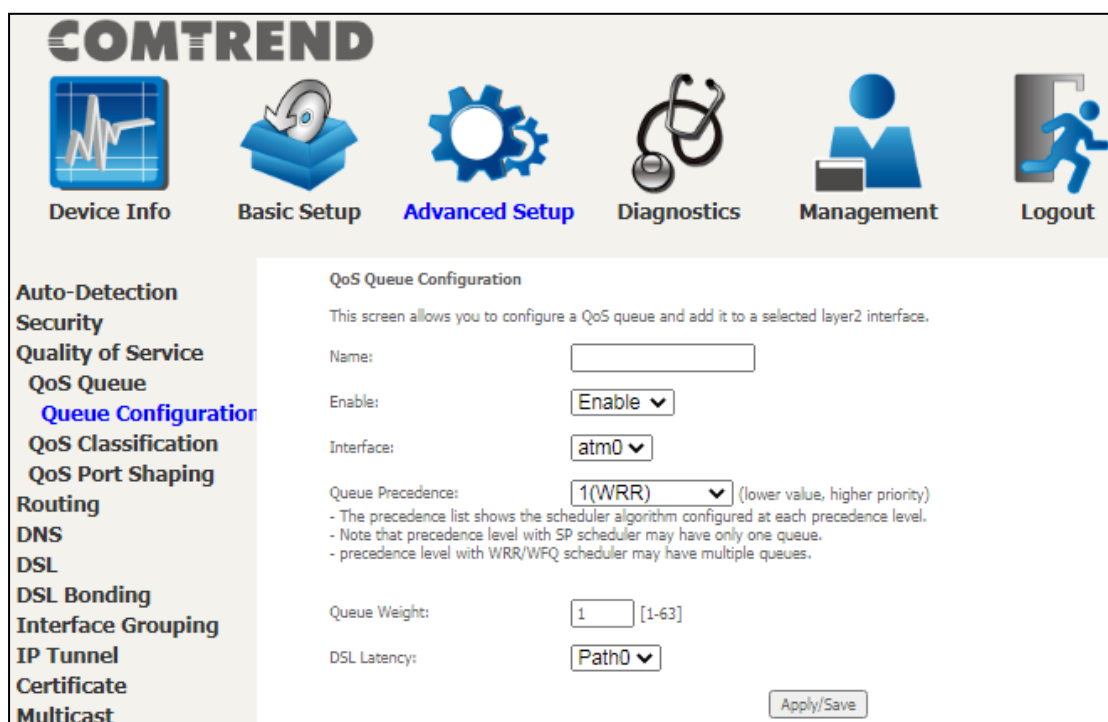


Name: Identifier for this Queue entry.

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.



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.

Queue Weight: A number to calculate queue priority based on Cisco IPP. The lower number gets the higher priority

DSL Latency: {Path0} → portID = 0

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

6.3.2 QoS Classification

The network traffic classes are listed in the following table.

COMTREND

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

Auto-Detection Security Quality of Service QoS Queue Queue Configuration **QoS Classification** QoS Port Shaping Routing

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

To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the rule after page reload.

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

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

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

Add Network Traffic Class Rule

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

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

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

Ingress Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

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

Specify Egress Interface (Required): ▼

Specify Egress Queue (Required): ▼

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

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

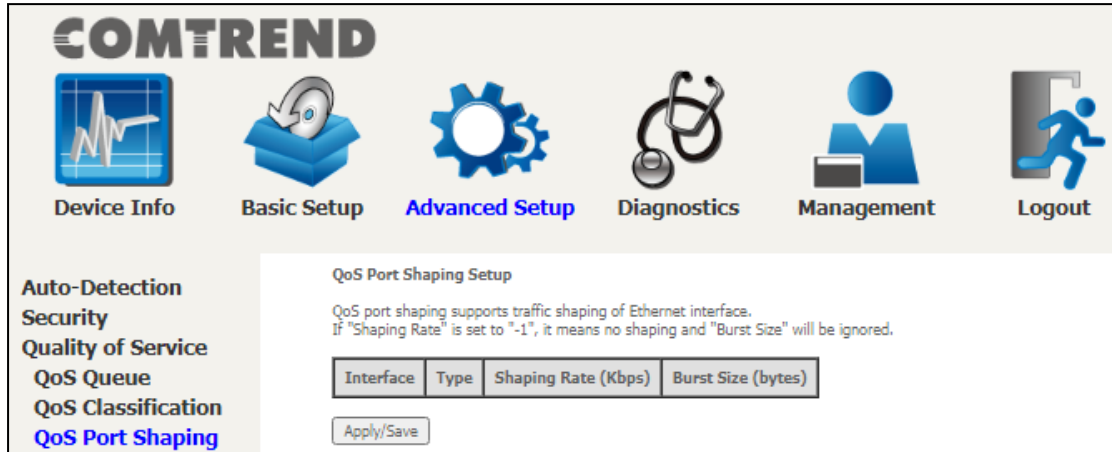
Set Rate Limit: [Kbits/s]

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

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.
Classification Criteria	
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.
Classification Results	
Specify Egress Interface	Choose the egress interface from the available list.
Specify Egress Queue	Choose the egress queue from the list of available for the specified egress interface.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. <ul style="list-style-type: none"> - Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits. - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added. - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits. - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.
Set Rate Limit	The data transmission rate limit in kbps.

6.3.3 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.



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.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
DSL
DSL Bonding
Interface Grouping
IP Tunnel
Certificate
Multicast

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

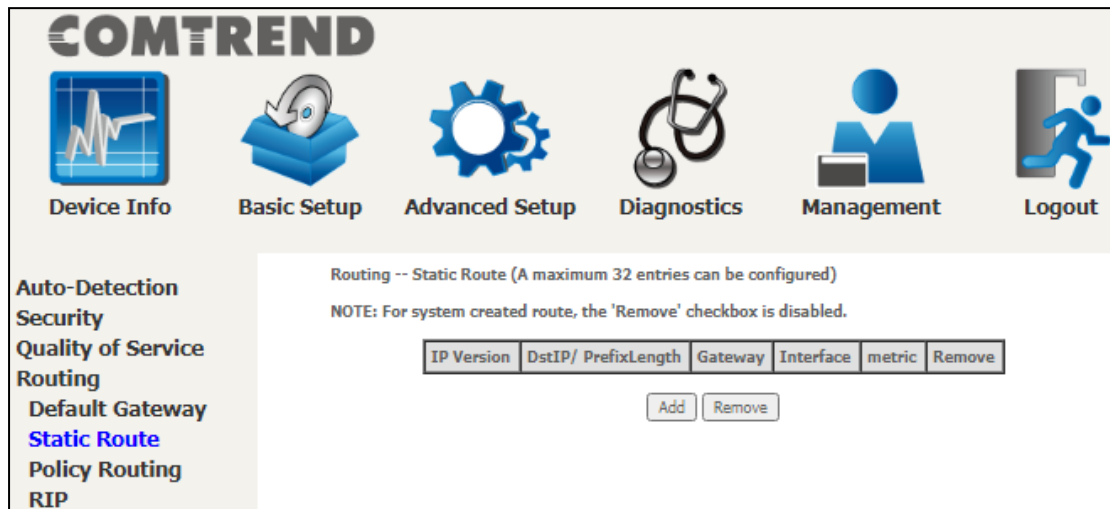
Selected WAN Interface **NO CONFIGURED INTERFACE**

Apply/Save

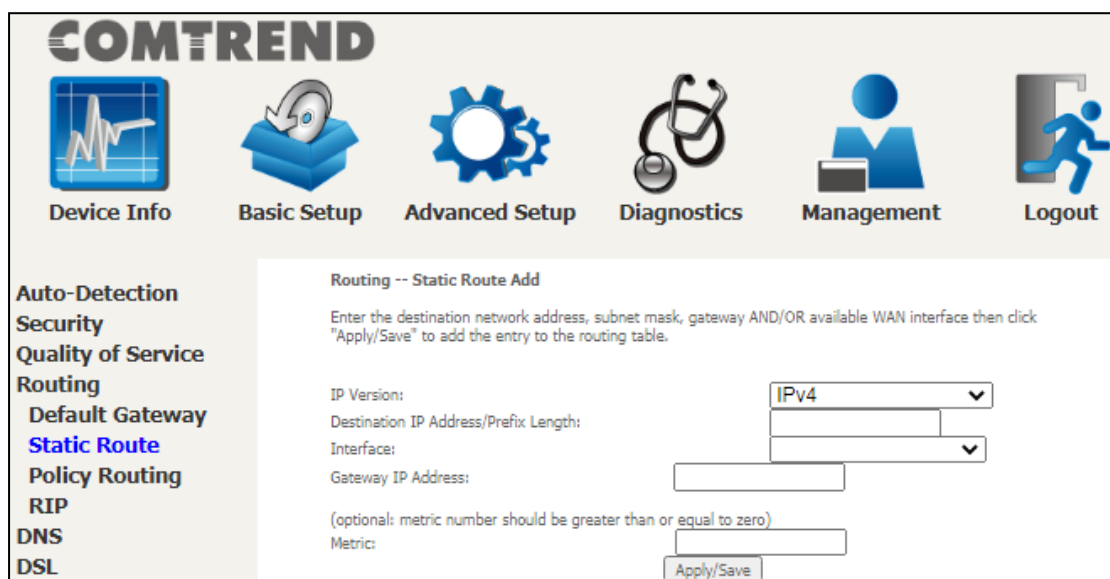
Click **Apply/Save** to apply and save the settings.

6.4.2 Static Route

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



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



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

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

6.4.3 Policy Routing

This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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

Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Add Remove

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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

Policy Routing Setup
Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Source IP:

Use Interface:

Default Gateway IP:

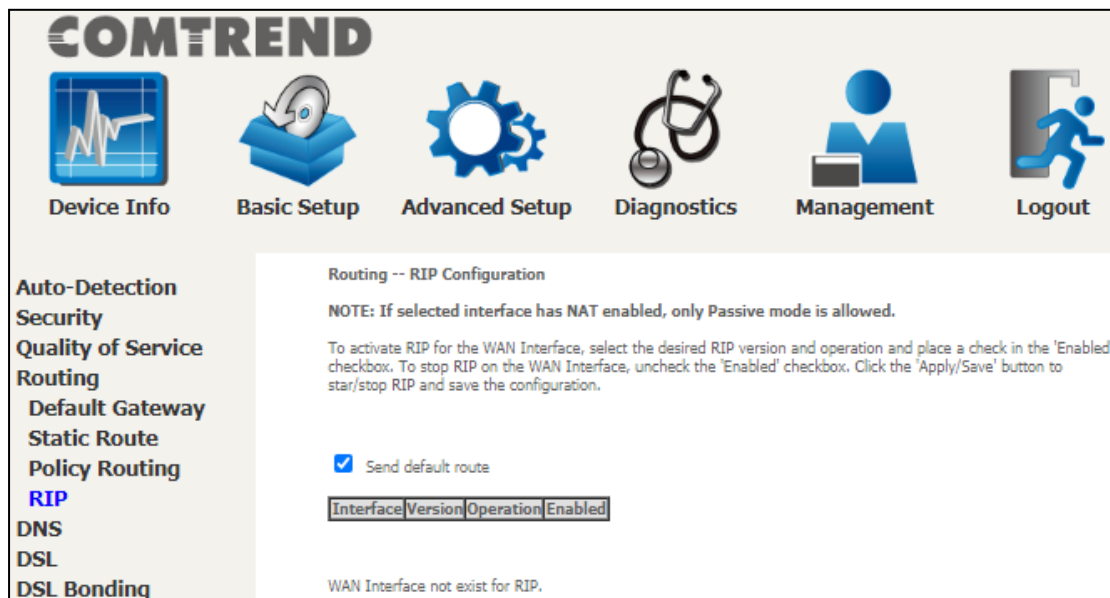
Apply/Save

Consult the table below for detailed item descriptions.

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

6.4.4 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**.



COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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

Routing -- RIP Configuration

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

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

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
Multicast

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS Server:

Secondary DNS Server:

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

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS Server:

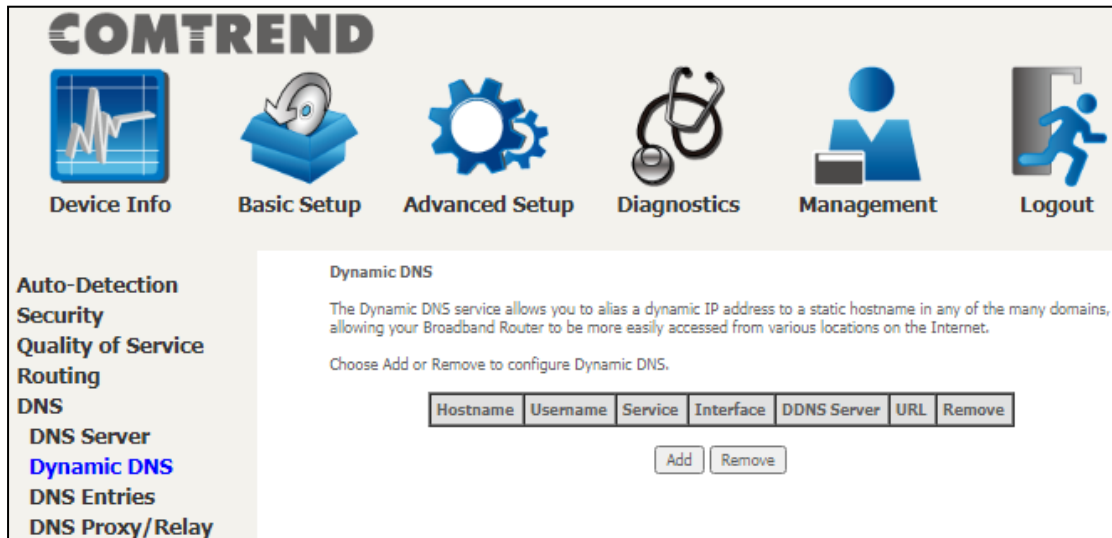
Secondary IPv6 DNS Server:

Apply/Save

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

6.5.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the NexusLink 3130 to be more easily accessed from various locations on the Internet.



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



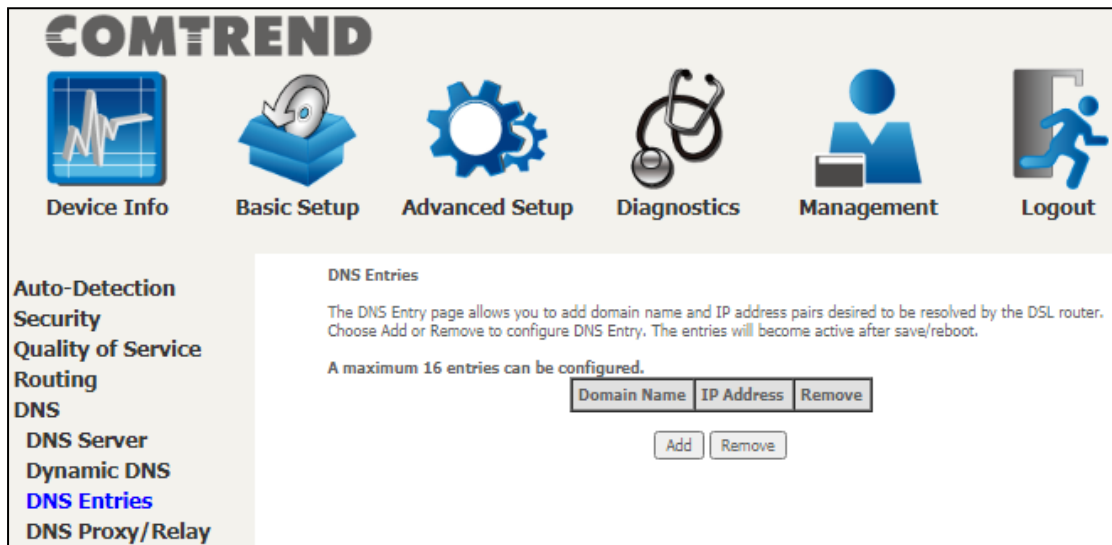
Click **Apply/Save** to save your settings.

Consult the table below for field descriptions.

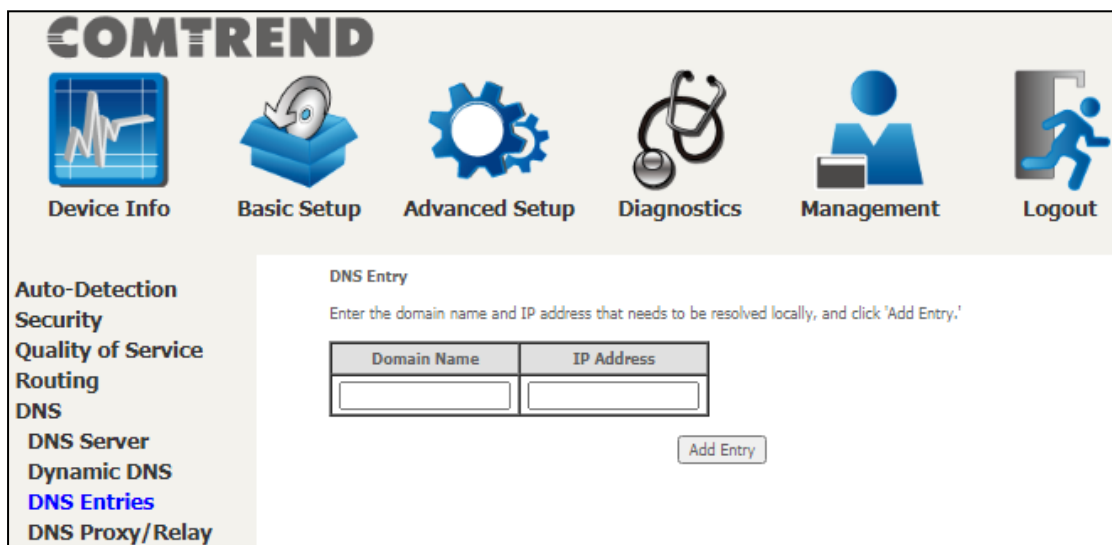
Item	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

6.5.3 DNS Entries

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



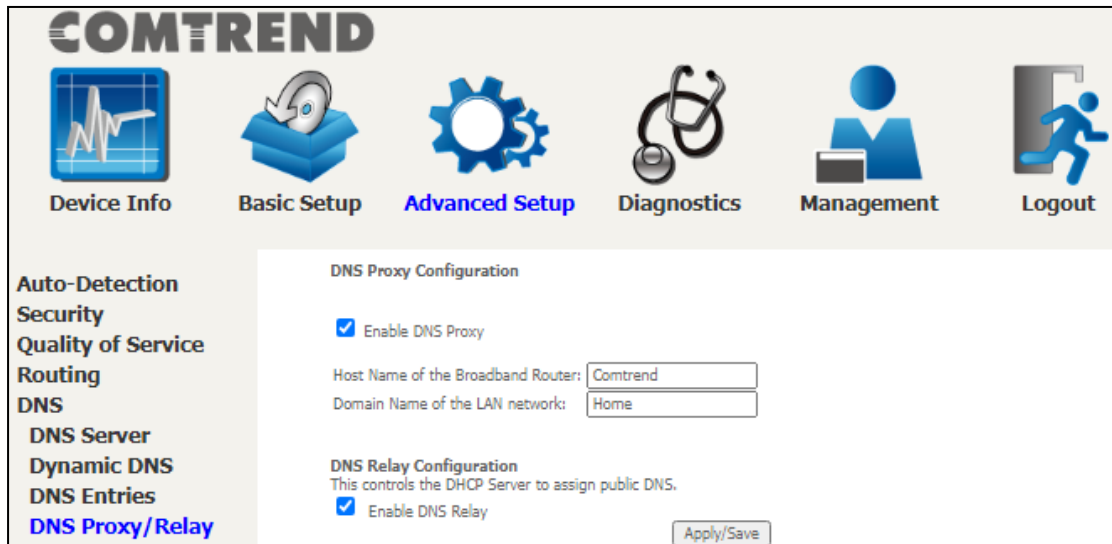
Choose Add or Remove to configure a DNS Entry. The entries will become active after save/reboot.



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

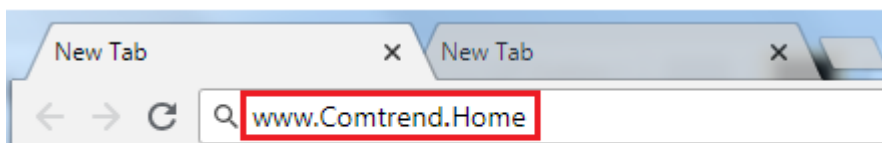
DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and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



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

See below for further details.

The Host Name and Domain Name are combined to form a unique label that is mapped to the router IP address. This can be used to access the WUI with a local name rather than by using the router IP address. The figure below shows an example of this. In the browser address bar (circled in red) the prefix "http://" is added to the local name "Comtrend.Home" [Host.Domain] for WUI access.



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.

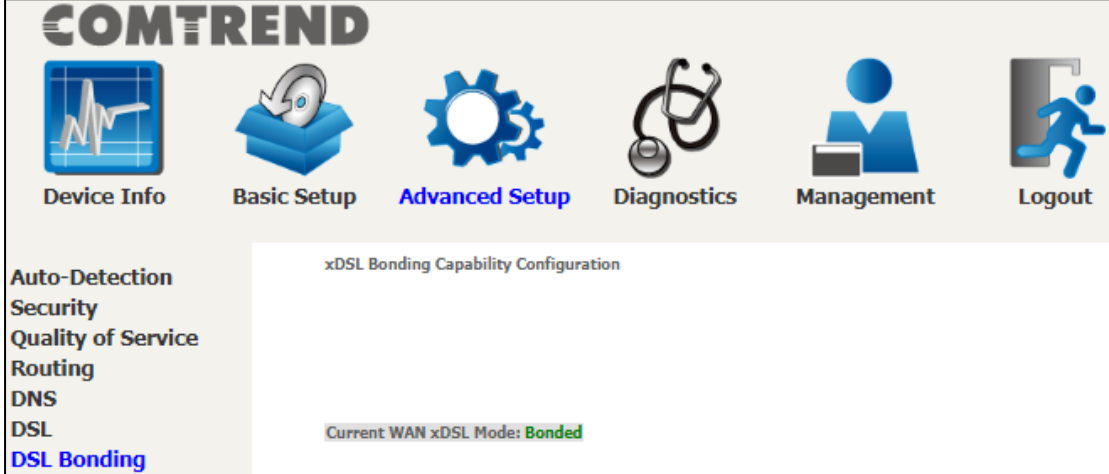
DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
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
35b	Downstream: 300
Options	Description
US0	Band between 20 and 138 kHz for long loops to upstream
Nitro Mode Sensing Enable	Nitro is a proprietary ATM header compression technique developed by Broadcom. It can provide throughput improvement when applied.
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
Select DSL LED behavior	Configure CPE to be complied with TR-68 ADSL requirements
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, the COMTREND logo is displayed. Below the logo is a navigation menu with six icons and labels: Device Info (line graph), Basic Setup (CD/DVD), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). Below the navigation menu is a sidebar with a list of menu items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, and DSL Bonding (highlighted in blue). The main content area is titled "xDSL Bonding Capability Configuration" and displays the text "Current WAN xDSL Mode: Bonded" in green.

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.

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

Interface Grouping -- A maximum 16 entries can be configured

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.

Group Name	Remove	Edit	WAN Interface	LAN Interfaces	DHCP Vendor IDs	MAC Address
Default						

Add Remove

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



Device Info



Basic Setup



Advanced Setup



Diagnostics



Management



Logout

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

Interface grouping Configuration

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

Here are the steps to create an Interface Group feature:

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

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

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

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

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

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

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

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

Group Name:

Grouped WAN Interfaces

Available WAN Interfaces

Grouped LAN Interfaces

Available LAN Interfaces

GE

Automatically Add Clients With the following DHCP Vendor IDs

MAC Address Match List for Any Port Any WAN

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.

The screenshot shows the COMTREND web interface. 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 **IP Tunnel** selected and **IPv6inIPv4** highlighted. The main content area displays the 'IP Tunneling -- 6in4 Tunnel Configuration' page. It features a table with columns: Name, WAN, LAN, Dynamic, IPv4 Mask Length, 6rd Prefix, Border Relay Address, and Remove. Below the table are 'Add' and 'Remove' buttons.

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

The screenshot shows the COMTREND web interface. 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 **IP Tunnel** selected and **IPv6inIPv4** highlighted. The main content area displays the 'IP Tunneling -- 6in4 Tunnel Configuration' page. It shows a message: 'Currently, only 6rd configuration is supported.' Below this, there are configuration fields: Tunnel Name (text input), Mechanism (dropdown menu with '6RD' selected), Associated WAN Interface (dropdown menu), Associated LAN Interface (dropdown menu with 'LAN/br0' selected), and radio buttons for Manual (selected) and Automatic. At the bottom, there are input fields for IPv4 Mask Length, 6rd Prefix with Prefix Length, and Border Relay IPv4 Address, followed by an 'Apply/Save' button.

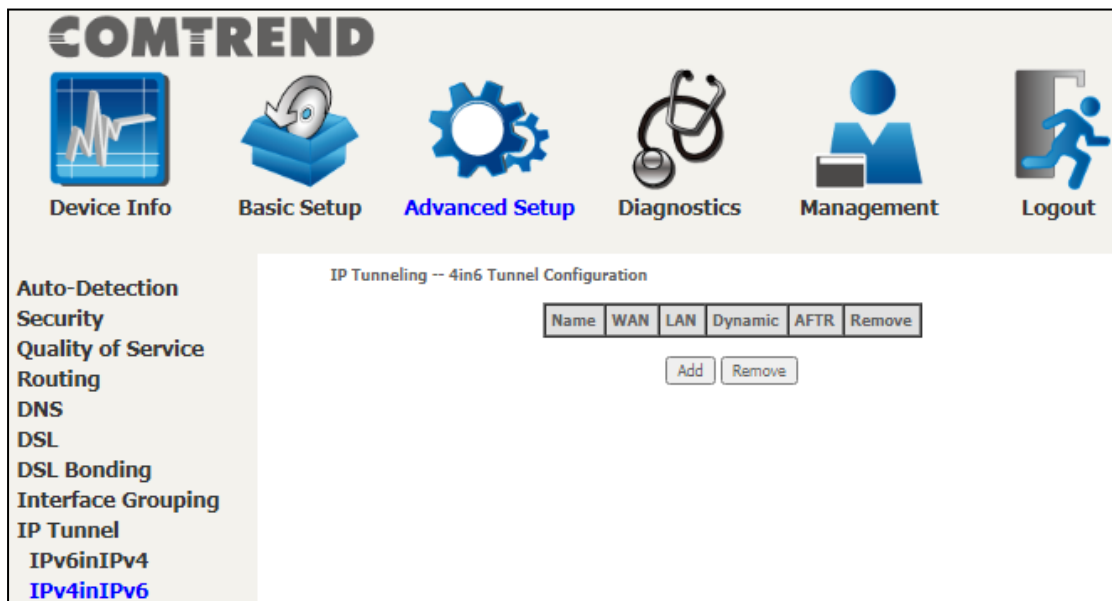
Click **Apply/Save** to apply and save the settings.

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

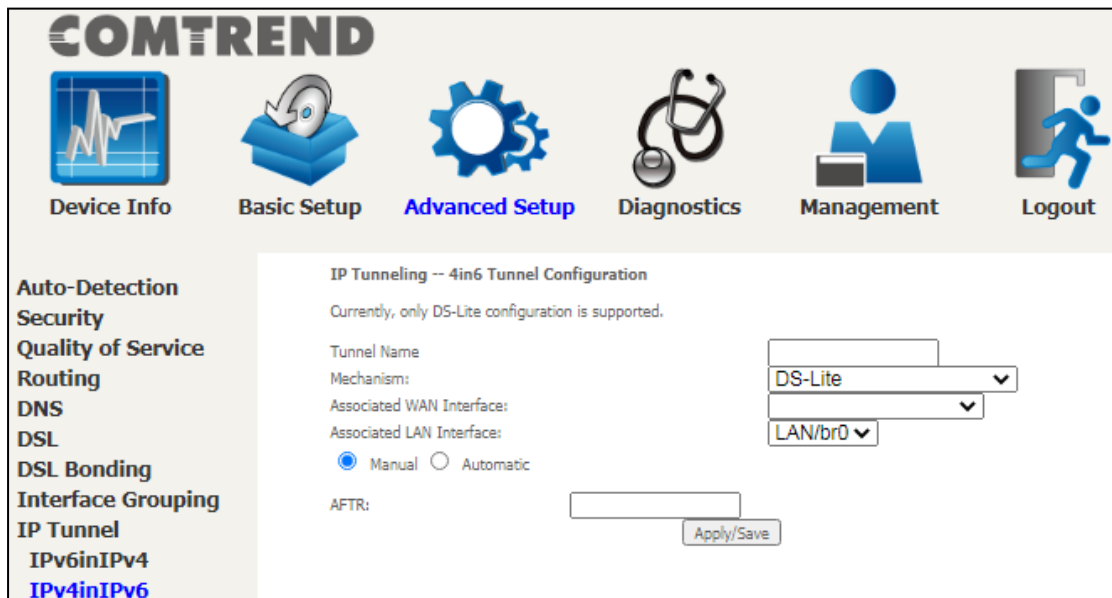
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used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

6.9.2 IPv4inIPv6

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



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



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

Item	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel

Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router

6.10 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

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
Local
Trusted CA

Local Certificates
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
<input type="button" value="Create Certificate Request"/> <input type="button" value="Import Certificate"/>				

CREATE CERTIFICATE REQUEST

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

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

The 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** (highlighted), 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, Local (highlighted), and Trusted CA. The main content area displays the 'Create new certificate request' form. The form includes a heading, a brief instruction, and five input fields: Certificate Name, Common Name, Organization Name, State/Province Name, and Country/Region Name (a dropdown menu currently showing 'US (United States)'). An 'Apply' button is located at the bottom right of the form.

The following table is provided for your reference.

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

IMPORT CERTIFICATE

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

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
Local
Trusted CA
Multicast

Import certificate
Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate Public Key:

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

Certificate Private Key:

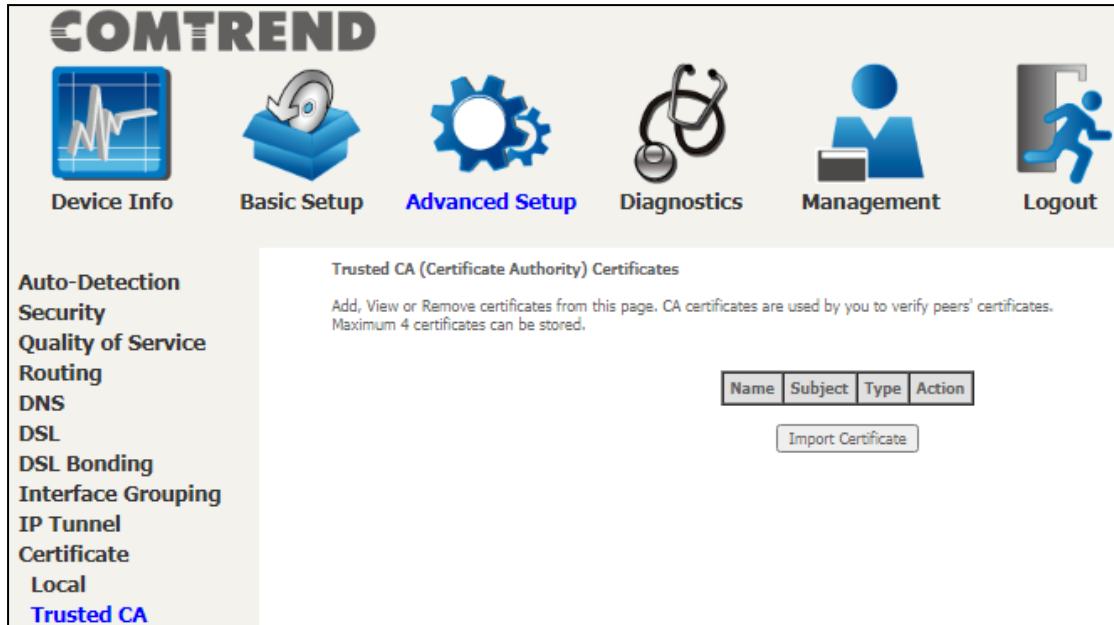
```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Apply

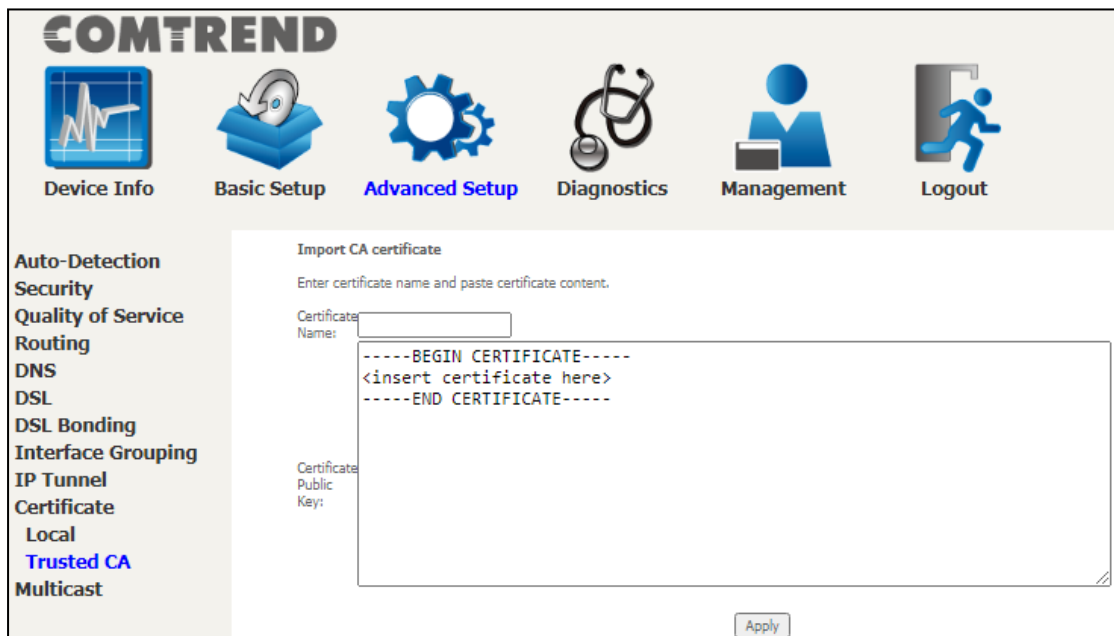
Enter a certificate name and click the **Apply** button to import the certificate and its private key.

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.



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



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

6.11 Multicast

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

Multicast Precedence: lower value, higher priority

Multicast Strict Grouping Enforcement:

IGMP Configuration
Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:
 Query Interval:
 Query Response Interval:
 Last Member Query Interval:
 Robustness Value:
 Maximum Multicast Groups:
 Maximum Multicast Data Sources (for IGMPv3):
 Maximum Multicast Group Members:
 Fast Leave Enable:

IGMP Group Exception List

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

MLD Configuration
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:
 Query Interval:
 Query Response Interval:
 Last Member Query Interval:
 Robustness Value:
 Maximum Multicast Groups:
 Maximum Multicast Data Sources (for mldv2):
 Maximum Multicast Group Members:
 Fast Leave Enable:

MLD Group Exception List

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

Multicast Precedence: Select precedence of multicast packets.

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

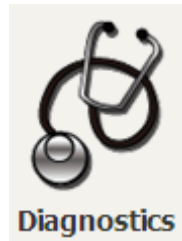
Item	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response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

IGMP Group Exception List / MLD Group Exception List

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

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		Device	
GE		Model	NexusLink 3130
LAN IPv4 Address	192.168.1.1	Serial Number	0
LAN Subnet Mask	255.255.255.0	Firmware Version	V011-416CTU-C01_R01.A2pvbH042x5.d27i
LAN MAC Address	00:00:00:55:55:55	Bootloader (CFE) Version	1.0.38-118.8-14
DHCP Server	Enabled	Up Time	3 mins:35 secs
DHCP IP Range	192.168.1.2 - 192.168.1.254	System Log	<input type="button" value="Show"/>

Click the Diagnostics Menu item on the left side of the screen to display the LAN connection.

Diagnostics

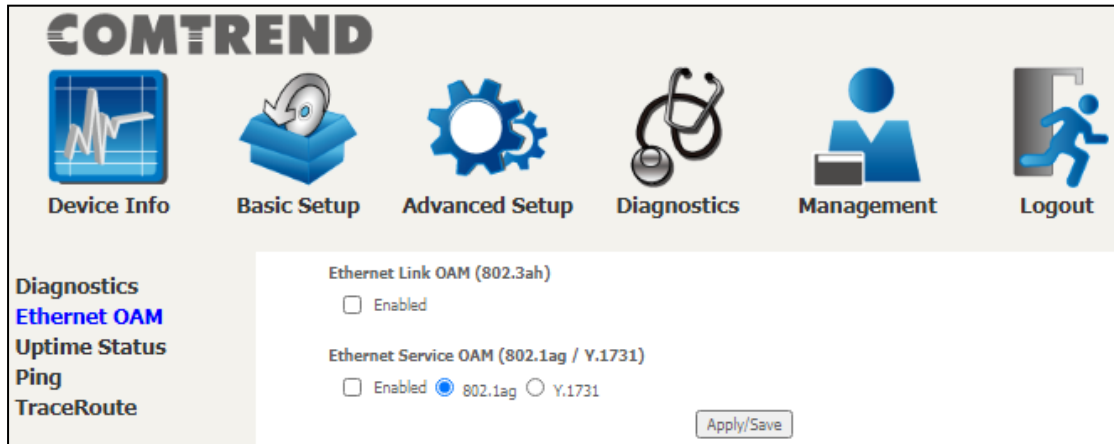
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your GE Connection: PASS [Help](#)

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.

Ethernet Link OAM (802.3ah)

Enabled

WAN Interface:

OAM ID: (positive integer)

Auto Event

Variable Retrieval

Link Events

Remote Loopback

Active Mode

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

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

Ethernet Service OAM (802.1ag / Y.1731)

Enabled 802.1ag Y.1731

WAN Interface:

MD Level: [0-7]

MD Name: [e.g. Broadcom]

MA ID: [e.g. BRCM]

Local MEP ID: [1-8191]

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

CCM Transmission

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

Loopback and Linktrace Test

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

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

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

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

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

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

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

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

7.3 Uptime Status

This page shows System, 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 10 mins:5 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=0.258 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.376 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.338 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.342 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.258/0.328/0.376 ms
    
```

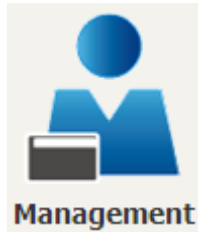
7.5 Trace Route

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

The screenshot displays the COMTREND web interface. At the top, the COMTREND logo is visible. Below the logo is a navigation menu with six icons and labels: Device Info (line graph), Basic Setup (floppy disk), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). On the left side, there is a vertical menu with the following items: Diagnostics, Ethernet OAM, Uptime Status, Ping, and TraceRoute (highlighted in blue). The main content area is titled 'TraceRoute' and contains the following text: 'Trace the route ip packets follow going to "host".' Below this is a form with the label 'TraceRoute IP Address / Hostname:' followed by an empty text input field and a 'TraceRoute' button. At the bottom of the form, there is a sample output: 'traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets' followed by '1 192.168.1.1 (192.168.1.1) 0.039 ms'.

Chapter 8 Management

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



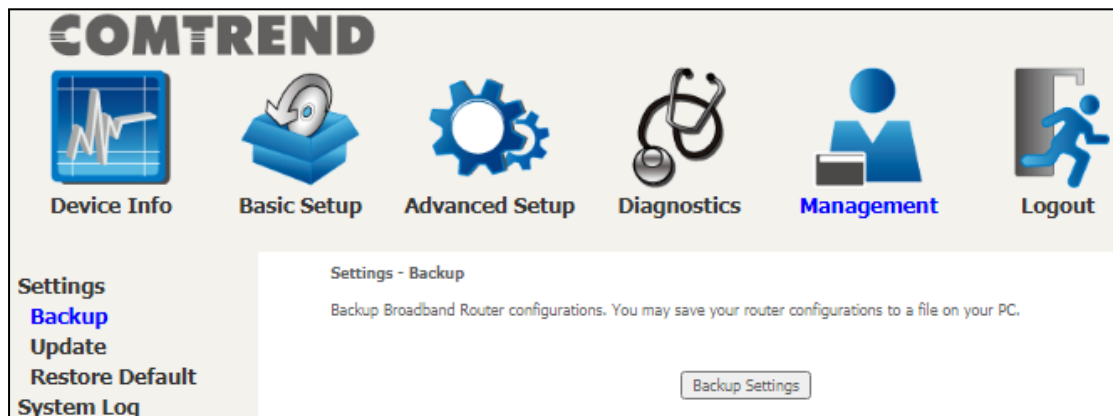
The Management menu has the following maintenance functions and processes:

8.1 Settings

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

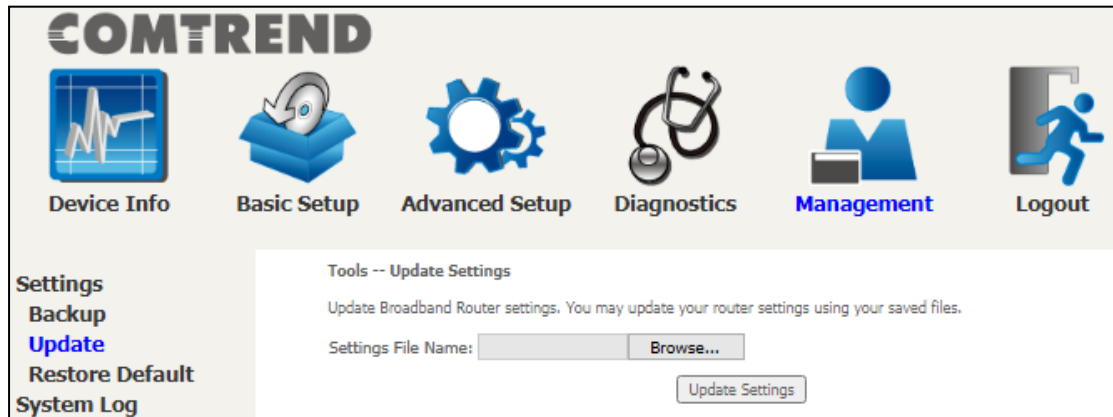
8.1.1 Backup Settings

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.



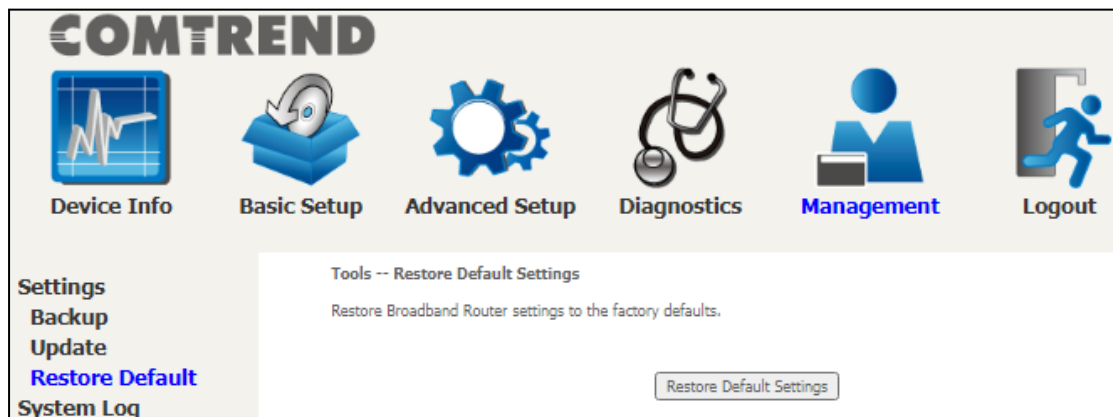
8.1.2 Update Settings

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.

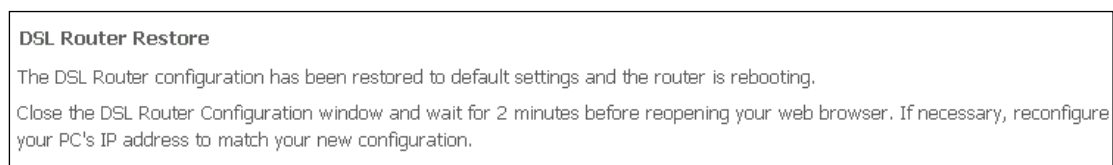


8.1.3 Restore Default

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



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



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.

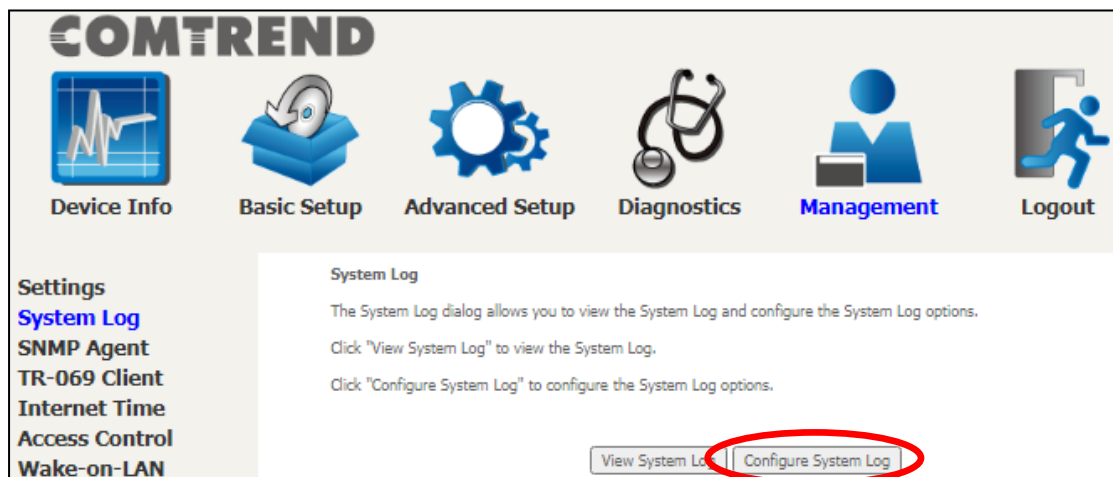
NOTE: This entry has the same effect as the **Reset** button. The NexusLink 3130 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase all configuration data saved in flash memory and enter bootloader mode.

8.2 System Log

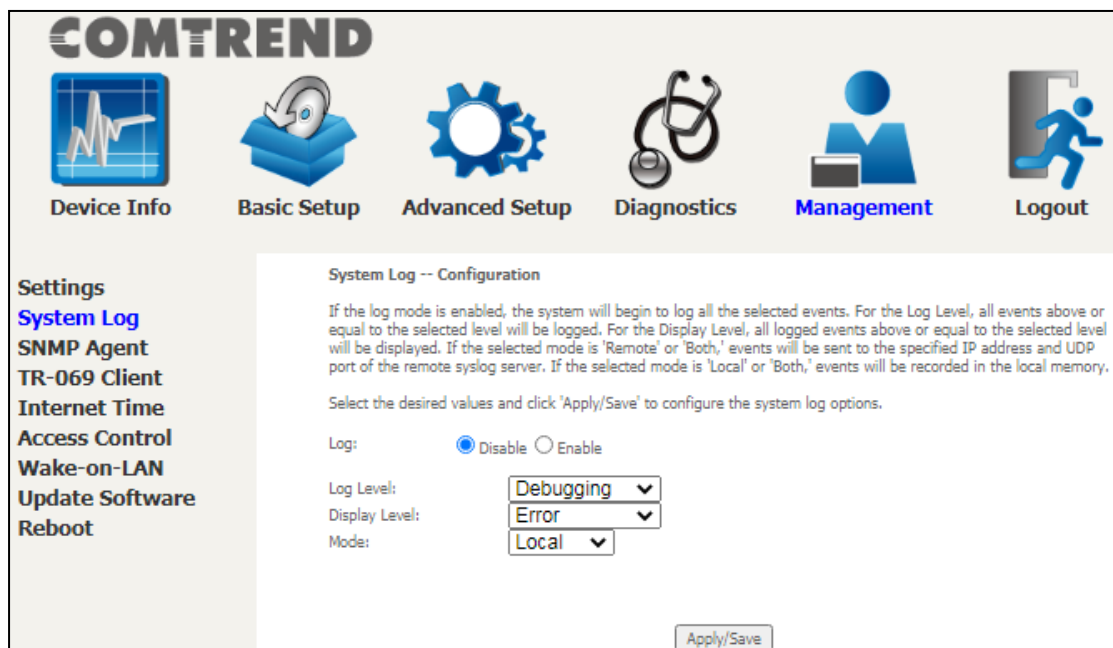
This function allows a system log to be kept and viewed upon request.

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

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



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



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

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

<p>Log Level</p>	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the WR-6895 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"> • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
<p>Display Level</p>	<p>Allows the user to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.</p>
<p>Mode</p>	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

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

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

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.

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

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:
Set Community:
System Name:
System Location:
System Contact:
Trap Manager IP:

Save/Apply

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
 DHCP Option 43 Disable Enable

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

Connection Request Authentication

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

Enable STUN Client

Apply/Save Send Inform

The table below is provided for ease of reference.

Item	Description
Enable TR-069	Tick the checkbox <input checked="" type="checkbox"/> to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with the ACS or select serial number to use the router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.

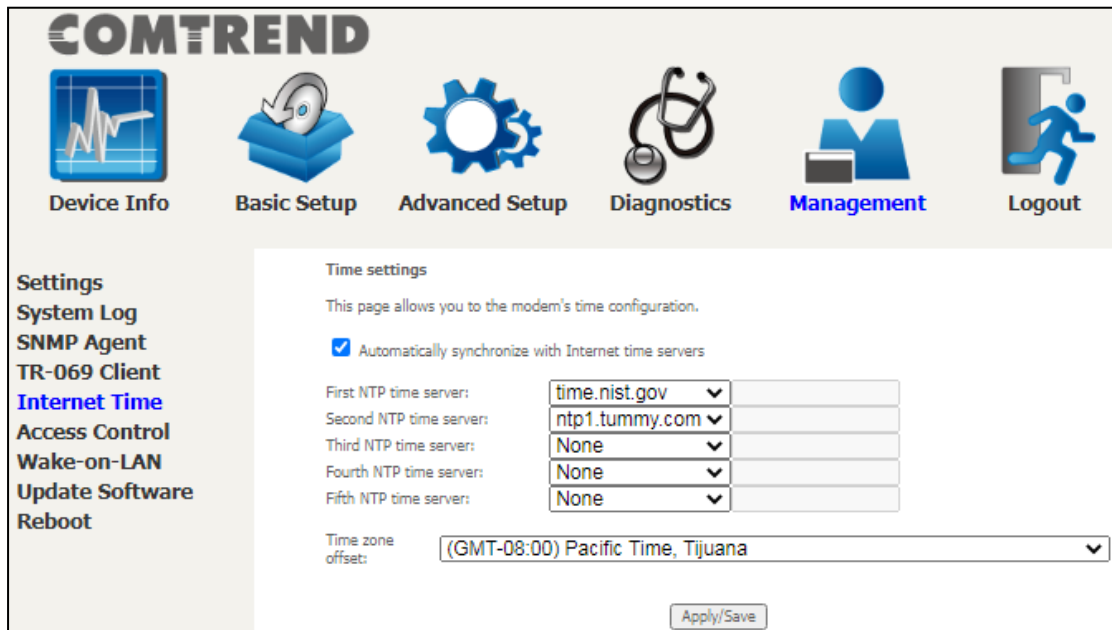
DHCP Option 43	Enable/Disable using DHCP option 43 received from WAN server to configure ACS URL.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Connection Request	
Authentication	Tick the checkbox <input checked="" type="checkbox"/> to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to the router.
Enable STUN Client	
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**.



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 3130 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.

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 32 characters but must not contain a space.

Select an account:

Create an account:

Old Password:

New Password:

Confirm Password:

Save/Apply
Delete

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

Feature	root	support	user	apuser
Account access	Both	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="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"/>
Interface Grouping	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"/>

Save/Apply

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.

COMTREND

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

Service Access Control Configuration

Select each listbox and click save/apply to configure your Setting.

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

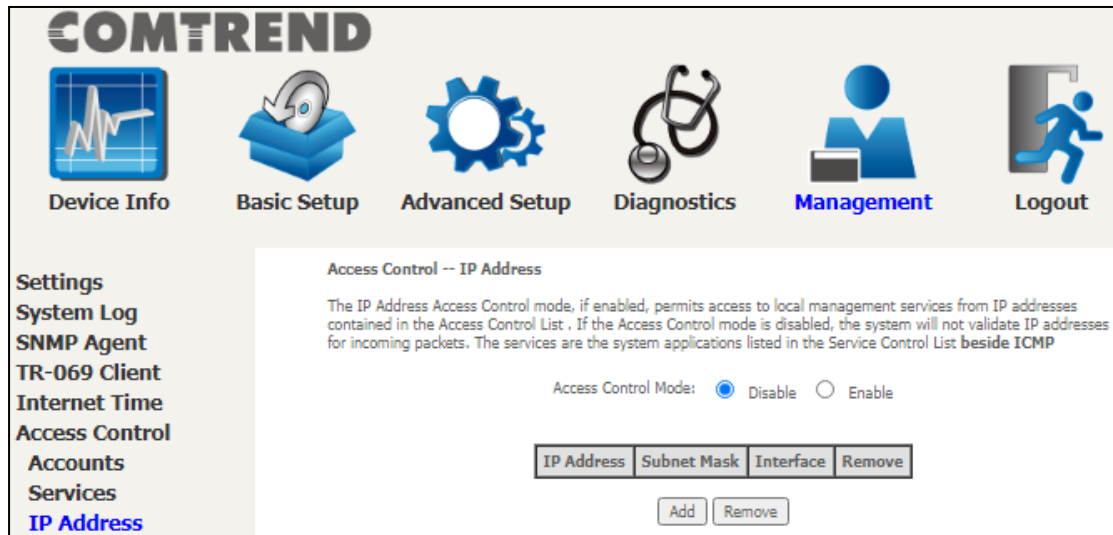
Access "CPU & Memory" from WAN side : Allow Deny

Apply/Save

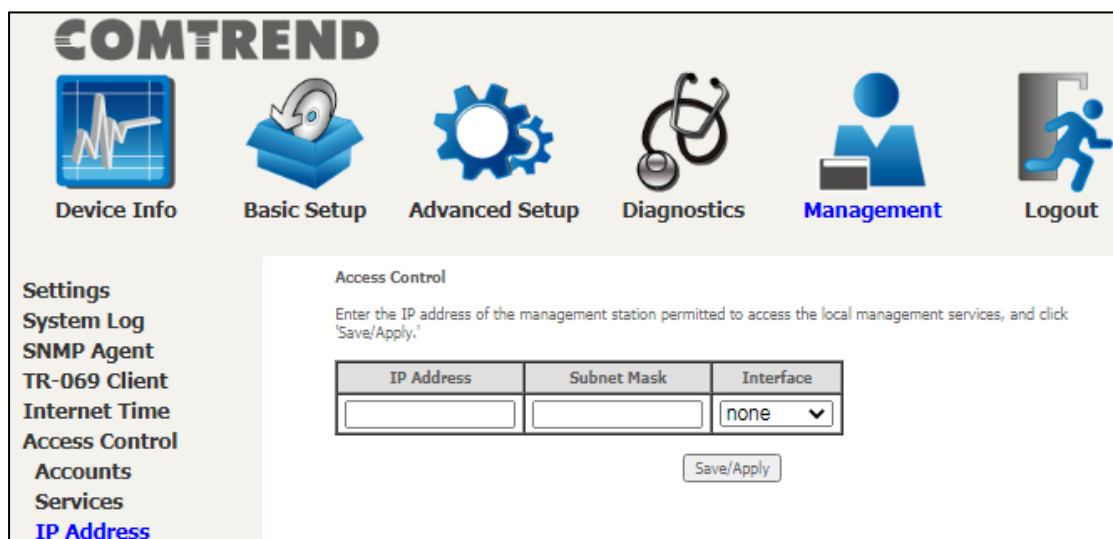
To access "CPU & Memory" from the WAN side, select the Allow radio button and click the **Apply/Save** button.

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**.



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



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

IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

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

8.7 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.

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

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.

Enter the device MAC address in the format xx:xx:xx:xx:xx:xx and then click "Wake Up!".

LAN Interface (default br0):

MAC Address:

Send WoL magic packet to the Broadcast address.

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.

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

Tools -- Update Software

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.

Configuration:

Software File Name:

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.

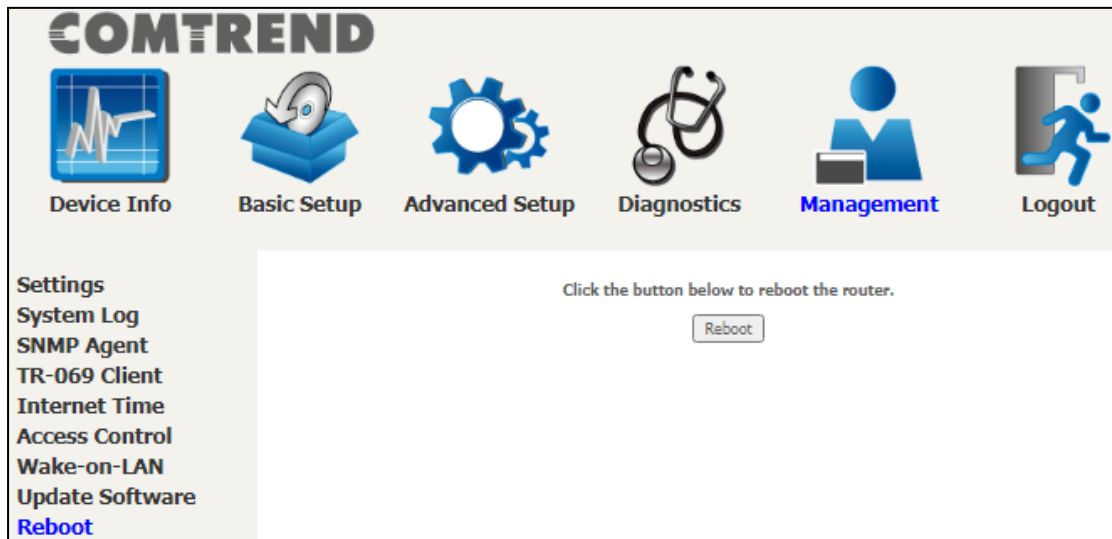
STEP 3: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

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

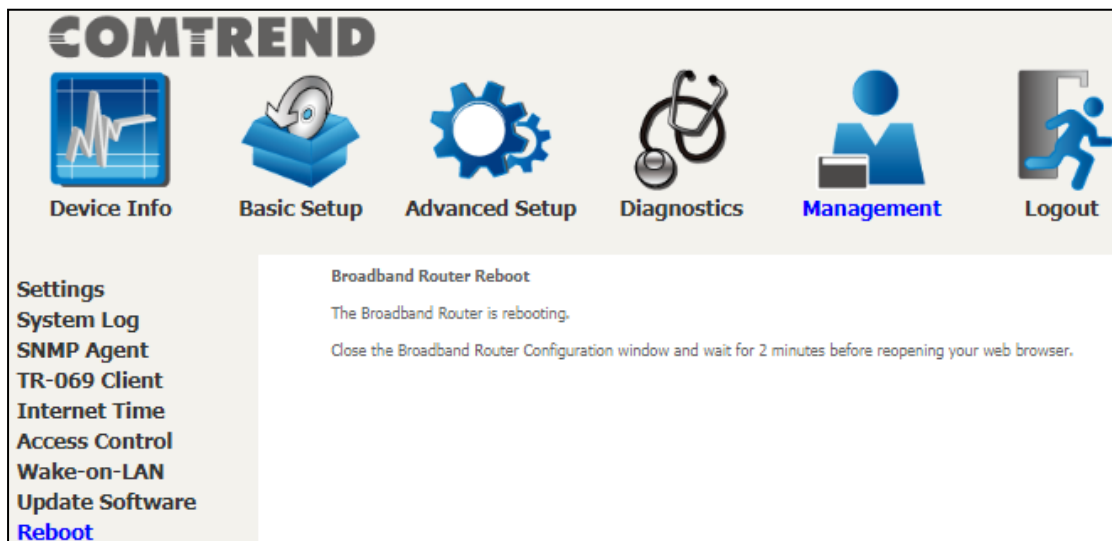
NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Information](#) screen with the firmware version installed,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

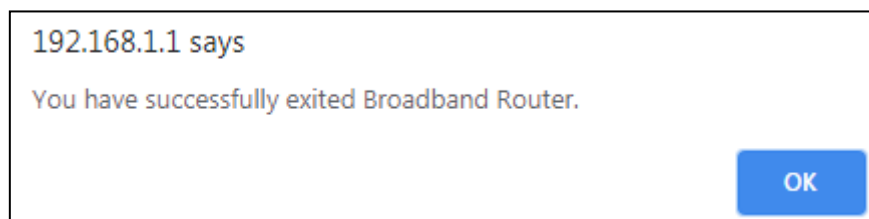
To log out from the device simply click the following icon located at the top of your screen.



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 3130, as per chosen days of the week and the chosen times.

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

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

Appendix B - Pin Assignments

Giga ETHERNET Ports (RJ45)

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

Appendix C - Specifications

Hardware

- RJ-14 X1 for 35b VDSL single line 17a VDSL2 bonding ADSL2+ (Annex A) bonding
- RJ-45 X 1 for GELAN
- Reset button X 1
- Power switch X 1

ADSL

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

VDSL

- G.993.2(VDSL2) 35b, 30a, 17a, 12a, 12b, 8a, 8b, 8c, 8d
- G.993.5 (G.vector)
- G.998.4 (G.INP)
- SRA (Seamless Rate Adaptation)
- UPBO (Upstream Power Back-off)

Ethernet

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

Networking Protocols

- RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Router, RFC 2516 (PPPoE); RFC 1577 (IPoA)
- PPPoE Pass-Through, Multiple PPPoE Sessions on Single WAN Interface
- PPPoE Filtering of Non-PPPoE Packets Between WAN and LAN
- Transparent Bridging Between all LAN and WAN Interfaces
- 802.1p/802.1q VLAN, DSCP
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP
- DHCP Server/Client/Relay, DNS Proxy/ Relay, Dynamic DNS, UPnP, DLNA
- IPv6 Dual Stack, IPV6 Rapid Deployment (6RD)

Management

- TR-069/TR-098/TR-104/TR-111/TR-181, SNMP, Telnet, Web- Based Management, Configuration Backup and Restoration
- Software Upgrade via HTTP, TFTP Server, or FTP Server

Firewall/Filtering

- Stateful Packet Inspection Firewall
- Stateless Packet Filter
- URI/URL Filtering
- Denial of Service (DOS): ARP Attacks, Ping Attacks, Ping of Death, LAND, SYNC, Smurf, Unreachable, Teardrop
- Port Scan Detection and Protection
- TCP/IP/Port/Interface Filtering

NAT/PAT

- Support One to One, Many to One, Many to Many (Overload), Many to Many (No Overload) NAT
- NAT Loopback
- Port Triggering
- Port Forwarding (Virtual Server)
- Symmetric port-overloading NAT, Full-Cone NAT
- DMZ host
- VPN Pass Through (PPTP, L2TP, IPSec)

Power Supply

- External power adapter: 12VDC/ 1.5A

Environment

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

Dimensions

- 171 x 122 x 38mm (WxDxH)

Weight

- 0.6 kg

NOTE: Specifications are subject to change without notice.

Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

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

For WAN access, type: `ssh -l 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.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
LAN
Router Limits
Parental Control
Home Networking
Print Server
DLNA

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

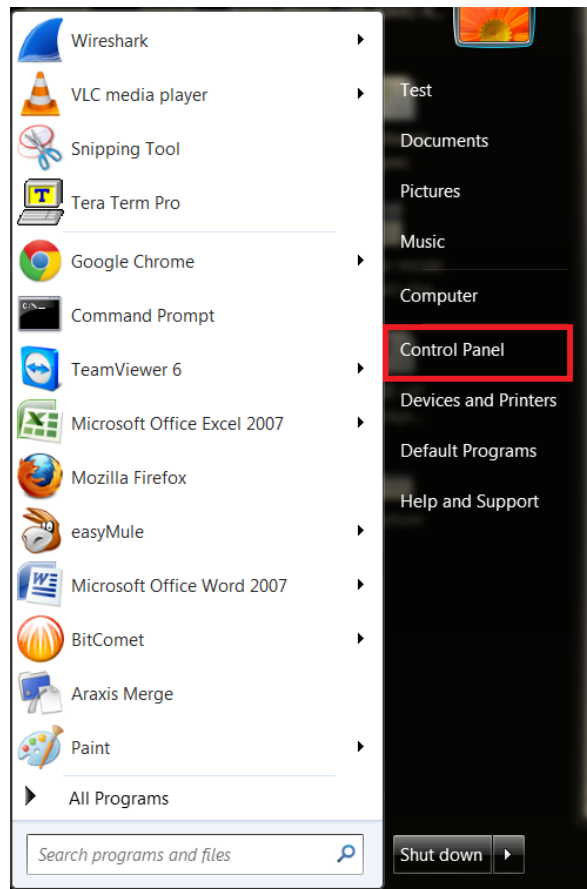
Manufacturer Product Serial Number

Enable on-board print server.

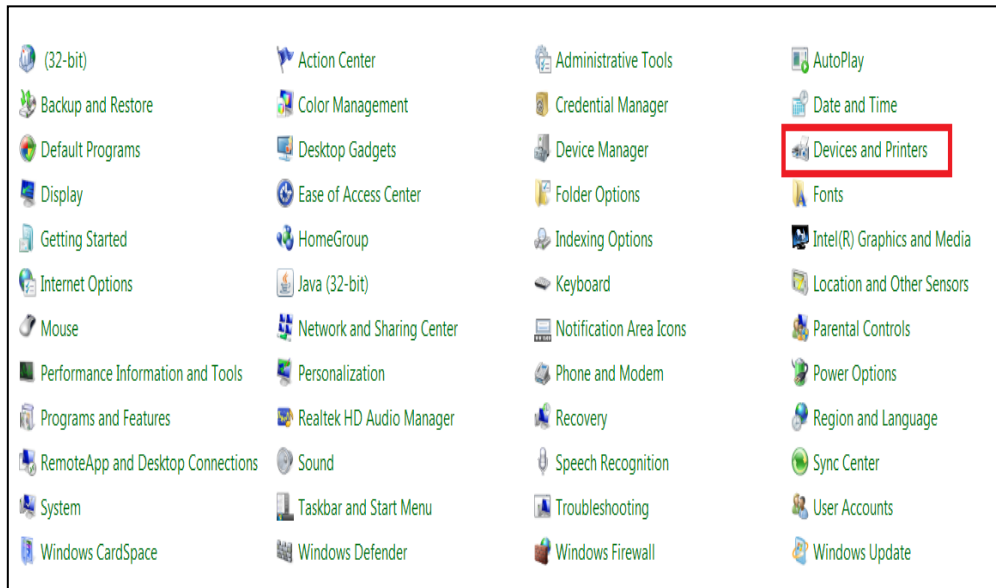
Printer name hpdeskjet
Make and model 321123

Apply/Save

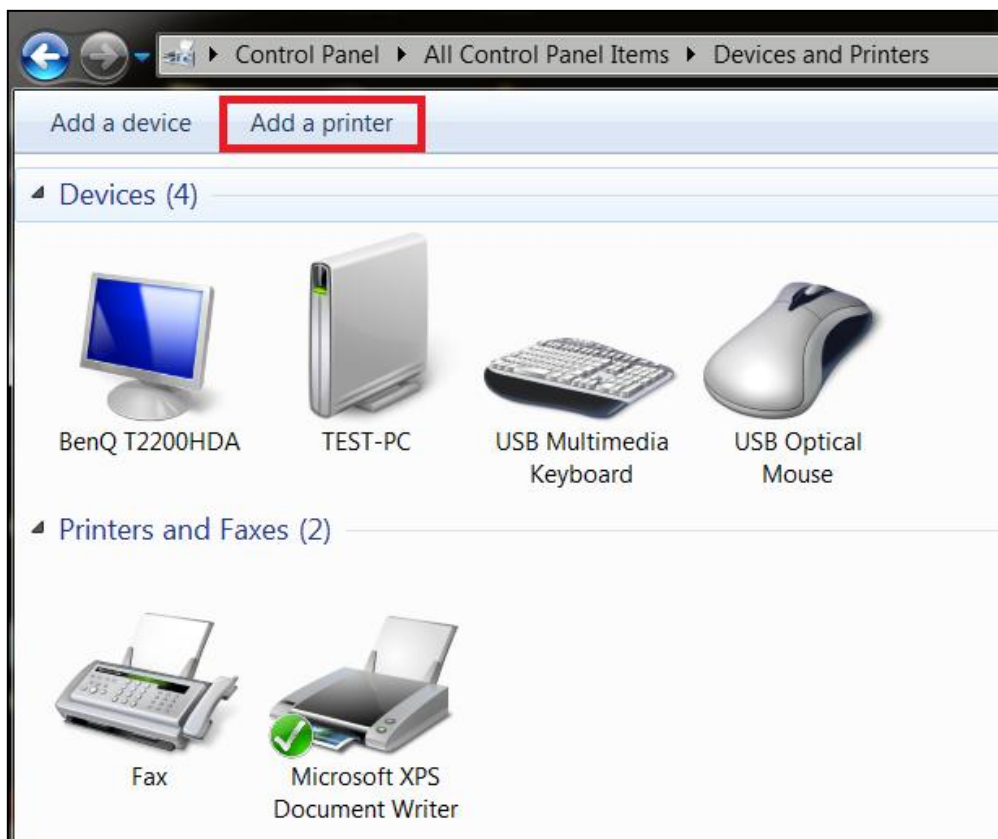
STEP 2: Click the Windows start button. → Then select **Control Panel**.



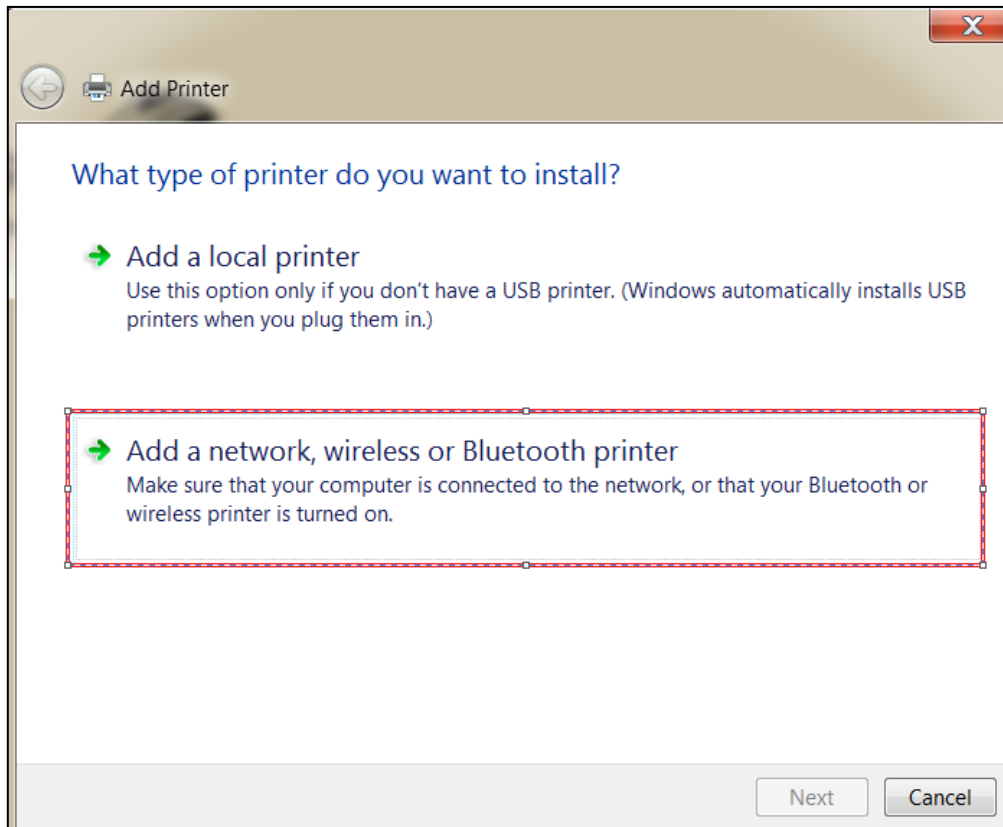
STEP 3: Select Devices and Printers.



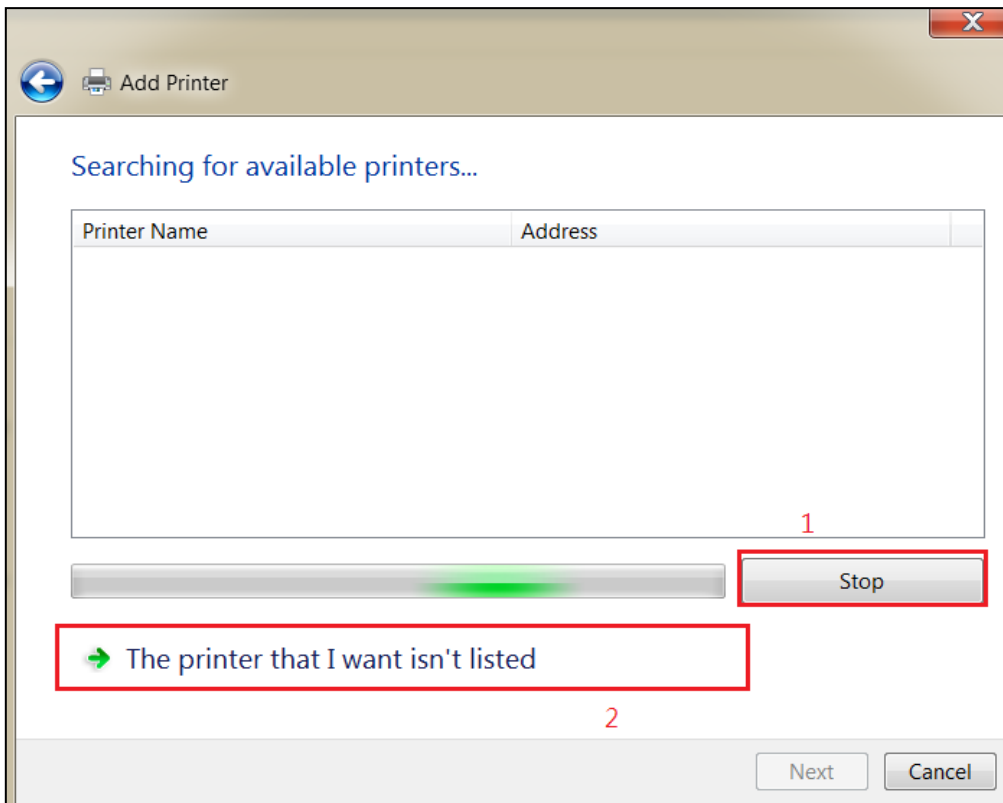
STEP 4: Select Add a printer.



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



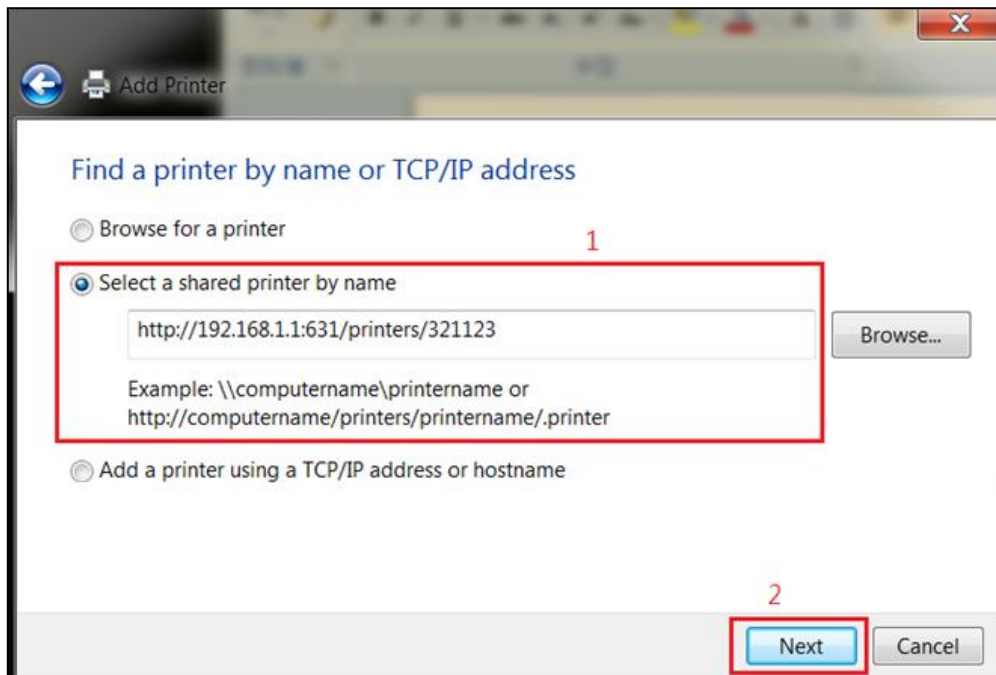
STEP 6: Click the **Stop** button. → Select **The printer that I want isn't listed.**



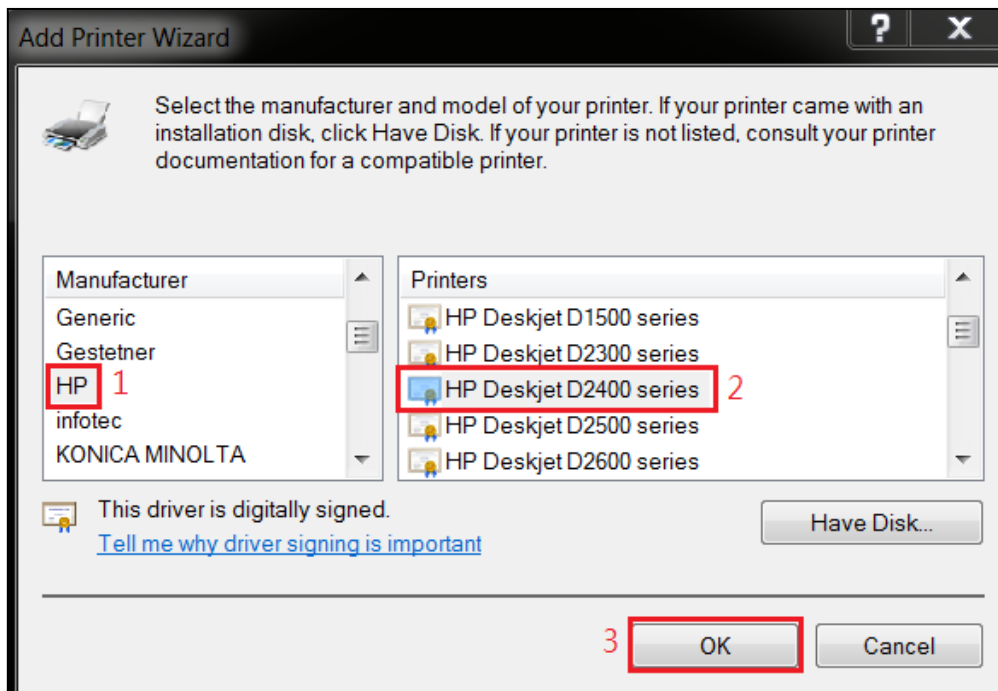
STEP 7: Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

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

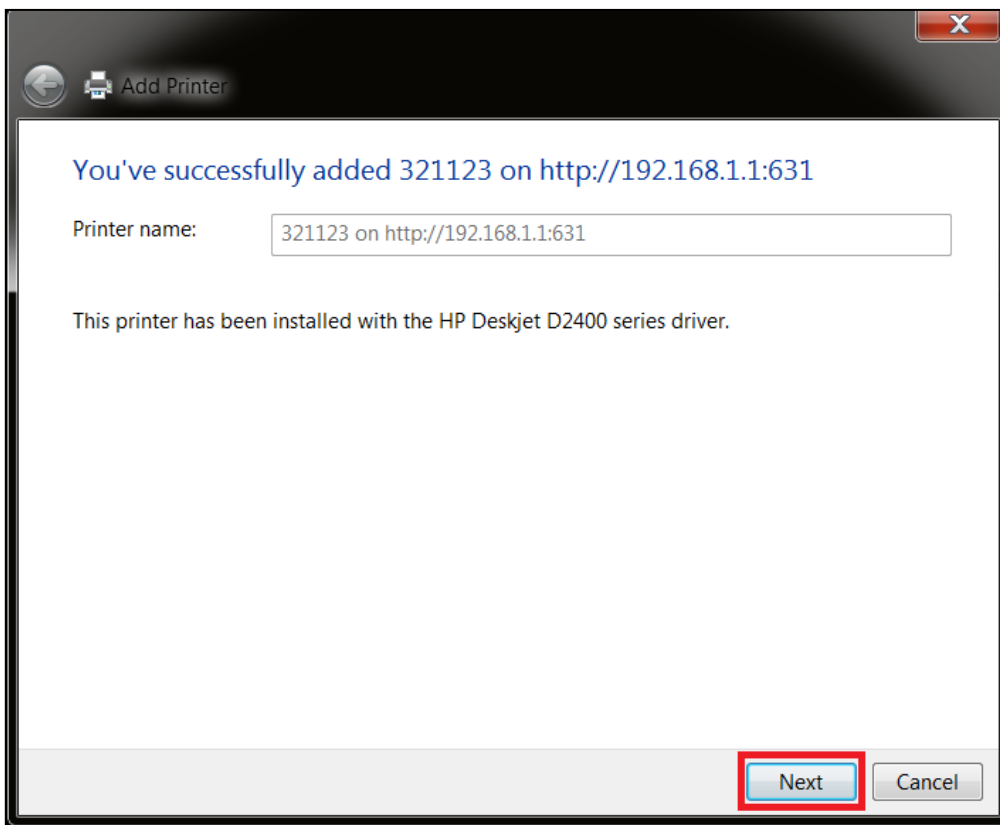
NOTE: The printer name must be the same name inputted in the WEB UI “printer server settings” as in step 1.



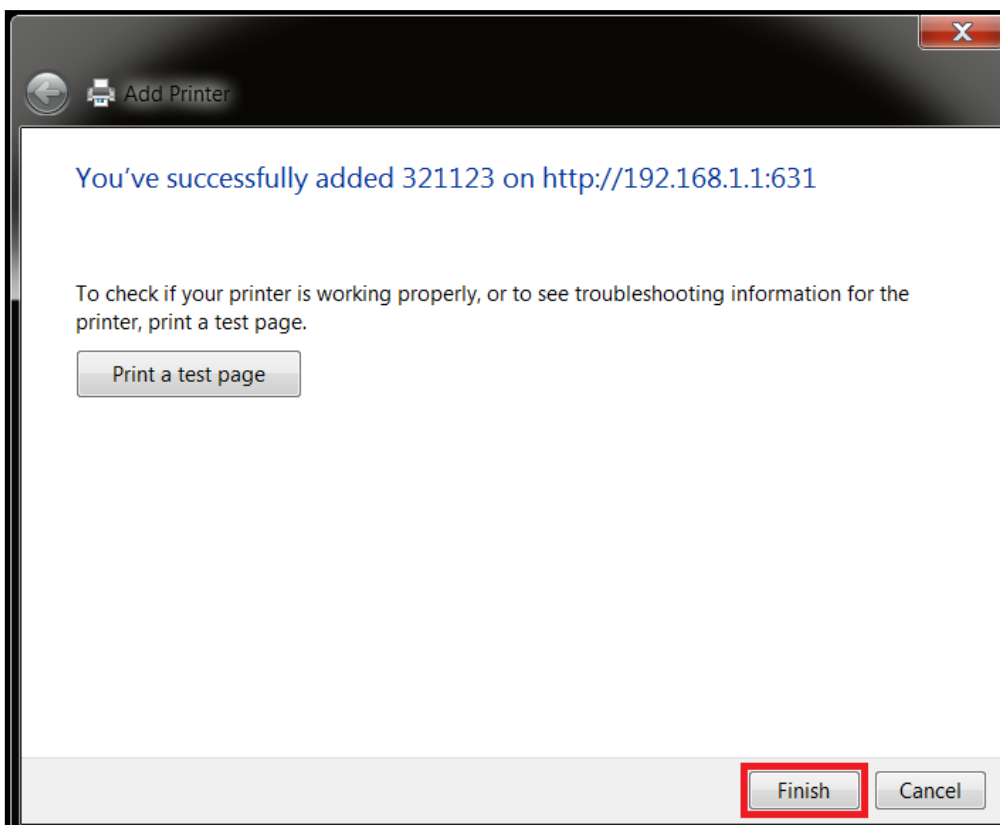
STEP 8: Select the **manufacturer** → and **model** of your printer → then, click **OK**.



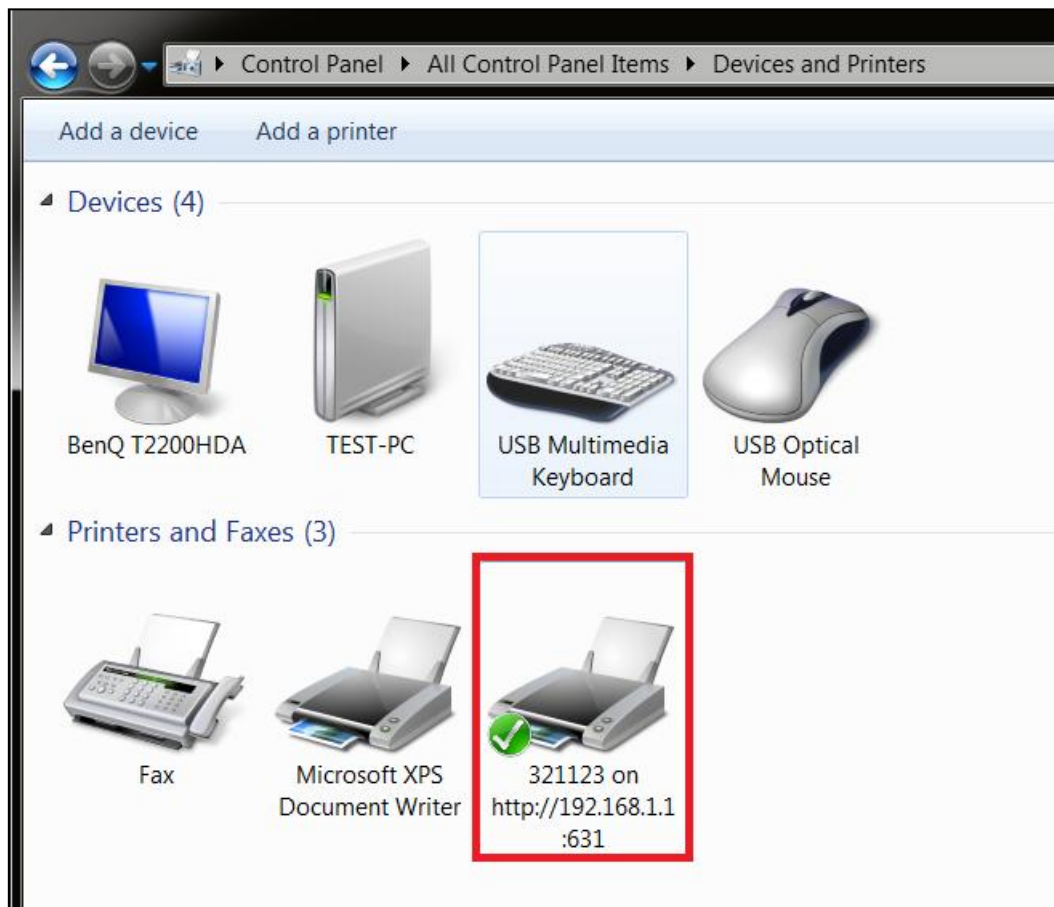
STEP 9: The printer has been successfully installed. Click the **Next** button.



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.

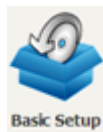
F1 ~ Layer 2 Interfaces

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 3130 supports up to 16 ATM interfaces.



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

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

WAN Setup

NAT

LAN

Router Limits

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.

147

Leading the **Communication Trend**

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

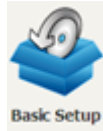
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	<input type="button" value="Remove"/>

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 3130 supports up to four PTM interfaces.



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

This table is provided here for ease of reference.

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

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

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

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.

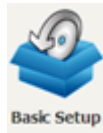
For example, a PTM interface in Default Mode is shown below.

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"/>

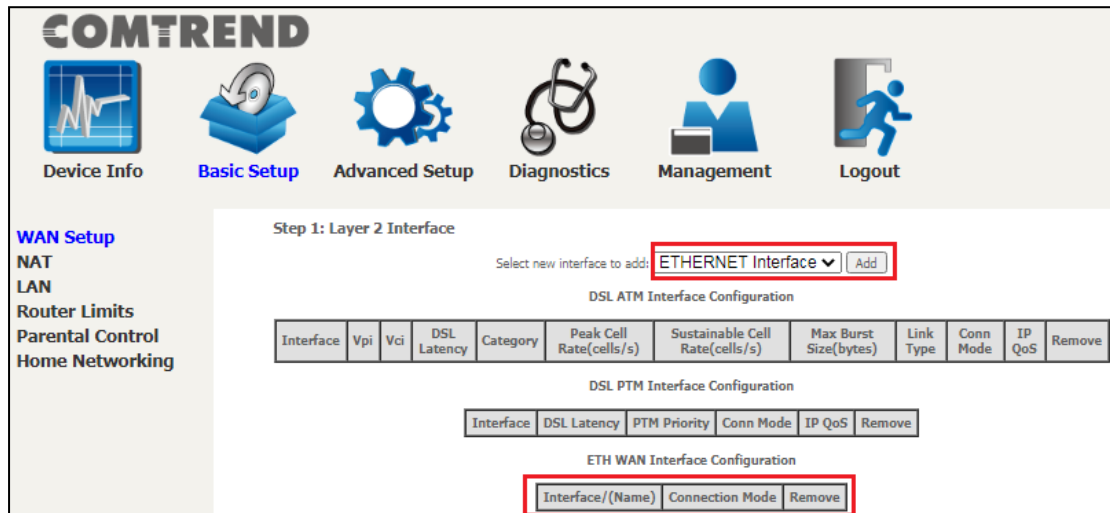
To add a WAN connection go to [Section F2 ~ WAN Connections](#).

F1.3 Ethernet WAN Interface

The NexusLink 3130 supports a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet interface.



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

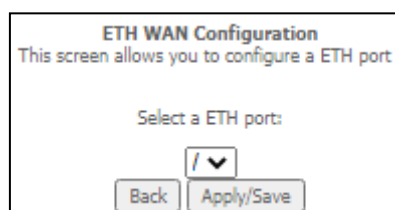


STEP 2: Click **Add** to proceed to the next screen.

This table is provided here for ease of reference.

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

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



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

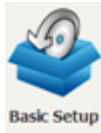
ETH WAN Interface Configuration		
Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	<input type="button" value="Remove"/>

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

F2 ~ WAN Connections

The NexusLink 3130 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
<input type="button" value="Add"/> <input type="button" value="Remove"/>														

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

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

atm0/(0_0_35) ▼

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 (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:

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**.

The screenshot shows the 'WAN Service Configuration' window. It has a title bar and a main content area. At the top, it says 'WAN Service Configuration'. Below that, it asks to 'Select WAN service type:' and has three radio buttons: 'PPP over Ethernet (PPPoE)' (which is selected), 'IP over Ethernet (DHCP/ Static IP)', and 'Bridging'. Below the radio buttons is a text input field for 'Enter Service Description:' containing 'pppoe_0_0_35'. Below that is a note: '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.' There are three input fields: 'Enter 802.1P Priority [0-7]:' with '-1', 'Enter 802.1Q VLAN ID [0-4094]:' with '-1', and 'Select VLAN TPID:' with a dropdown menu showing 'Select a TPID'. Below these is 'Internet Protocol Selection:' with a dropdown menu showing 'IPv4 Only'. At the bottom right are 'Back' and 'Next' buttons.

*

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: ▼

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

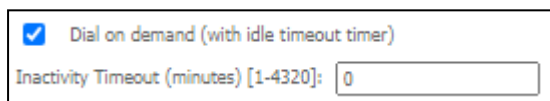
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

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 3130 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 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 3130 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**.

The screenshot shows the 'WAN Service Configuration' window. Under 'Select WAN service type:', the 'IP over Ethernet (DHCP/ Static IP)' radio button is selected. The 'Enter Service Description:' field contains 'ipoe_0_0_35'. Below this, instructions state: '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.' The 'Enter 802.1P Priority [0-7]:' field is set to '-1', and the 'Enter 802.1Q VLAN ID [0-4094]:' field is also set to '-1'. The 'Select VLAN TPID:' dropdown menu is open, showing 'Select a TPID' with a downward arrow. The 'Internet Protocol Selection:' dropdown menu is set to 'IPv4 Only'. At the bottom, there are 'Back' and 'Next' buttons.

*

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 12 Hostname:

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.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
atm0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	

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	<input type="button" value="->"/> <input type="button" value="<-"/>	

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**.

The screenshot shows the 'WAN Service Configuration' window. Under 'Select WAN service type:', the 'Bridging' radio button is selected. Below it are two unchecked checkboxes: 'Allow as IGMP Multicast Source' and 'Allow as MLD Multicast Source'. The 'Enter Service Description:' field contains 'br_0_0_35'. Below that, instructions state: '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.' The 'Enter 802.1P Priority [0-7]:' field has '-1'. The 'Enter 802.1Q VLAN ID [0-4094]:' field has '-1'. The 'Select VLAN TPID:' dropdown menu is set to 'Select a TPID'. At the bottom are 'Back' and 'Next' buttons.

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.

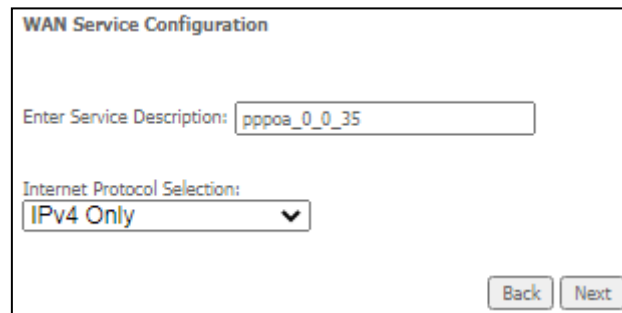
Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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 3130 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' with 'IPv4 Only' selected. At the bottom right, there are 'Back' and 'Next' buttons.

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: ▼

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 3130 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.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer) Inactivity Timeout (minutes) [1-4320]: <input type="text" value="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
ppp0a0	

->

<-

Back Next

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

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

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="->"/> <input type="button" value="-<"/>	

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.

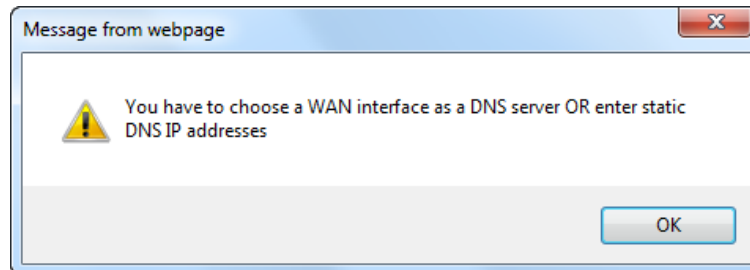
Routing -- Default Gateway

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 Available WAN Interfaces

▲

▼

->

<-

▲

▼

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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

WAN Setup - Summary

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

Connection Type:	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

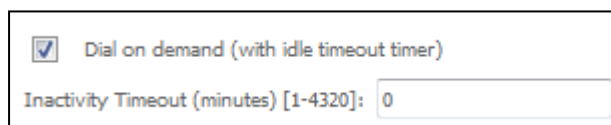
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

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 3130 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 **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 3130 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="->"/> <input type="button" value="<-"/>	

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:

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;">ppp0.1</div>	<div style="border: 1px solid gray; padding: 2px; width: 20px; margin: 5px auto;">-></div> <div style="border: 1px solid gray; padding: 2px; width: 20px; margin: 5px auto;"><-</div>	<p>Available WAN Interfaces</p> <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:

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: pppoe_0_0_35/ppp0.1 ▼

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 12 Hostname:

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

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="->"/> <input type="button" value="<-"/>	

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="->"/> <input type="button" value="<-"/>	

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.

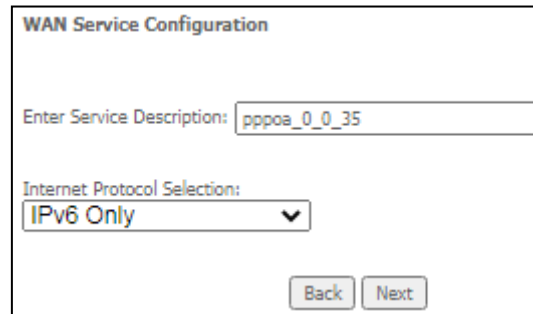
Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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 screenshot shows a web-based configuration interface titled "WAN Service Configuration". It contains the following elements:

- A text input field labeled "Enter Service Description:" containing the text "pppoa_0_0_35".
- A dropdown menu labeled "Internet Protocol Selection:" with "IPv6 Only" selected.
- Two buttons at the bottom: "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: ▼

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

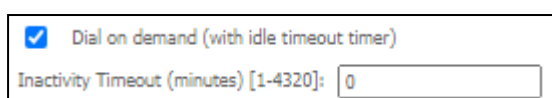
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

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 3130 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/PCP 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
<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">pppoa0</div>	<div style="border: 1px solid #ccc; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">-></div> <div style="border: 1px solid #ccc; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;"><-</div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"></div>

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

Selected WAN Interface: pppoa_0_0_35/pppoa0

Back
Next

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

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

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

DNS Server Configuration

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

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;">pppoa0</div>	<div style="border: 1px solid gray; padding: 2px 5px; margin: 5px 0;">-></div> <div style="border: 1px solid gray; padding: 2px 5px; margin: 5px 0;"><-</div>	<p>Available WAN Interfaces</p> <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:

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.