COMTREND CORPORATION

NexusLink 3112u

Multi-DSL Bonded Router

User Manual

Version A1.1, June 04, 2014

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:

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

⚠ WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C – Specifications.

Copyright

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

The NexusLink 3112u Multi DSL Bonded Router is a single box solution for triple play applications. It features dual xDSL bonded ports that provide twice the xDSL bandwidth (ADSL2+ in both ATM/PTM modes and VDSL2 PTM 8a/8b/8c/8d/12a/12b/17a profiles) over comparable single-port models. With PTM mode supported, it can provide better performance than a regular ATM mode router. The NexusLink 3112u is equipped with three Fast Ethernet ports, one Gigabit port and 802.11n WLAN Access Point (AP). It goes above and beyond with high level features such as QoS, VPN and remote management (with TR-069 support).

1.1 Features

- Integrated 802.11n AP (802.11b/g backward-compatible)
- Automatically switches to ADSL2+/VDSL2 according to the port setting of DSLAM
- Supports bonded xDSL lines
- VDSL2 12a/12b profile support
- Per-VC packet level QoS
- WPA and 802.1x
- WPS 2.0
- RADIUS client
- Up to VDSL2 17a Profile
- US0
- □PhyR and G.INP
- G.Vector
- Static routing & RIP/RIP v2
- NAT/PAT
- IGMP Snooping/Proxy and fast leave
- Supports remote administration
- Web-based management
- Configuration backup and restoration
- Up to 16 PVCs and Up to 8 PTM flows
- IPv6 compliant
- Printer Server (IPP)
- Firmware upgrade and configuration
- Auto PVC configuration
- UPnP
- IP/MAC address filtering
- Dynamic IP assignment
- Parental Control
- DHCP Server/Client
- DNS Relay/Proxy
- FTP/TFTP server
- USB mass-storage and file sharing (Samba)
- Embedded SNMPv2 agent
- HTTPS/HTTP server
- TR-069/TR-098/TR-111

Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

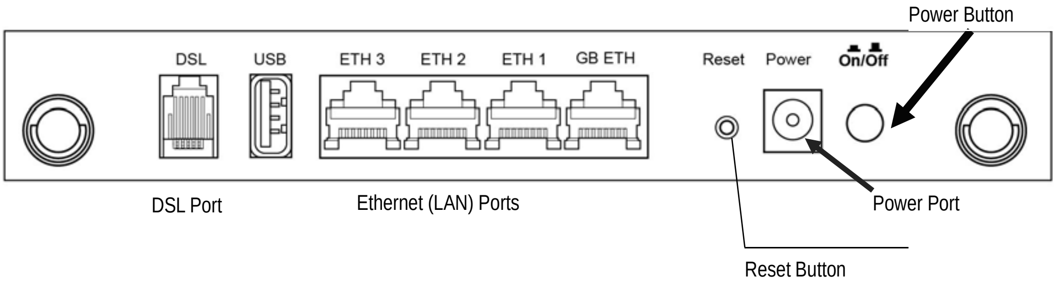
Non-stackable
This device is not stackable – do not place units on top of each other, otherwise damage could occur.

2.2 Hardware Setup

Follow the instructions below to complete the hardware setup.

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 2.3 LED Indicators for details).

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 2.3 LED Indicators for details).

NOTE: If pressed down for more than 60 seconds, the NexusLink 3112u 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.

GB ETH Port

Use RJ45 straight through or crossover MDI/X cable to connect to Ethernet WAN.

Ethernet (LAN) Ports

Use 10/100 BASE-T RJ-45 cables to connect up to four network devices (as the GB ETH port can also be used). These ports are auto-sensing MDI/X; so either straight-through or crossover cable can be used.

USB Host Port (Type A)

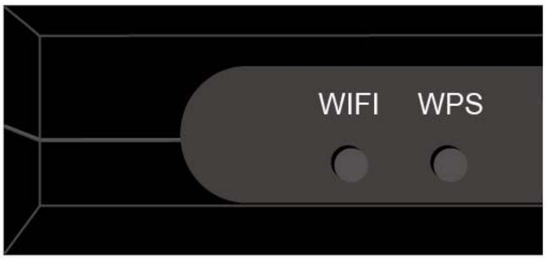
This port can be used to connect the router to the print server.

DSL Port

Connect to a 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.

FRONT PANEL

The Wi-Fi & WPS buttons are located on the bottom-left of the front panel, as shown.



WiFi Switch

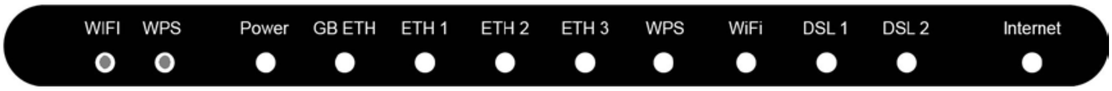
Press this button to enable/disable the wireless LAN (WLAN).

WPS Button

Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode (see Appendix F - WPS OPERATION for instructions).

2.3 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.
GB ETH	Green (for 1000 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.
	Yellow (for 10/100 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.
ETH 1-3	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
WPS	Green	On	WPS enabled.
		Off	WPS disenabled.
		Blink	The router is searching for WPS clients.
WiFi	Green	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.
DSL1	Green	On	The DSL1 link is established.
		Off	The device is powered down.
		Blink	DSL1 attempting sync:

			● Flashing at 2 Hz with a 50% duty cycle when trying to detect carrier signal flashing at 4 Hz with a 50% duty cycle when the carrier has been detected and the modem is trying to train.
DSL2	Green	On	The DSL2 link is established.
		Off	The device is powered down.
		Blink	DSL2 attempting sync: ● Flashing at 2 Hz with a 50% duty cycle when trying to detect carrier signal flashing at 4 Hz with a 50% duty cycle when the carrier has been detected and the modem is trying to train.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an VDSL connection is still present.
		Off	Modem power off, modem in bridged mode or VDSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

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

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the NexusLink 3112u powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

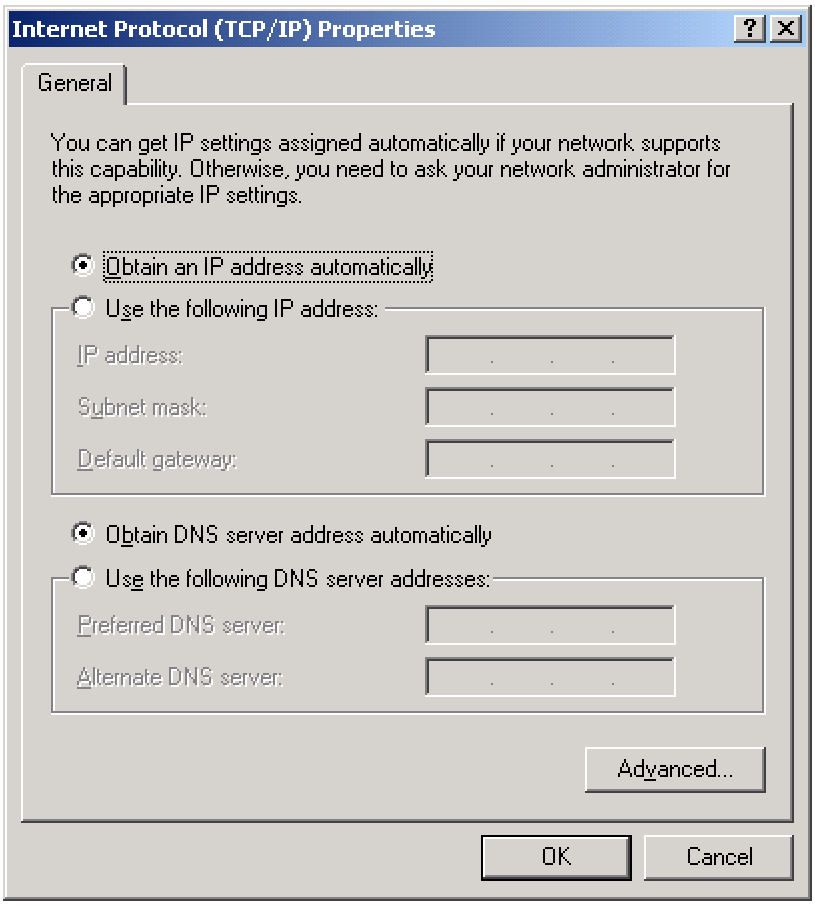
To obtain an IP address from the DCHP server, follow the steps provided below.

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

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

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

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



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

STATIC IP MODE

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

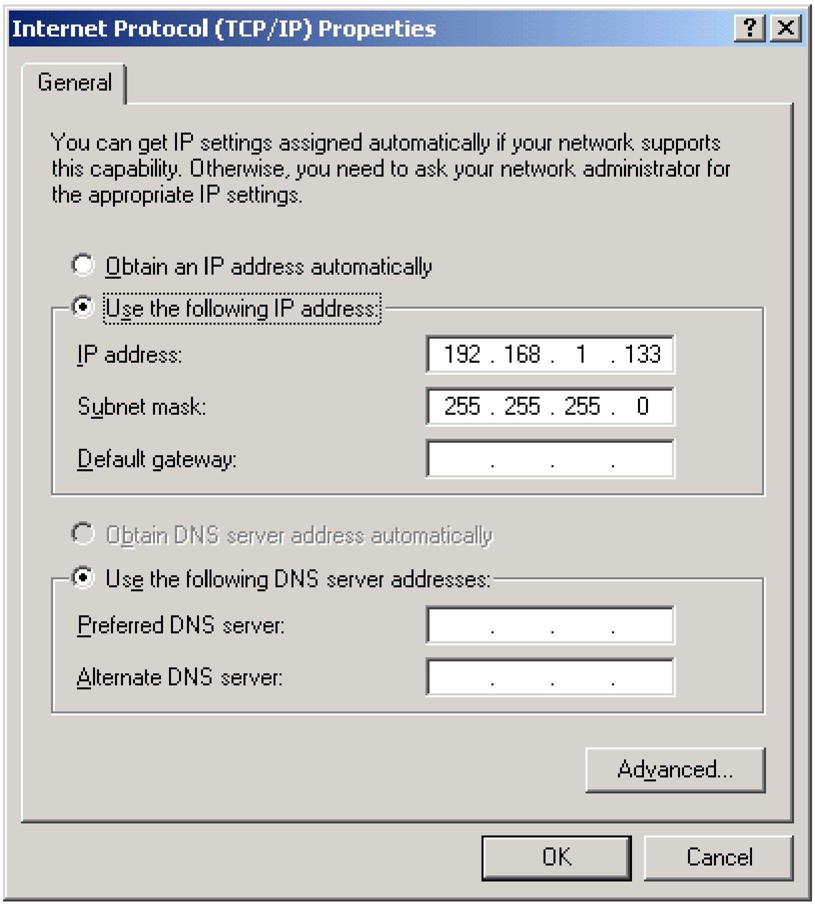
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

3.3 Login Procedure

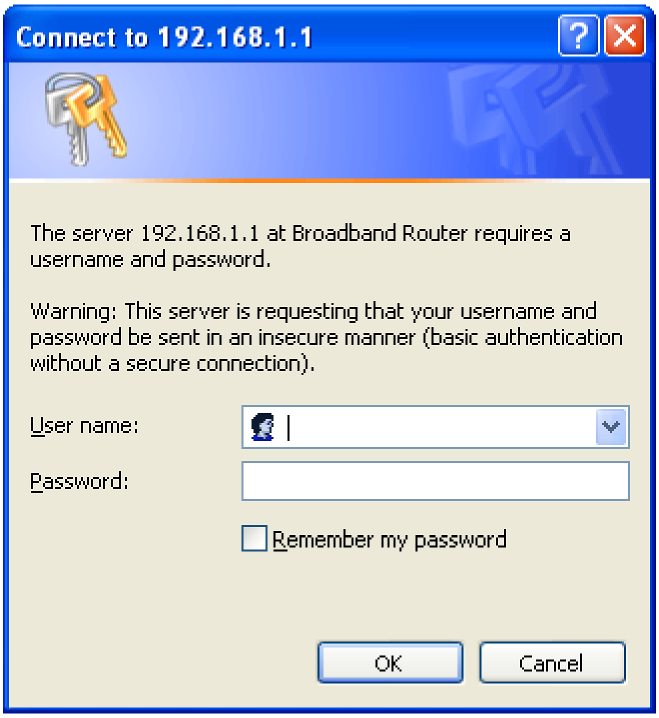
Perform the following steps to login to the web user interface.

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.



Connect to 192.168.1.1

The server 192.168.1.1 at Broadband Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

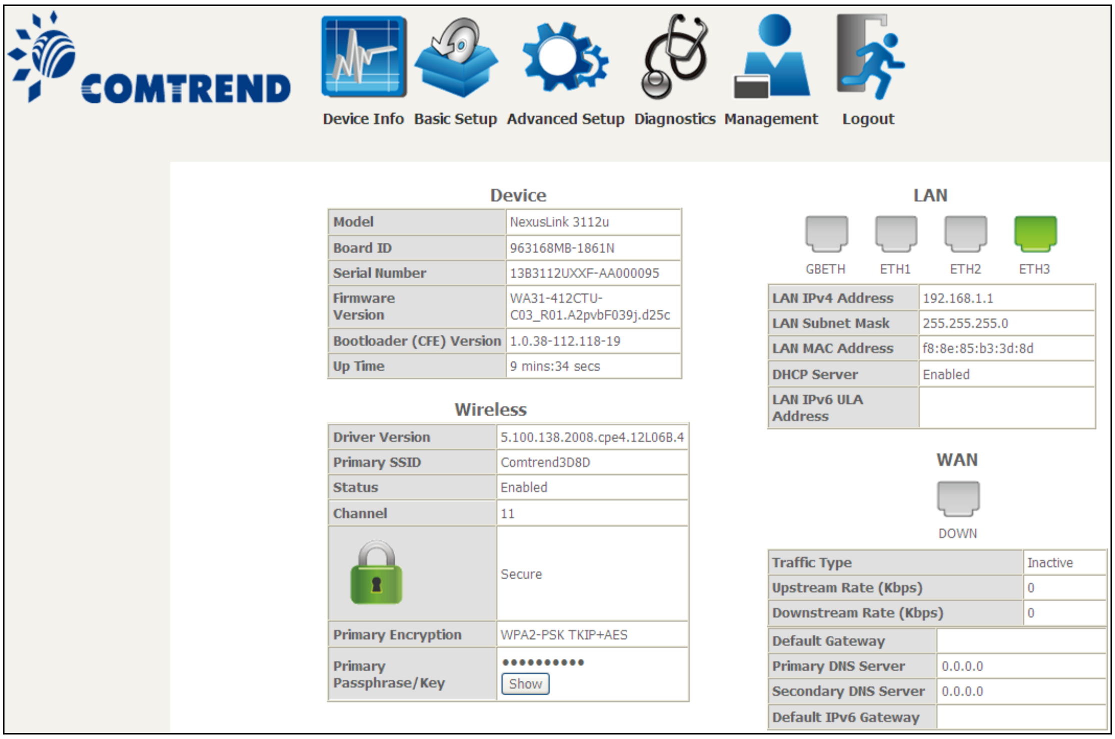
Password:

□ Remember my password

Click **OK** to continue.

NOTE: The login password can be changed later (see section 8.6.1 Passwords).

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



Device

Model	NexusLink 3112u
Board ID	963168MB-1861N
Serial Number	13B3112UXXF-AA000095
Firmware Version	WA31-412CTU-C03_R01.A2pvbF039j.d25c
Bootloader (CFE) Version	1.0.38-112.118-19
Up Time	9 mins:34 secs

Wireless

Driver Version	5.100.138.2008.cpe4.12L06B.4
Primary SSID	Comtrend3D8D
Status	Enabled
Channel	11
🔒	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	●●●●●●●●●● Show

LAN

GBETH ETH1 ETH2 ETH3

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:b3:3d:8d
DHCP Server	Enabled
LAN IPv6 ULA Address	

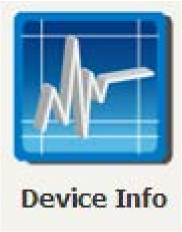
WAN

DOWN

Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0

Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway	

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



Chapter 4 Device Information

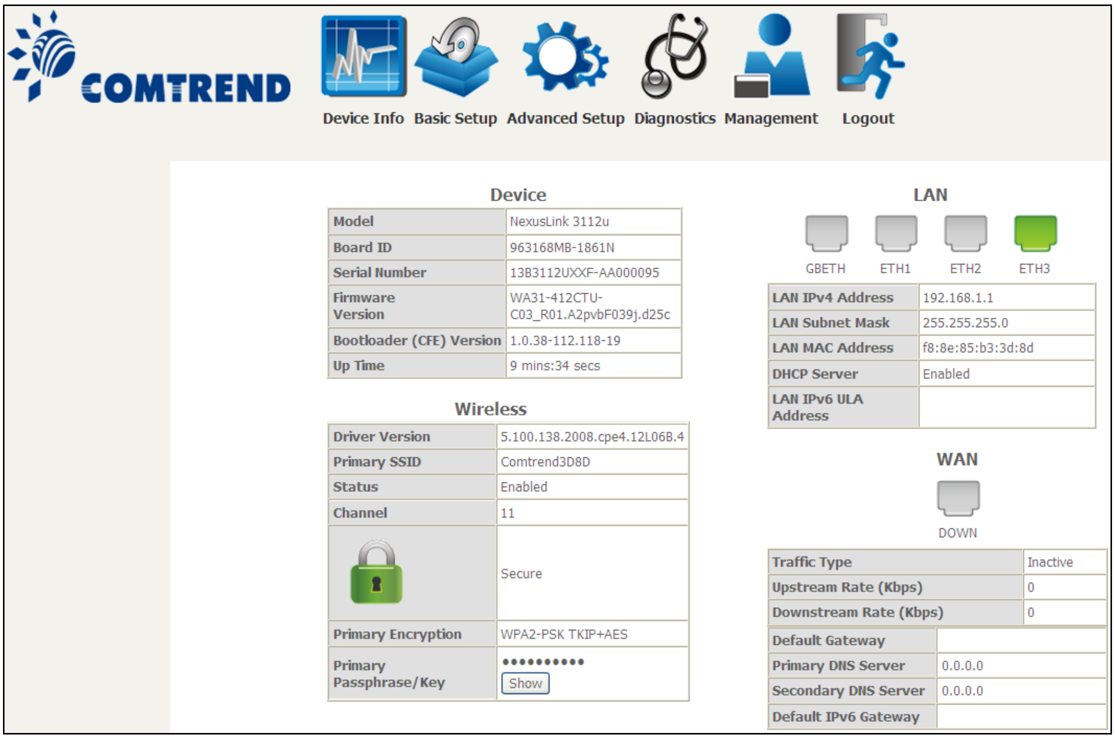
You can reach this page by clicking on the following icon located at the top of the screen.

The web user interface window is divided into two frames, the main menu (at 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, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

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

The Device Info Summary screen displays at startup.



Device

Model	NexusLink 3112u
Board ID	963168MB-1861N
Serial Number	13B3112UXXF-AA000095
Firmware Version	WA31-412CTU-C03_R01.A2pvbF039j.d25c
Bootloader (CFE) Version	1.0.38-112.118-19
Up Time	9 mins:34 secs

Wireless

Driver Version	5.100.138.2008.cpe4.12L06B.4
Primary SSID	Comtrend3D8D
Status	Enabled
Channel	11
🔒	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	•••••••••• Show

LAN

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:b3:3d:8d
DHCP Server	Enabled
LAN IPv6 ULA Address	

WAN

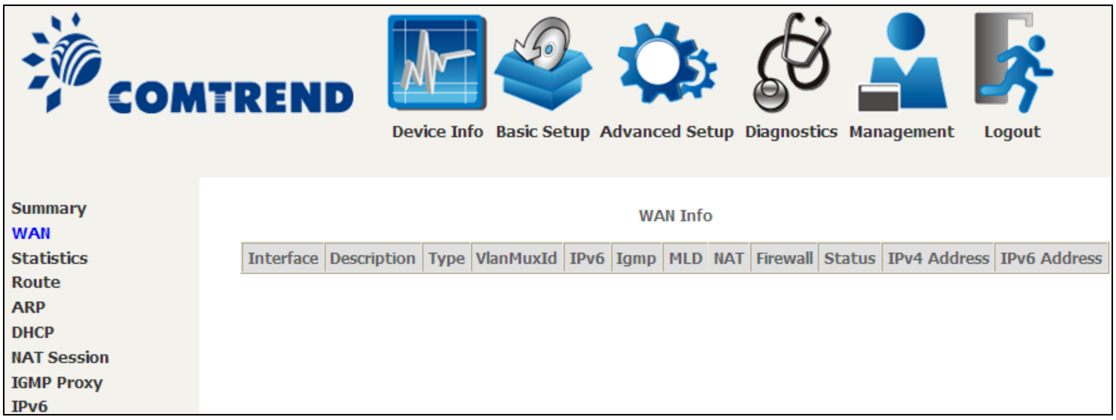
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0

Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway	

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).



WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address

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

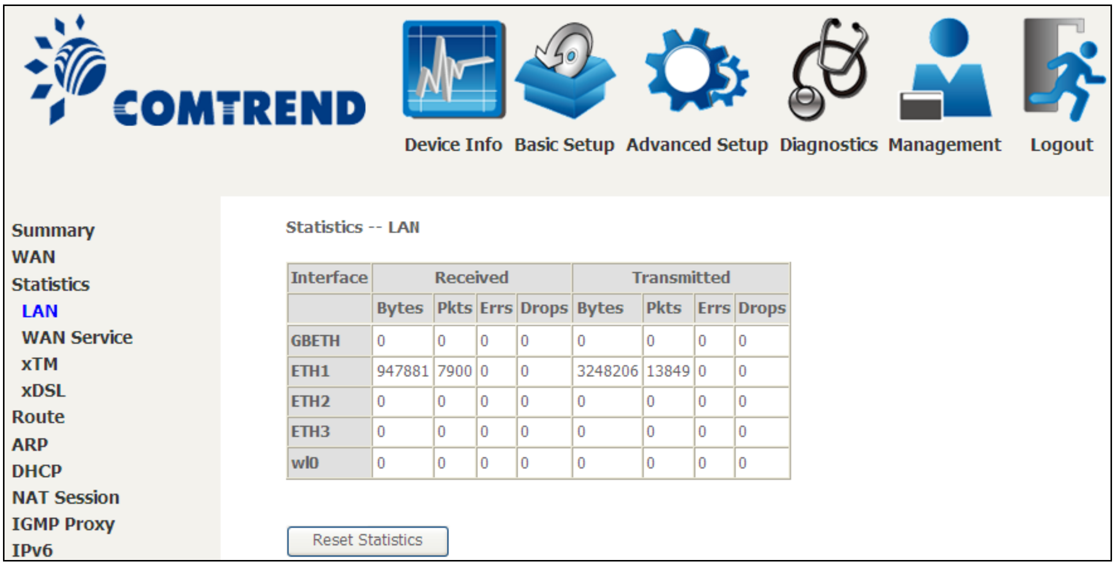
4.2 Statistics

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

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

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



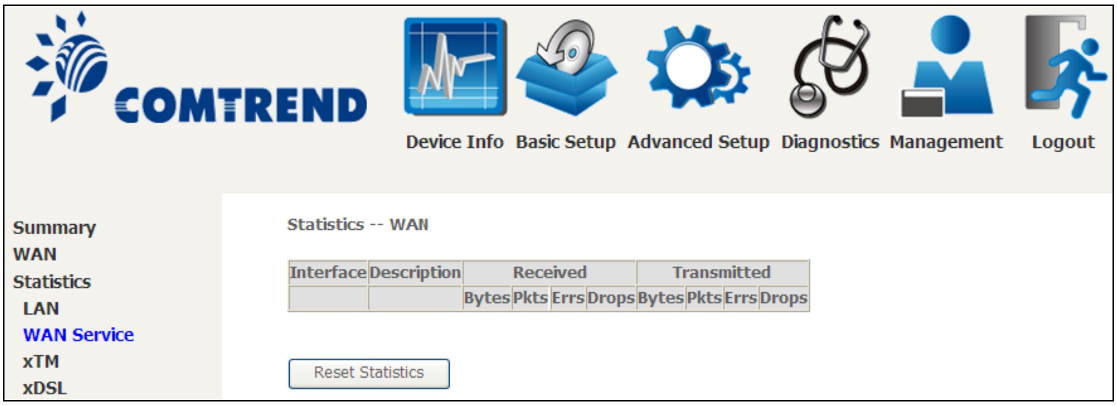
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
GBETH	0	0	0	0	0	0	0	0
ETH1	947881	7900	0	0	3248206	13849	0	0
ETH2	0	0	0	0	0	0	0	0
ETH3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

Heading	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.



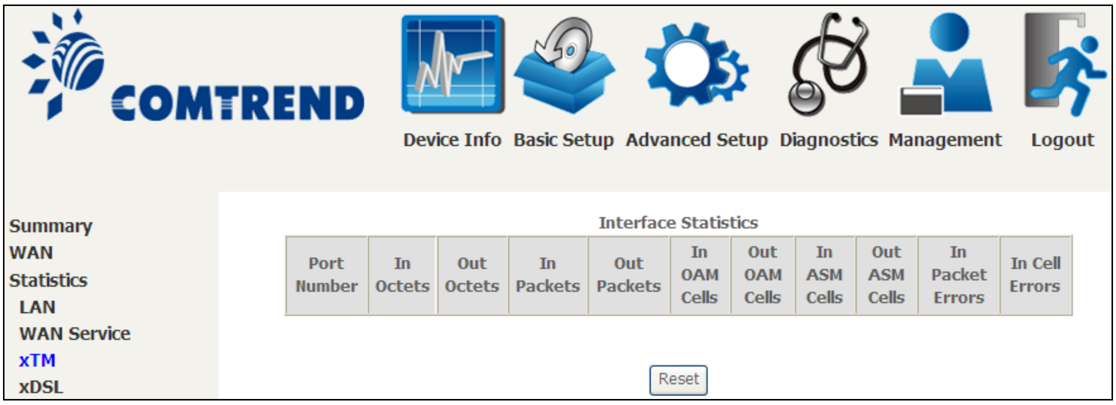
Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

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

4.2.3 XTM Statistics

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



Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

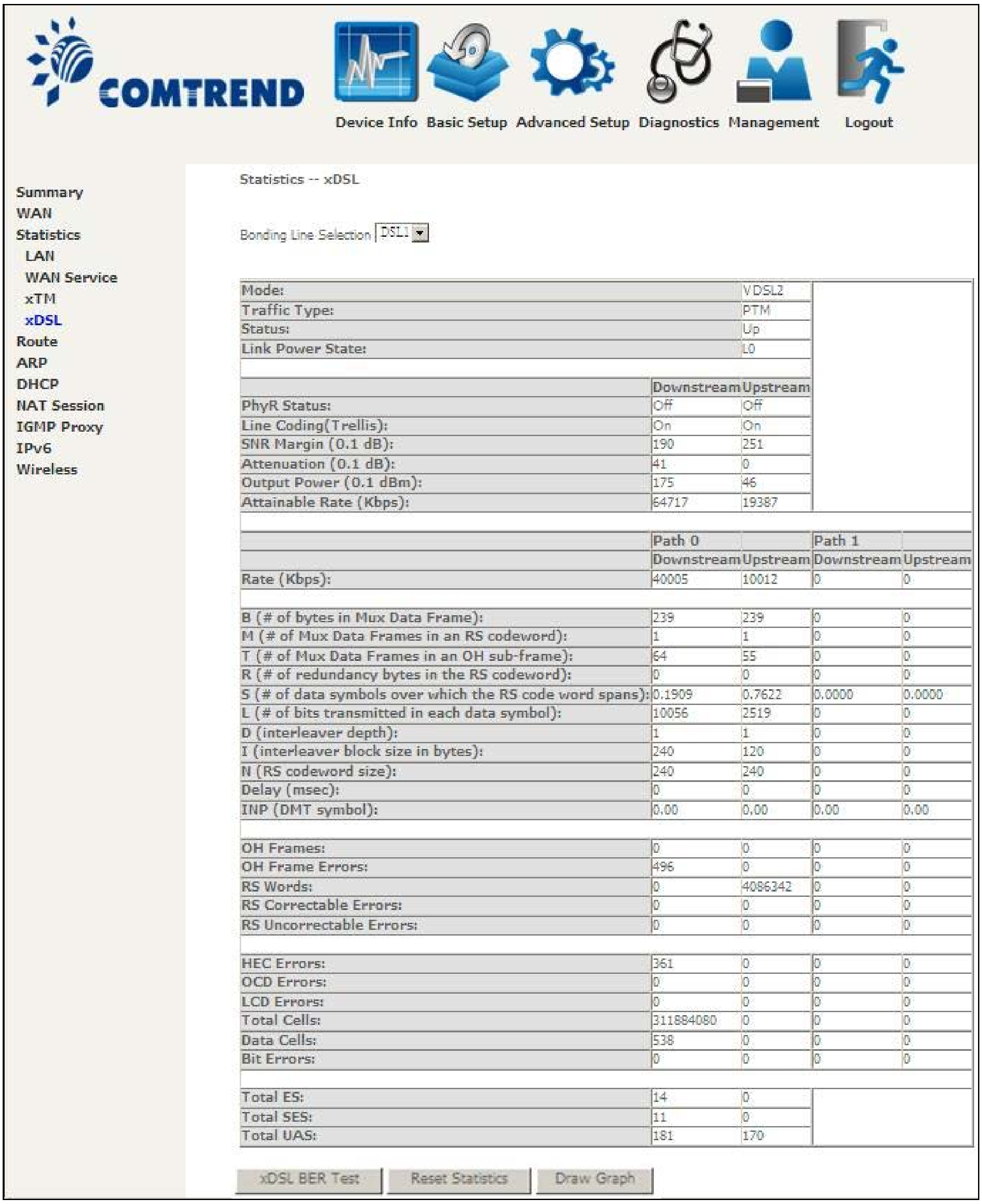
XTM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-3)
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

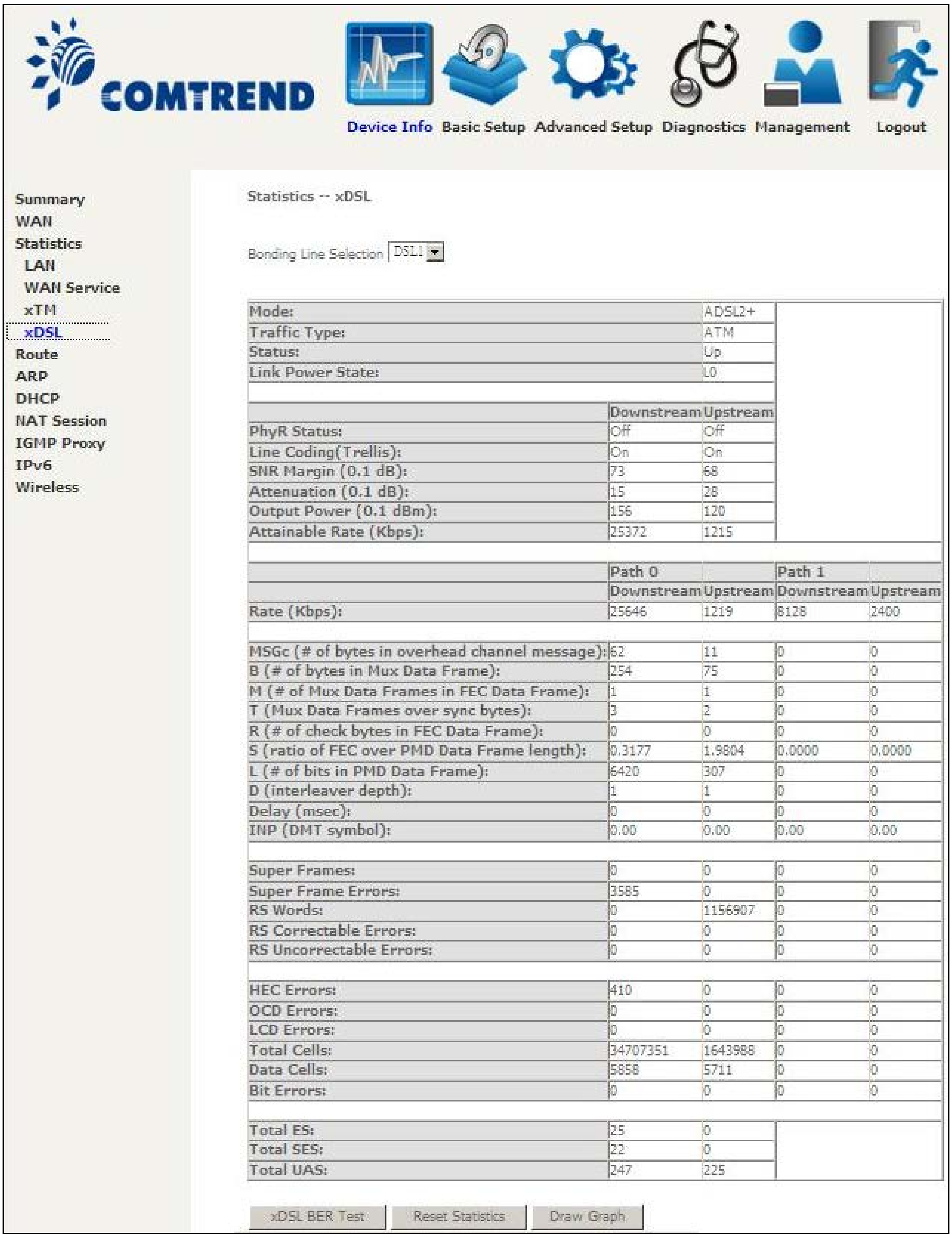


Statistics -- xDSL

Bonding Line Selection DSL1

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):	190	251		
Attenuation (0.1 dB):	41	0		
Output Power (0.1 dBm):	175	46		
Attainable Rate (Kbps):	64717	19387		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	40005	10012	0	0
B (# of bytes in Mux Data Frame):	239	239	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	64	55	0	0
R (# of redundancy bytes in the RS codeword):	0	0	0	0
S (# of data symbols over which the RS code word spans):	0.1909	0.7622	0.0000	0.0000
L (# of bits transmitted in each data symbol):	10056	2519	0	0
D (interleaver depth):	1	1	0	0
I (interleaver block size in bytes):	240	120	0	0
N (RS codeword size):	240	240	0	0
Delay (msec):	0	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
OH Frames:	0	0	0	0
OH Frame Errors:	496	0	0	0
RS Words:	0	4086342	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	361	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	311884080	0	0	0
Data Cells:	538	0	0	0
Bit Errors:	0	0	0	0
Total ES:	14	0		
Total SES:	11	0		
Total UAS:	181	170		

ADSL



Statistics -- xDSL

Bonding Line Selection DSL1

Mode:	ADSL2+			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	L0			
	Downstream	Upstream		
PhyR Status:	Off	Off		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	73	68		
Attenuation (0.1 dB):	15	28		
Output Power (0.1 dBm):	156	120		
Attainable Rate (Kbps):	25372	1215		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	25646	1219	8128	2400
MSGc (# of bytes in overhead channel message):	62	11	0	0
B (# of bytes in Mux Data Frame):	254	75	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	1	0	0
T (Mux Data Frames over sync bytes):	3	2	0	0
R (# of check bytes in FEC Data Frame):	0	0	0	0
S (ratio of FEC over PMD Data Frame length):	0.3177	1.9804	0.0000	0.0000
L (# of bits in PMD Data Frame):	6420	307	0	0
D (interleaver depth):	1	1	0	0
Delay (msec):	0	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
Super Frames:	0	0	0	0
Super Frame Errors:	3585	0	0	0
RS Words:	0	1156907	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	410	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	34707351	1643988	0	0
Data Cells:	5858	5711	0	0
Bit Errors:	0	0	0	0
Total ES:	25	0		
Total SES:	22	0		
Total UAS:	247	225		

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

Field	Description
Link Power State	Link output power state.
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.

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

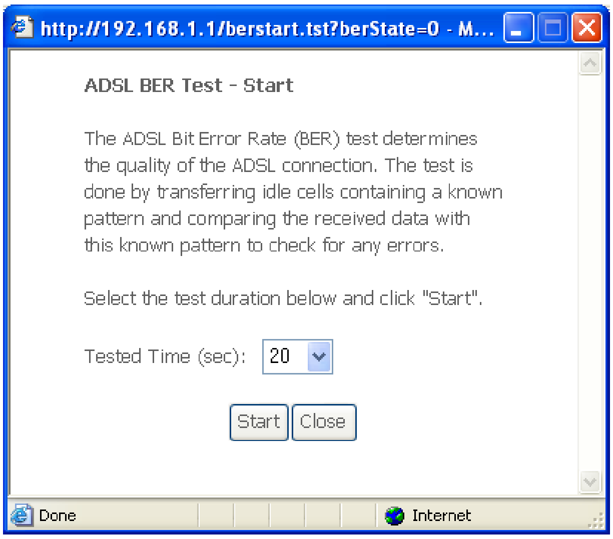
OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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.



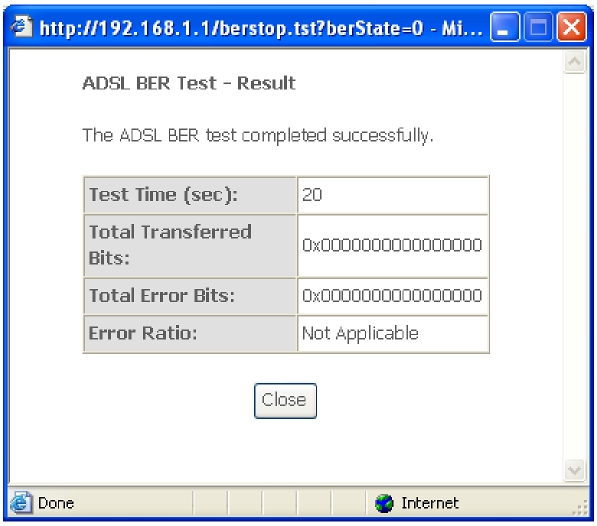
ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

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.



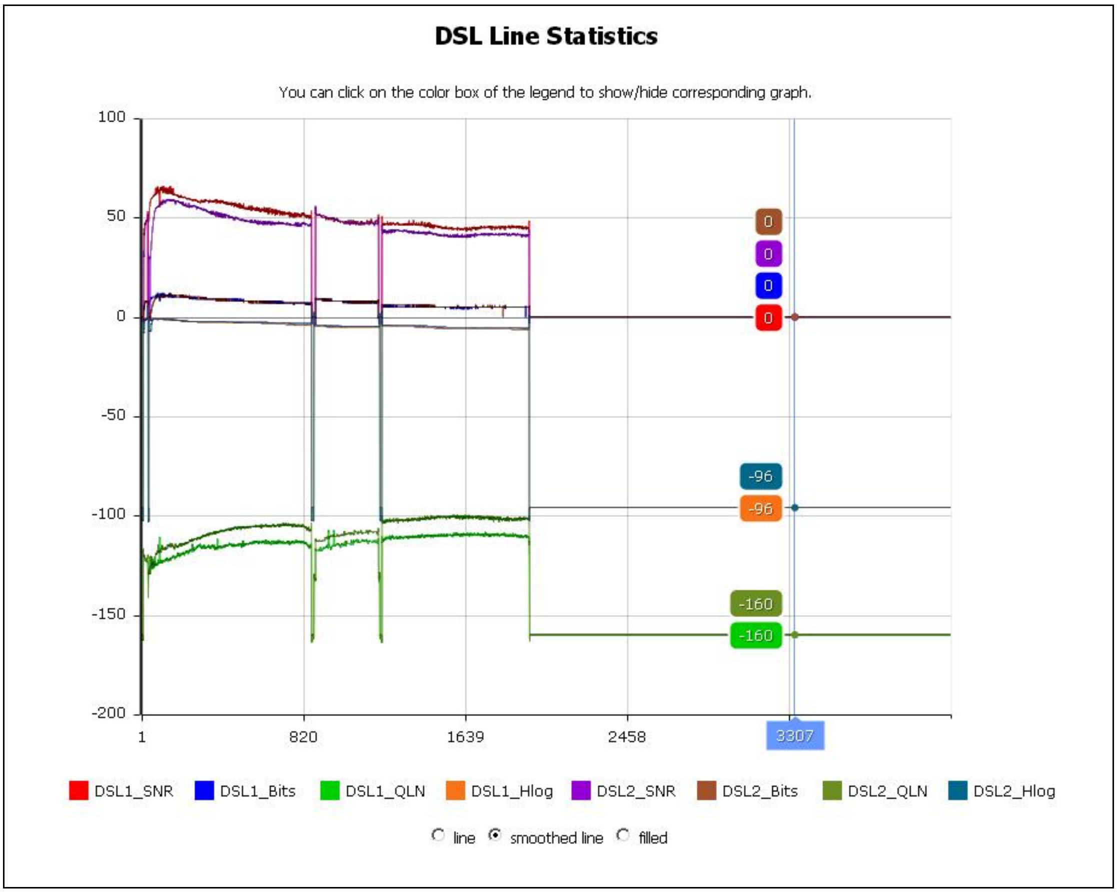
ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000000000000
Total Error Bits:	0x0000000000000000
Error Ratio:	Not Applicable

xDSL TONE GRAPH

Click **Draw Tone Graph** on the xDSL Statistics screen and a pop-up window will display the xDSL bits per tone status, as shown below.



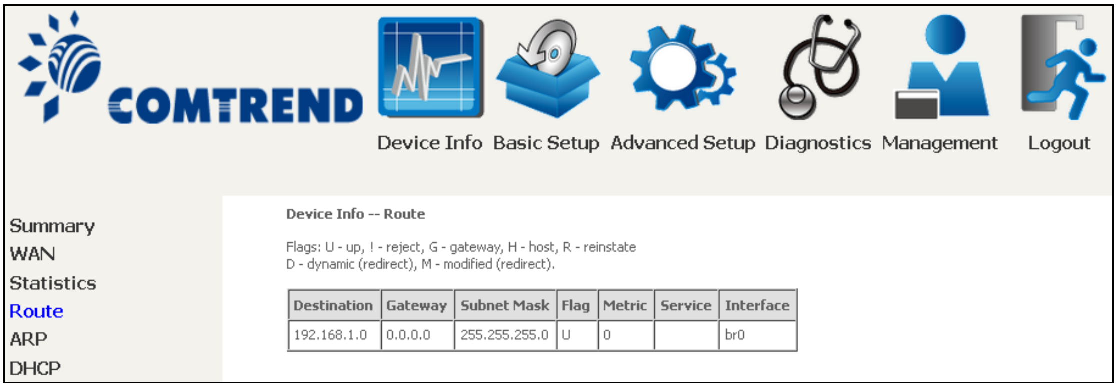
DSL Line Statistics

You can click on the color box of the legend to show/hide corresponding graph.

○ line ● smoothed line ○ filled

4.3 Route

Choose **Route** to display the routes that the NexusLink 3112u has found.



Device Info -- Route

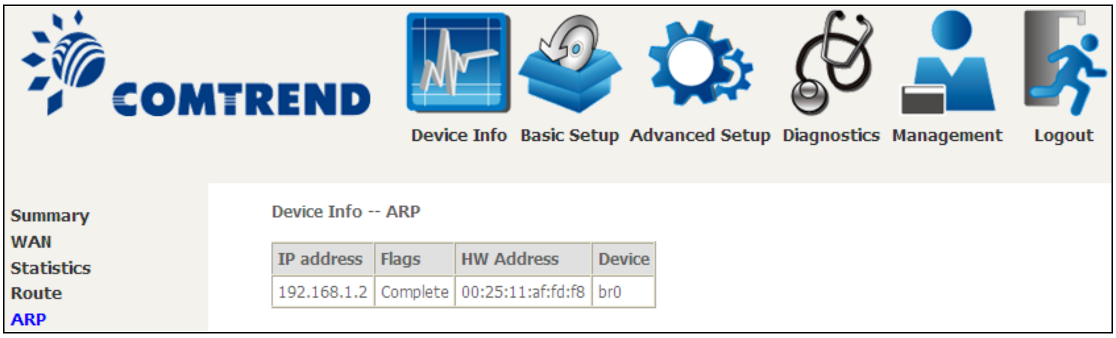
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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

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

4.4 ARP

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



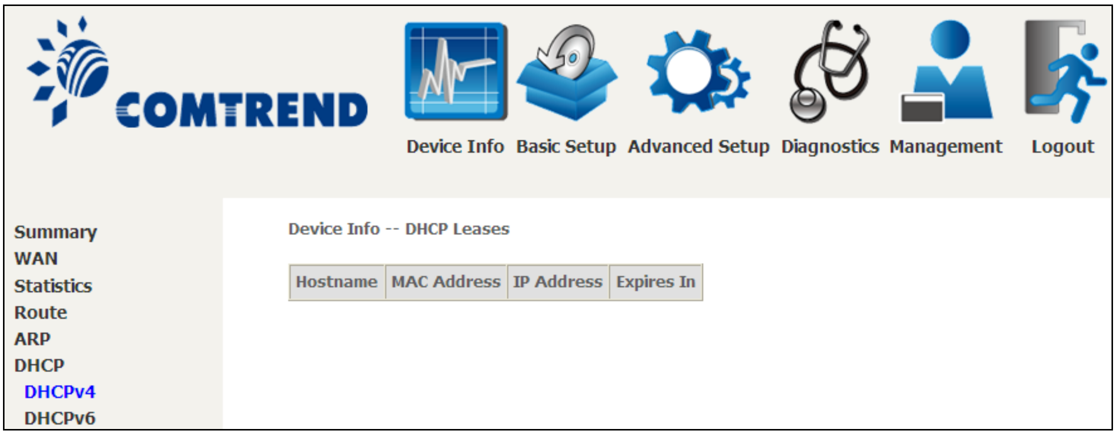
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:25:11:af:fd:f8	br0

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

4.5 DHCP

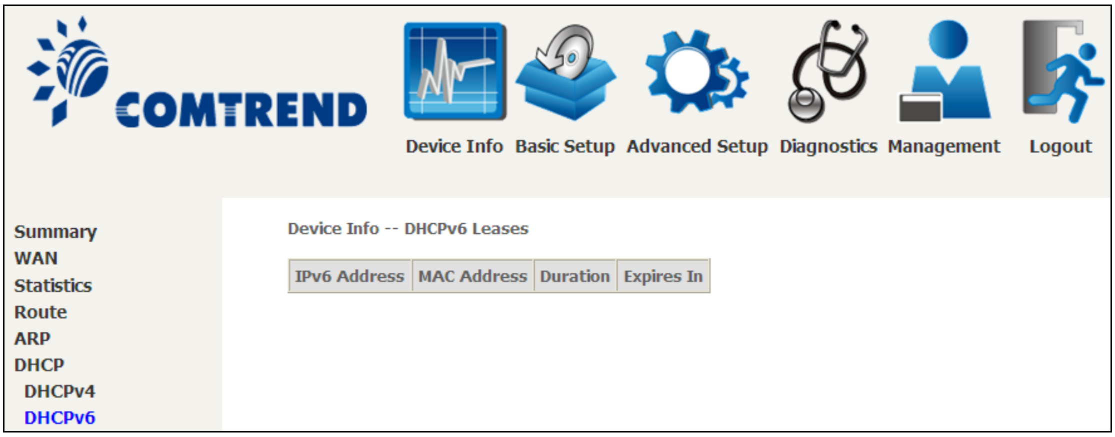
Click **DHCP** to display all DHCP Leases.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

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

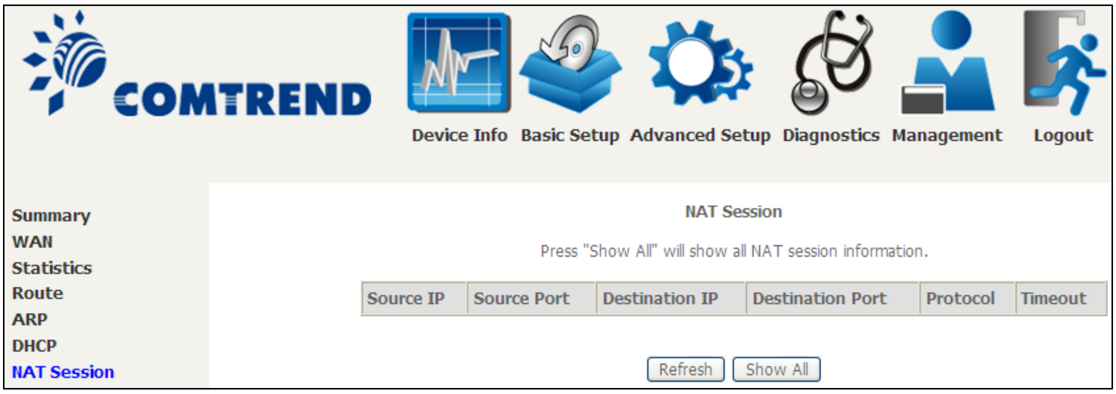


Device Info -- DHCPv6 Leases

IPv6 Address	MAC Address	Duration	Expires In

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

4.6 NAT Session

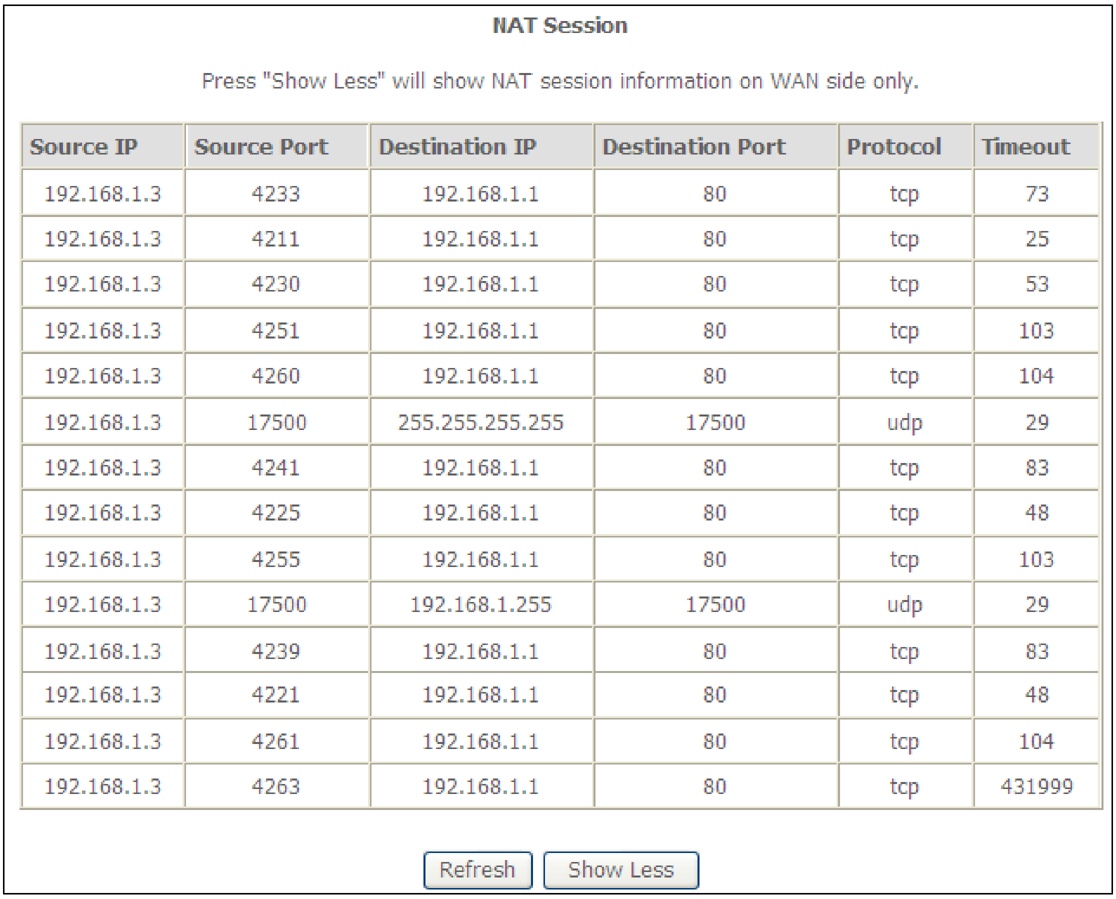


NAT Session

Press "Show All" will show all NAT session information.

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout

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



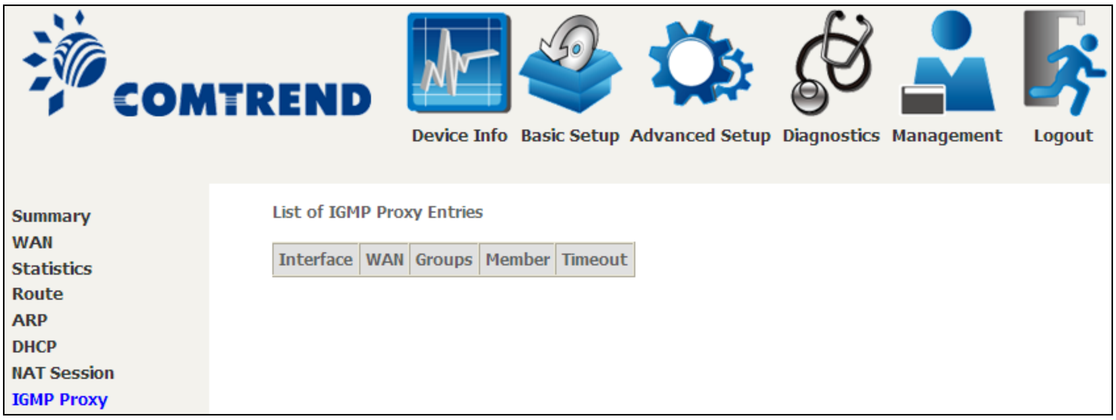
NAT Session

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

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.3	4233	192.168.1.1	80	tcp	73
192.168.1.3	4211	192.168.1.1	80	tcp	25
192.168.1.3	4230	192.168.1.1	80	tcp	53
192.168.1.3	4251	192.168.1.1	80	tcp	103
192.168.1.3	4260	192.168.1.1	80	tcp	104
192.168.1.3	17500	255.255.255.255	17500	udp	29
192.168.1.3	4241	192.168.1.1	80	tcp	83
192.168.1.3	4225	192.168.1.1	80	tcp	48
192.168.1.3	4255	192.168.1.1	80	tcp	103
192.168.1.3	17500	192.168.1.255	17500	udp	29
192.168.1.3	4239	192.168.1.1	80	tcp	83
192.168.1.3	4221	192.168.1.1	80	tcp	48
192.168.1.3	4261	192.168.1.1	80	tcp	104
192.168.1.3	4263	192.168.1.1	80	tcp	431999

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

4.7 IGMP Proxy



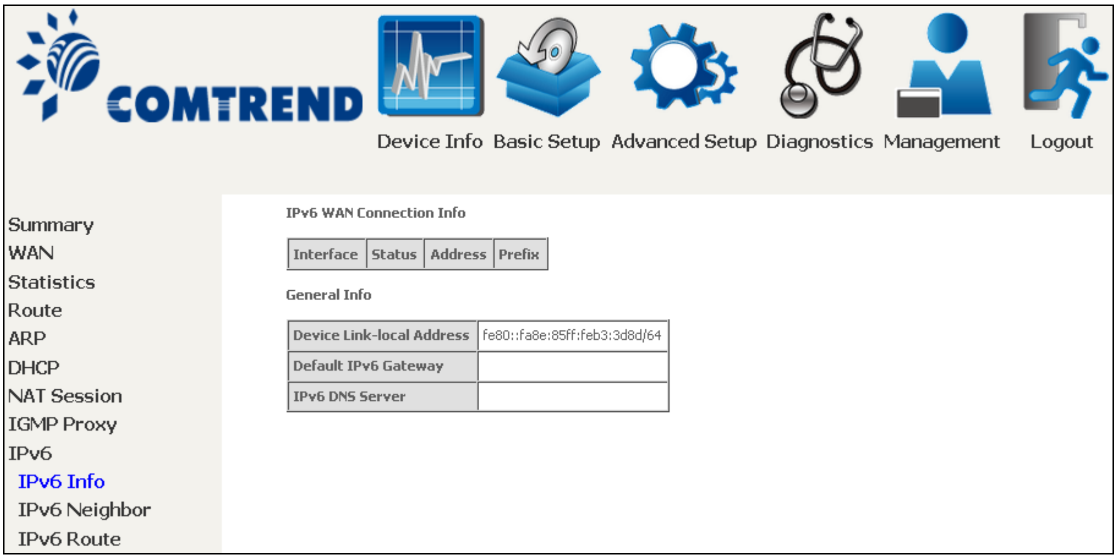
List of IGMP Proxy Entries

Interface	WAN	Groups	Member	Timeout

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

4.8 IPv6

4.8.1 IPv6 Info



IPv6 WAN Connection Info

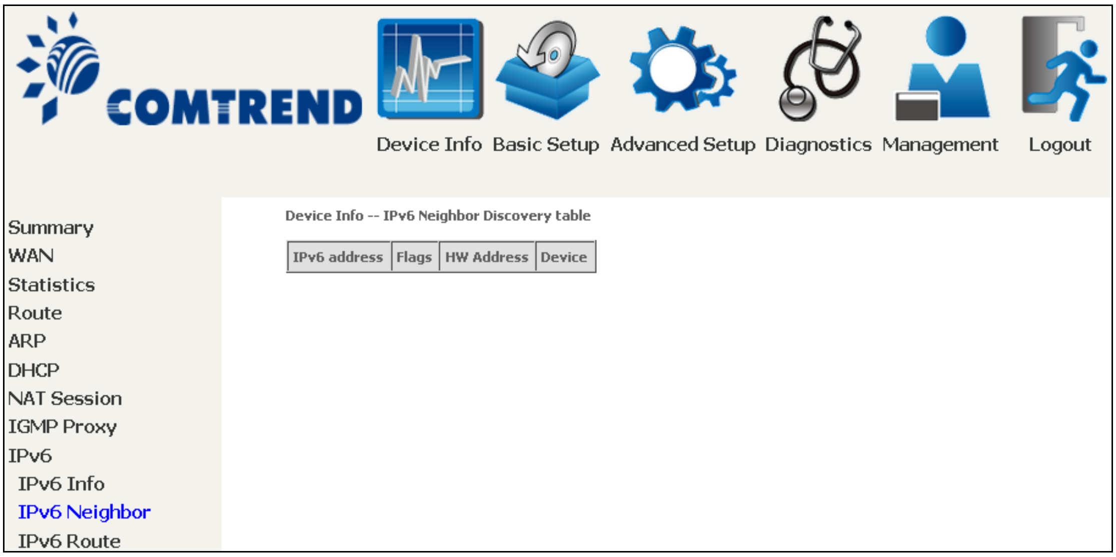
Interface	Status	Address	Prefix

General Info

Device Link-local Address	fe80::fa8e:85ff:feb3:3d8d/64
Default IPv6 Gateway	
IPv6 DNS Server	

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

4.8.2 IPv6 Neighbor

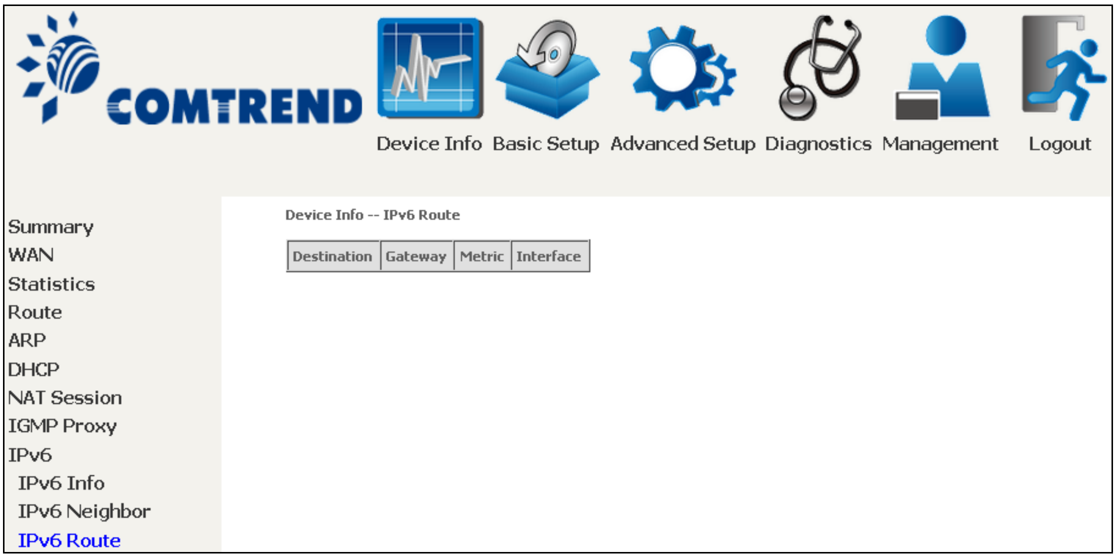


Device Info -- IPv6 Neighbor Discovery table

IPv6 address	Flags	HW Address	Device

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

4.8.3 IPv6 Route

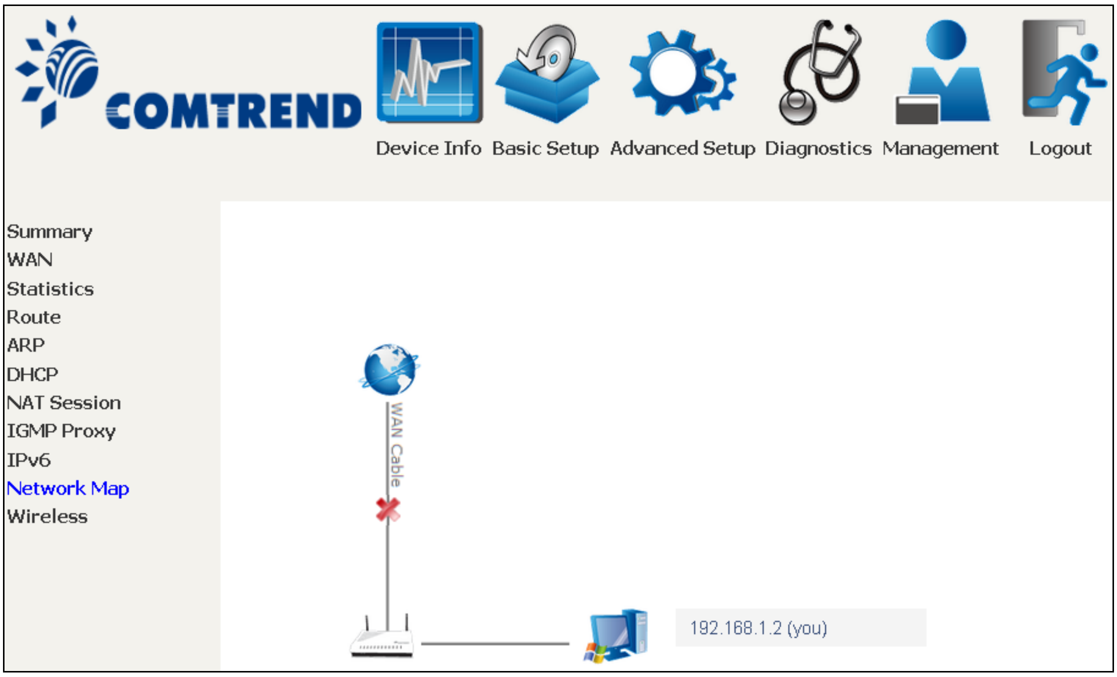


Device Info -- IPv6 Route

Destination	Gateway	Metric	Interface

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

4.9 Network Map



The network map feature provides an illustration of connected devices on the router.

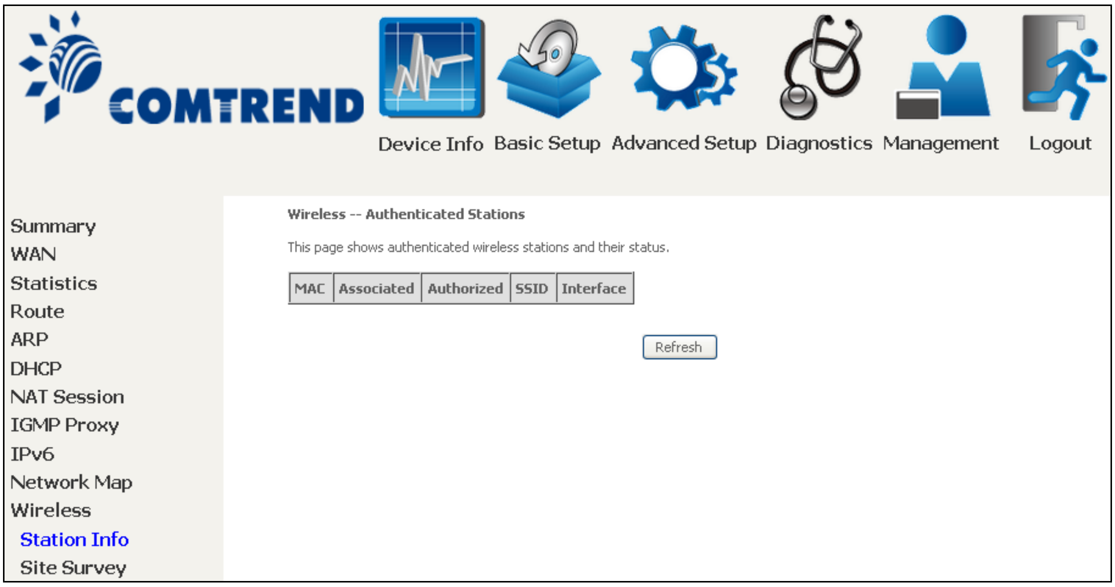
The current wan status (firewall on/off) is displayed on the left side.

Detailed information of PC/USB connected to the router is shown on the right side.

4.10 Wireless

4.10.1 Station Info

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



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

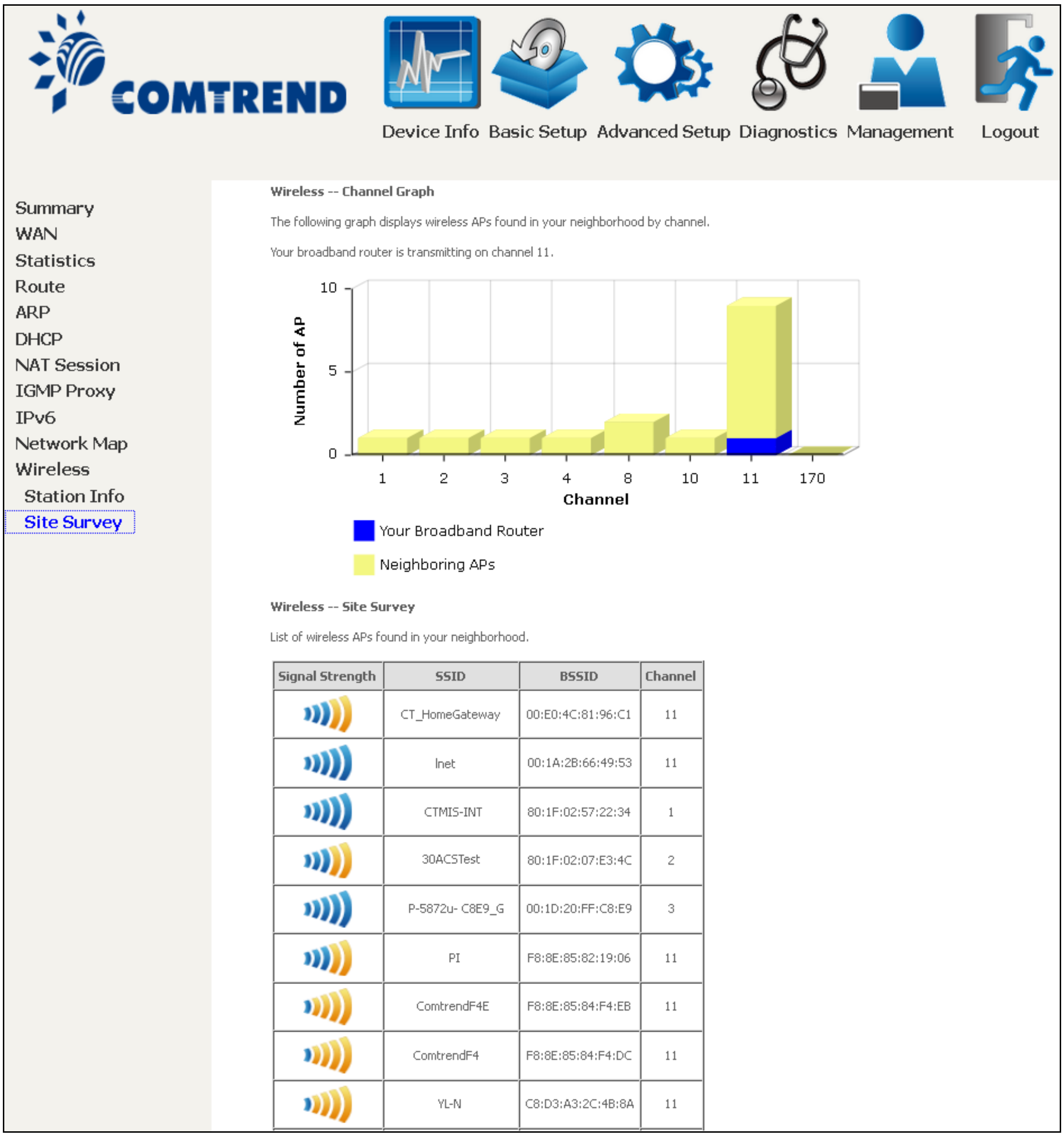
MAC	Associated	Authorized	SSID	Interface

Consult the table below for descriptions of each column heading.

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

4.10.2 Site Survey

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



Wireless -- Channel Graph

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

Your broadband router is transmitting on channel 11.

🟦 Your Broadband Router

🟨 Neighboring APs

Wireless -- Site Survey

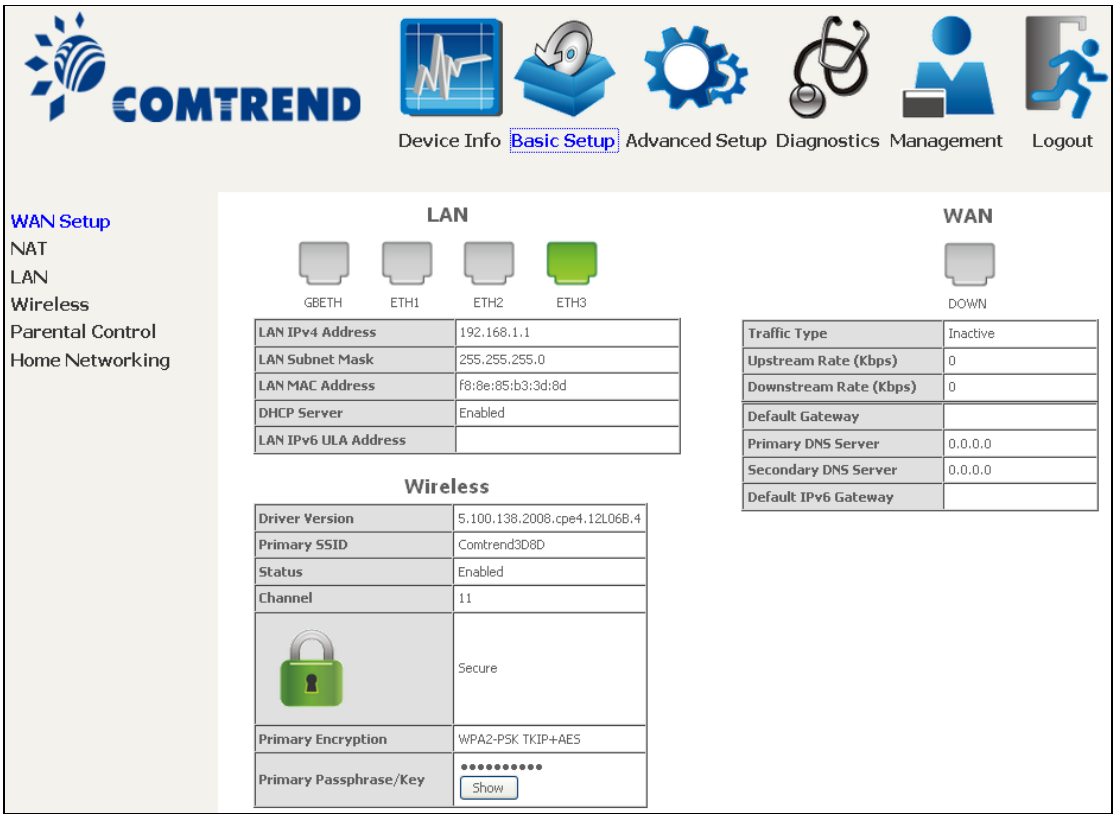
List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
📶	CT_HomeGateway	00:E0:4C:81:96:C1	11
📶	Inet	00:1A:2B:66:49:53	11
📶	CTMIS-INT	80:1F:02:57:22:34	1
📶	30ACSTest	80:1F:02:07:E3:4C	2
📶	P-5872u- C8E9_G	00:1D:20:FF:C8:E9	3
📶	PI	F8:8E:85:82:19:06	11
📶	ComtrendF4E	F8:8E:85:84:F4:EB	11
📶	ComtrendF4	F8:8E:85:84:F4:DC	11
📶	YL-N	C8:D3:A3:2C:4B:8A	11

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.



LAN

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:b3:3d:8d
DHCP Server	Enabled
LAN IPv6 ULA Address	

WAN

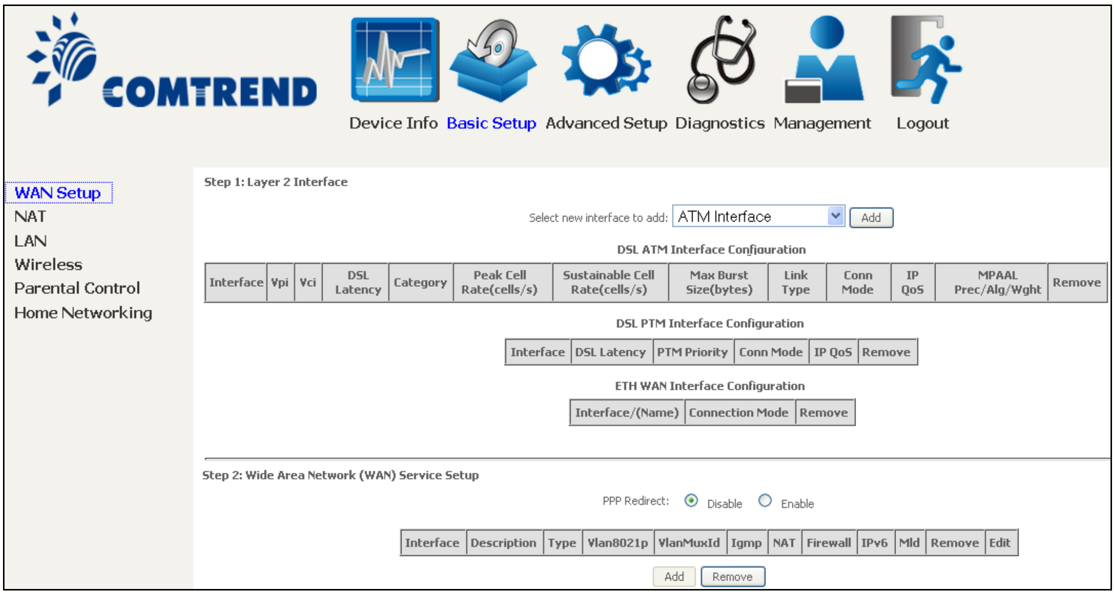
Traffic Type	Inactive
Upstream Rate (Kbps)	0
Downstream Rate (Kbps)	0
Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway	

Wireless

Driver Version	5.100.138.2008.cpe4.12L06B.4
Primary SSID	Comtrend3D8D
Status	Enabled
Channel	11
	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	●●●●●●●●●●

5.1 Wan Setup

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



Step 1: Layer 2 Interface

Select new interface to add: ATM Interface

DSL ATM Interface Configuration

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	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

PPP Redirect: ● Disable ○ Enable

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit

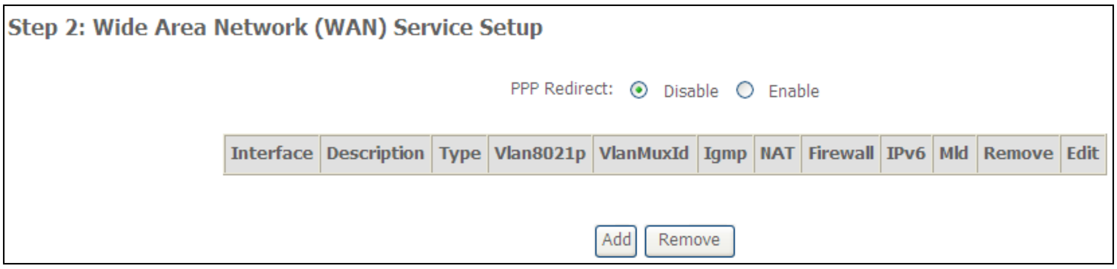
Click **Add** to create a new ATM interface (see Appendix E - Connection Setup).

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

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

5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.



Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: ● Disable ○ Enable

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit

Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see Appendix E - Connection Setup.

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

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD	Shows Multicast Listener Discovery (MLD) status
Remove	Select interfaces to remove

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

NOTE: ETH and ATM service connections cannot coexist. In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux Connection Mode supports up to 16 WAN connections.

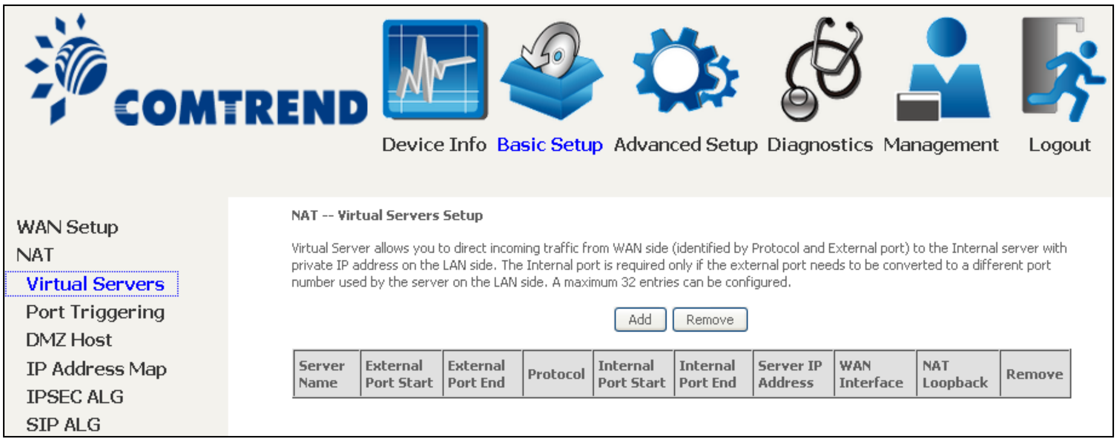
NOTE: Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist.

5.2 NAT

To display this option, NAT must be enabled in at least one PVC. *NAT is not an available option in Bridge mode*.

5.2.1 Virtual Servers

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

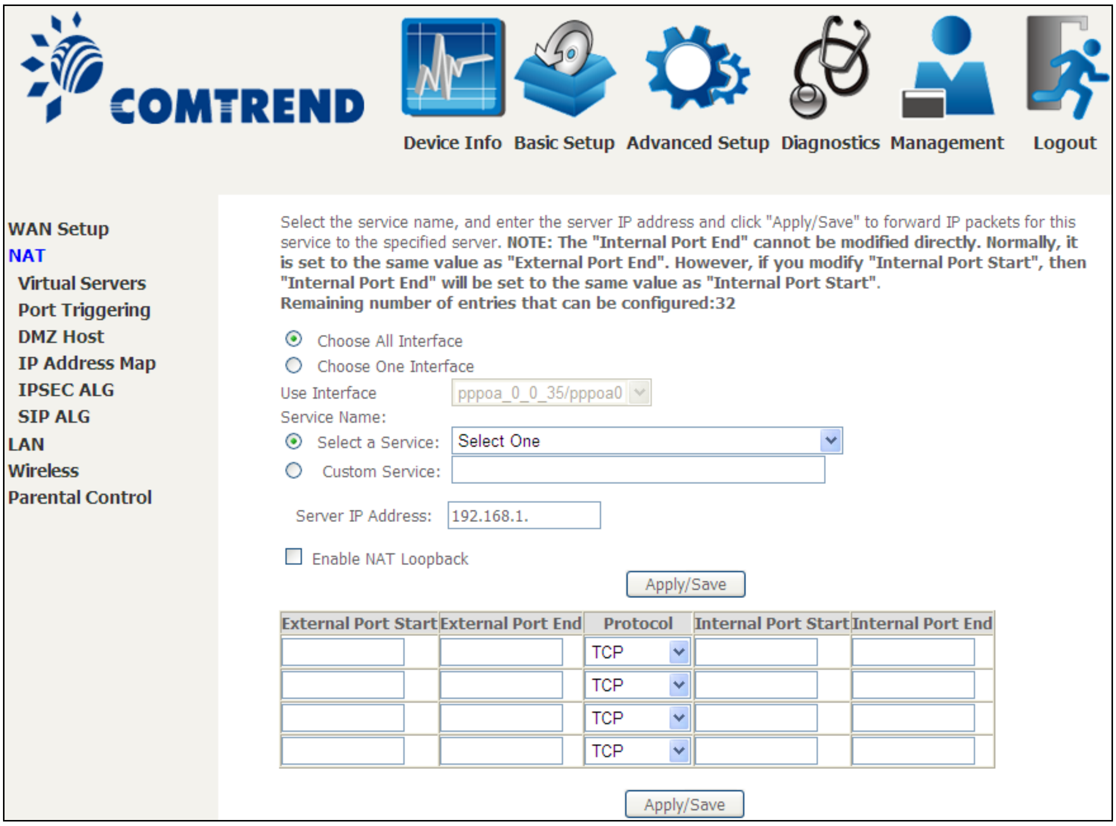


NAT -- Virtual Servers Setup

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

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.



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: pppoa_0_0_35/pppoa0
Service Name:
● Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.1.

□ Enable NAT Loopback

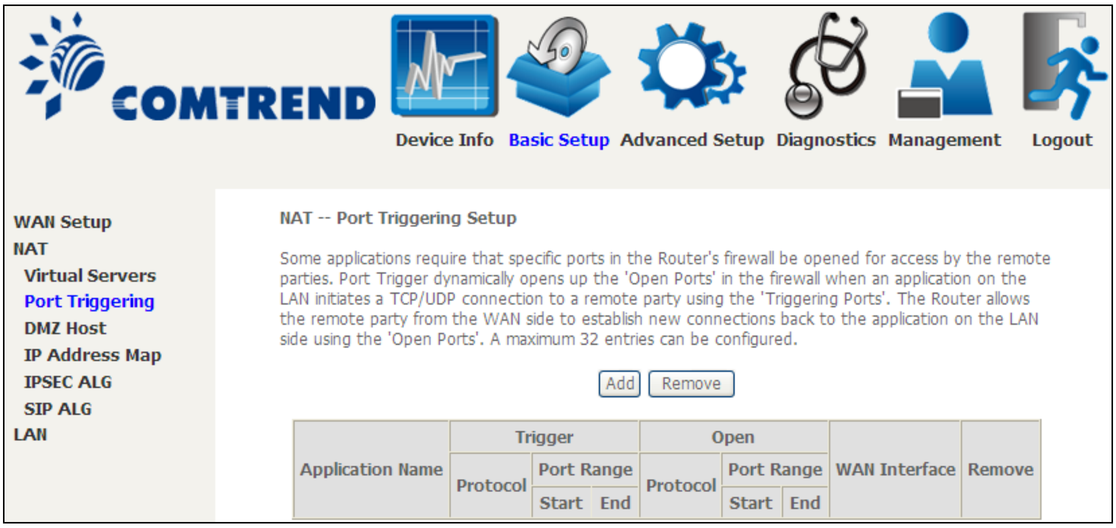
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		

Consult the table below for field and header descriptions.

Field/Header	**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 box.
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.

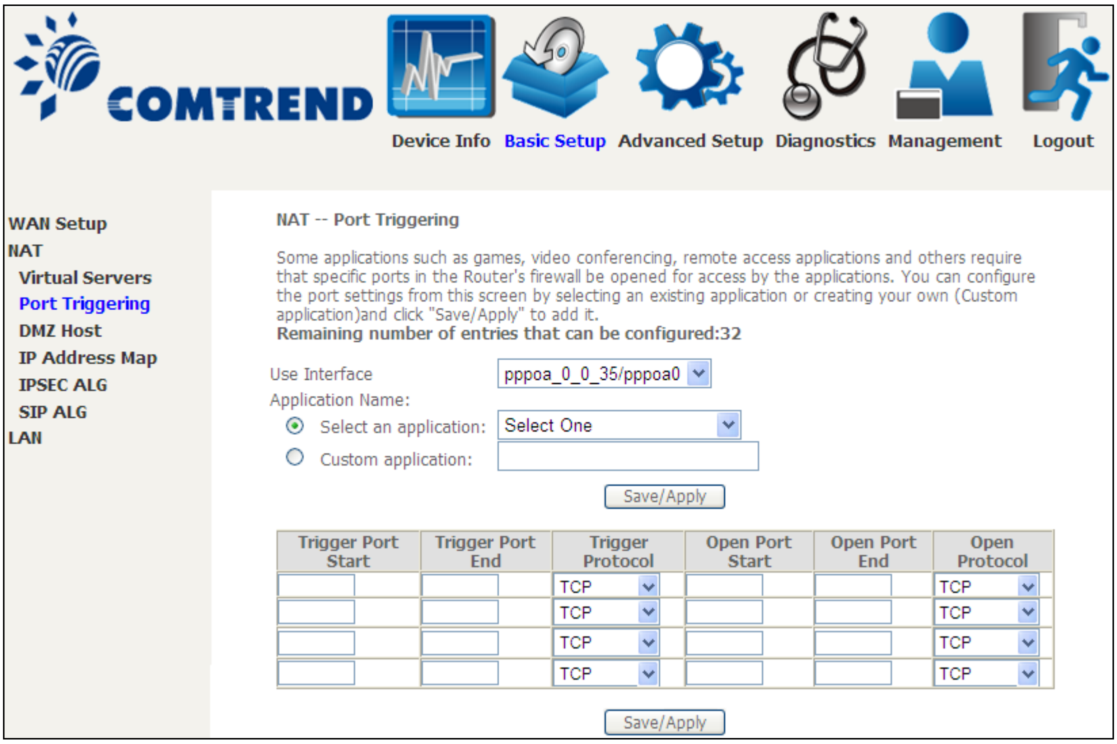


NAT -- Port Triggering Setup

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.

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: pppoa_0_0_35/pppoa0
Application Name:
● Select an application: Select One
○ Custom application:

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

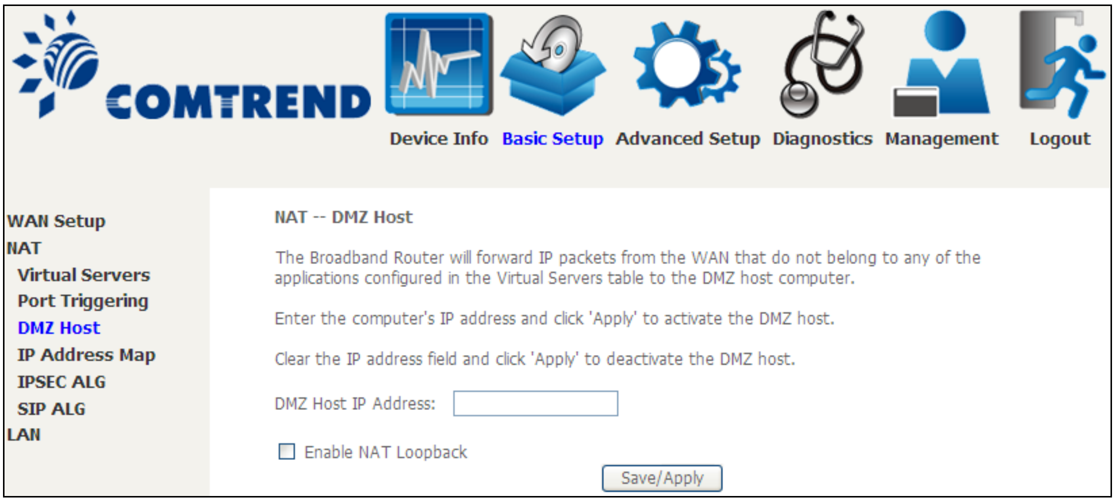
Click Save/Apply to save and apply the settings.

Consult the table below for field and header descriptions.

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



NAT -- DMZ Host

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

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

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

DMZ Host IP Address:

□ Enable NAT Loopback

Save/Apply

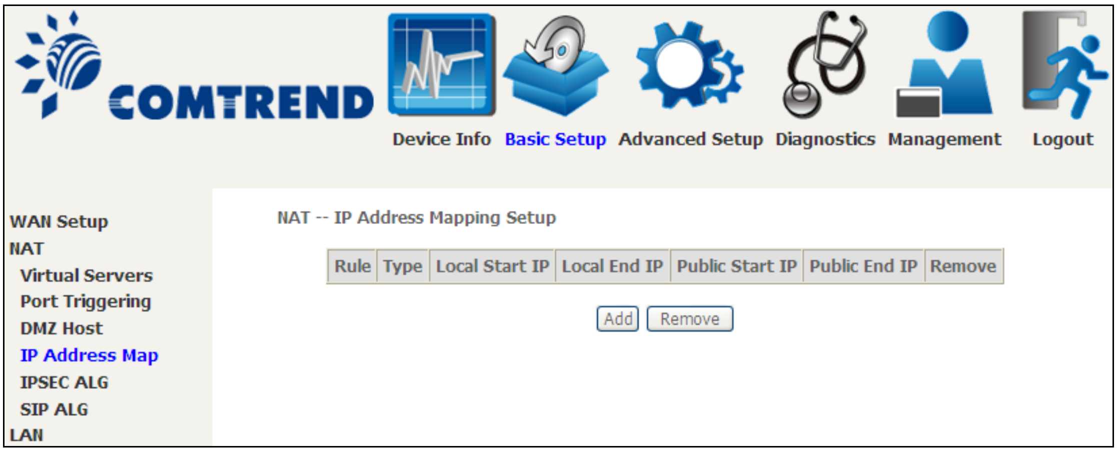
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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

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

5.2.4 IP Address Map

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

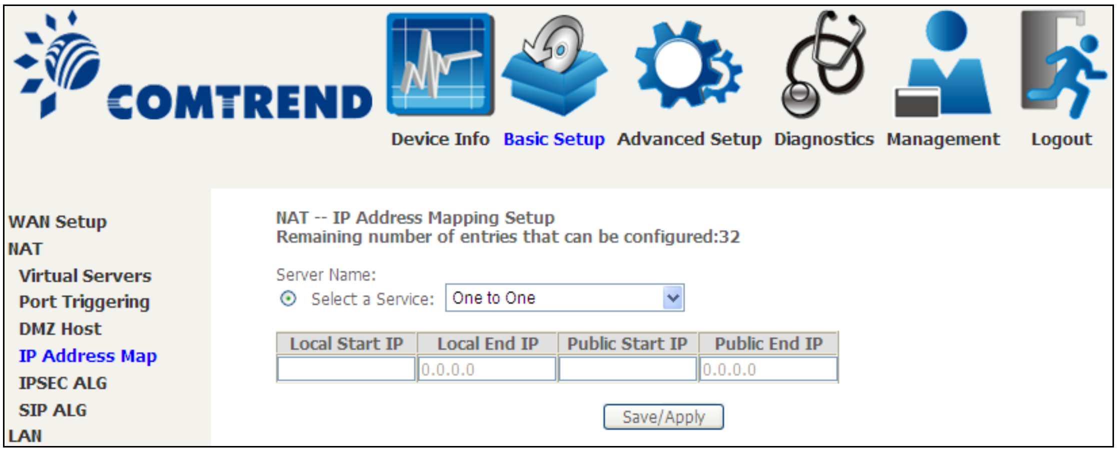


NAT -- IP Address Mapping Setup

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP	Remove

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

Click the Add button to display the following.



NAT -- IP Address Mapping Setup
Remaining number of entries that can be configured:32

Server Name:
● Select a Service: One to One

Local Start IP	Local End IP	Public Start IP	Public End IP
	0.0.0.0		0.0.0.0

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

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

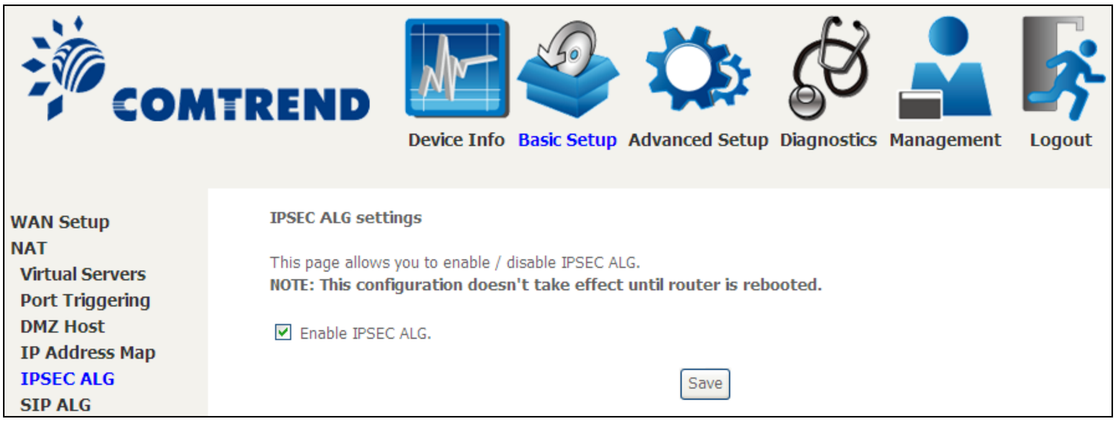
Many to one: mapping a range of local IP to a specific public IP

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 IPSEC ALG

IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.



IPSEC ALG settings

This page allows you to enable / disable IPSEC ALG.

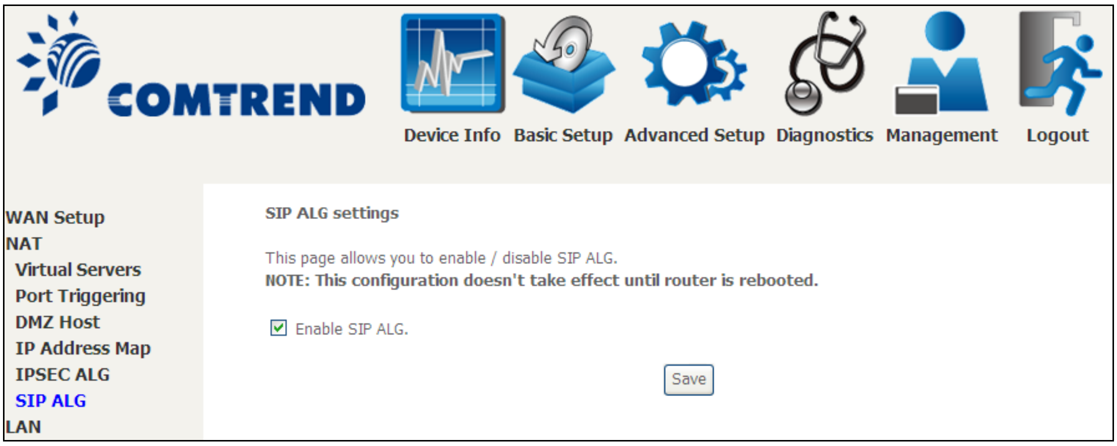
NOTE: This configuration doesn't take effect until router is rebooted.

☑ Enable IPSEC ALG.

To enable IPSEC ALG, tick the checkbox and click the **Save** button.

5.2.6 SIP ALG

This page allows you to enable / disable SIP ALG.



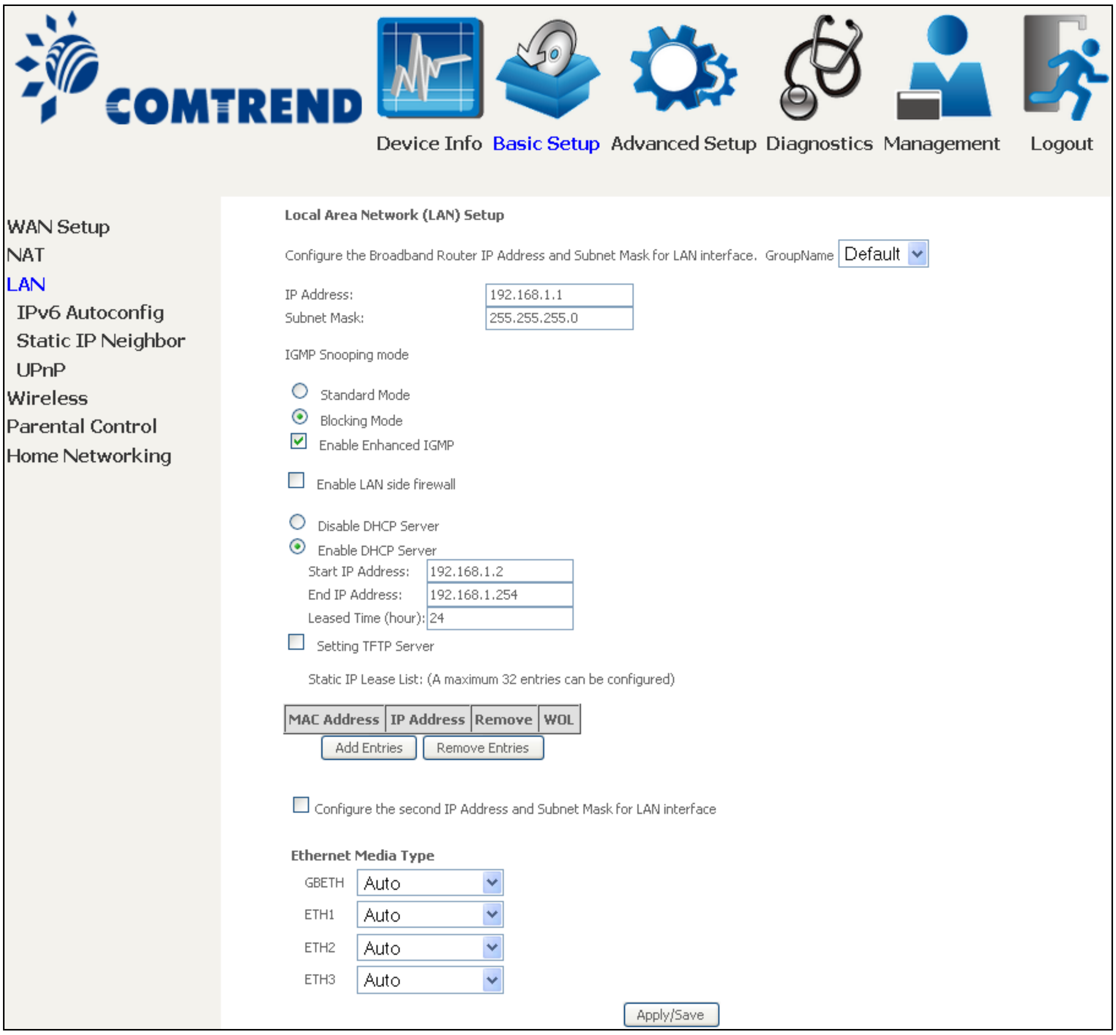
SIP ALG settings

This page allows you to enable / disable SIP ALG.
NOTE: This configuration doesn't take effect until router is rebooted.

☑ Enable SIP ALG.

5.3 LAN

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



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

IGMP Snooping mode

○ Standard Mode
● Blocking Mode
☑ Enable Enhanced IGMP

□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24

□ Setting TFTP Server

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

MAC Address	IP Address	Remove	WOL

□ Configure the second IP Address and Subnet Mask for LAN interface

Ethernet Media Type

GBETH: Auto
ETH1: Auto
ETH2: Auto
ETH3: Auto

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.

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.

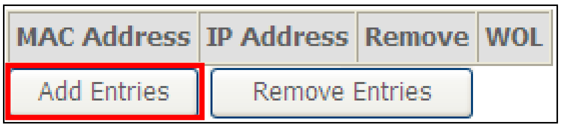
Enable Enhanced IGMP: Enable by ticking the checkbox ☑. IGMP packets between LAN ports will be blocked.

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

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

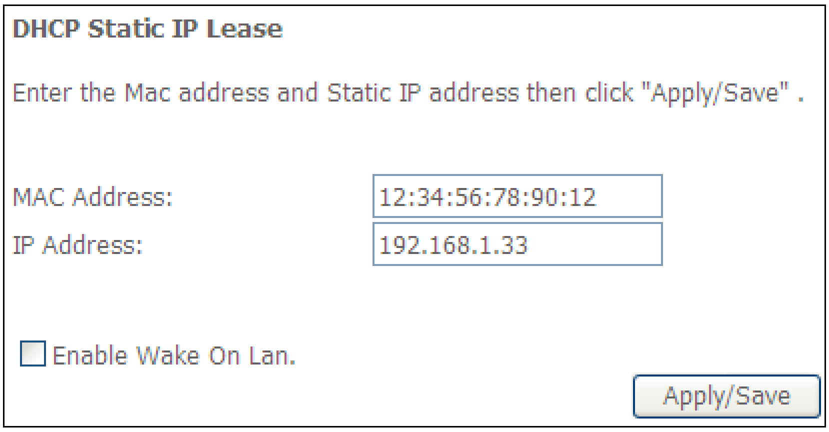
Setting TFTP Server: Enable by ticking the checkbox ☑. Then, input the TFTP server address or an IP address.

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



MAC Address	IP Address	Remove	WOL

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



DHCP Static IP Lease

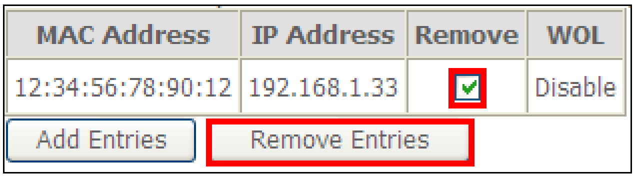
Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address: 12:34:56:78:90:12

IP Address: 192.168.1.33

□ Enable Wake On Lan.

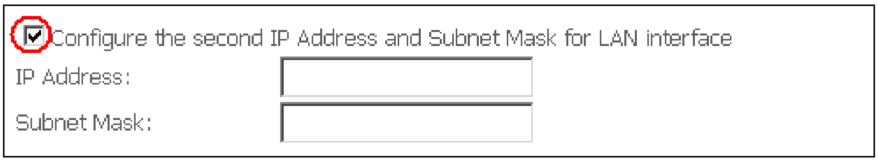
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



MAC Address	IP Address	Remove	WOL
12:34:56:78:90:12	192.168.1.33	☑	Disable

2ND LAN INTERFACE

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



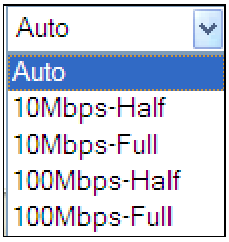
☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

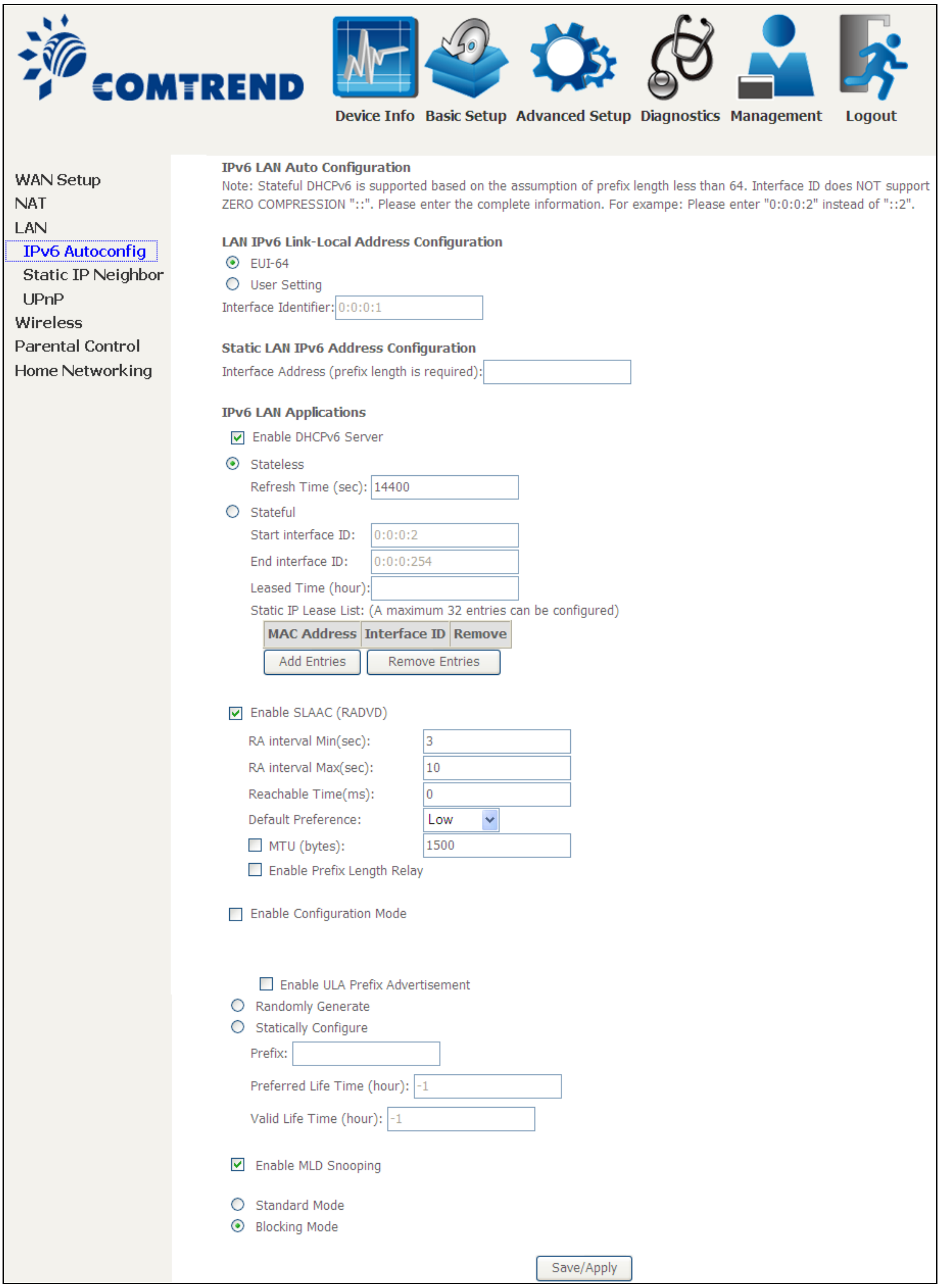
IP Address: Enter the secondary IP address for the LAN port.
Subnet Mask: Enter the secondary subnet mask for the LAN port.
Ethernet Media Type:

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



5.3.1 LAN IPv6 Autoconfig

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



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 exampe: Please enter "0:0:0:2" instead of "::2".

LAN IPv6 Link-Local Address Configuration

● EUI-64

○ User Setting

Interface Identifier: 0:0:0:1

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☑ Enable DHCPv6 Server

● Stateless

Refresh Time (sec): 14400

○ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour):

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

MAC Address	Interface ID	Remove

Add Entries   Remove Entries

☑ Enable SLAAC (RADVD)

RA interval Min(sec): 3

RA interval Max(sec): 10

Reachable Time(ms): 0

Default Preference: Low

□ MTU (bytes): 1500

□ Enable Prefix Length Relay

□ Enable Configuration Mode

□ Enable ULA Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Prefix:

Preferred Life Time (hour): -1

Valid Life Time (hour): -1

☑ Enable MLD Snooping

○ Standard Mode

● Blocking Mode

Save/Apply

Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

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

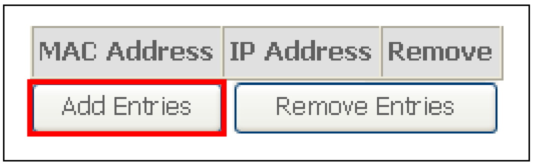
Static LAN IPv6 Address Configuration

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

IPv6 LAN Applications

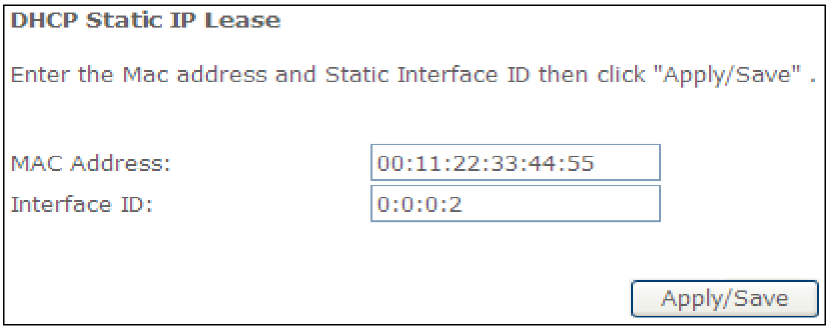
Heading	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to 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

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

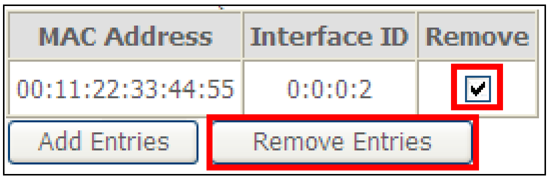


DHCP Static IP Lease

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

MAC Address:	00:11:22:33:44:55
Interface ID:	0:0:0:2

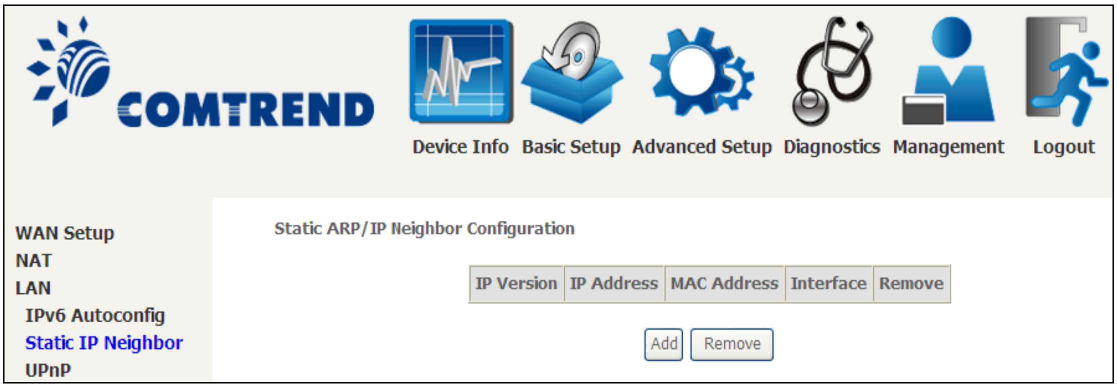
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



MAC Address	Interface ID	Remove
00:11:22:33:44:55	0:0:0:2	☑

Heading	**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 Configuration Mode	Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure Prefix	Specify the prefix to be used
Statically Configure	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

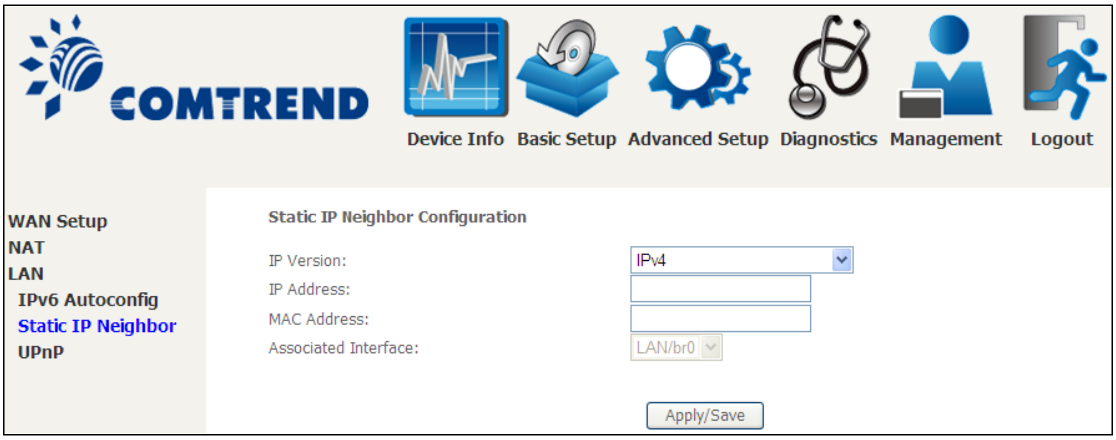
5.3.2 Static IP Neighbor



Static ARP/IP Neighbor Configuration

IP Version	IP Address	MAC Address	Interface	Remove

Click the Add button to display the following.



Static IP Neighbor Configuration

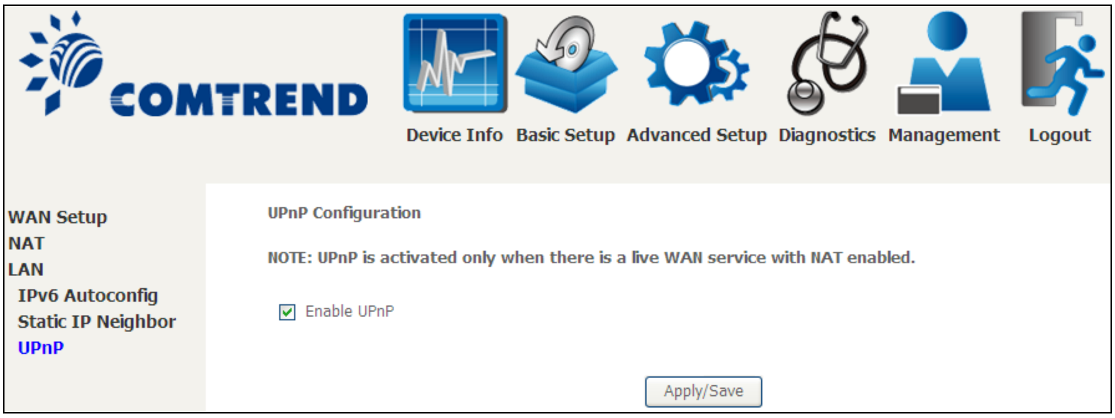
IP Version: IPv4
IP Address:
MAC Address:
Associated Interface: LAN/br0

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

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

5.3.3 UPnP

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



UPnP Configuration

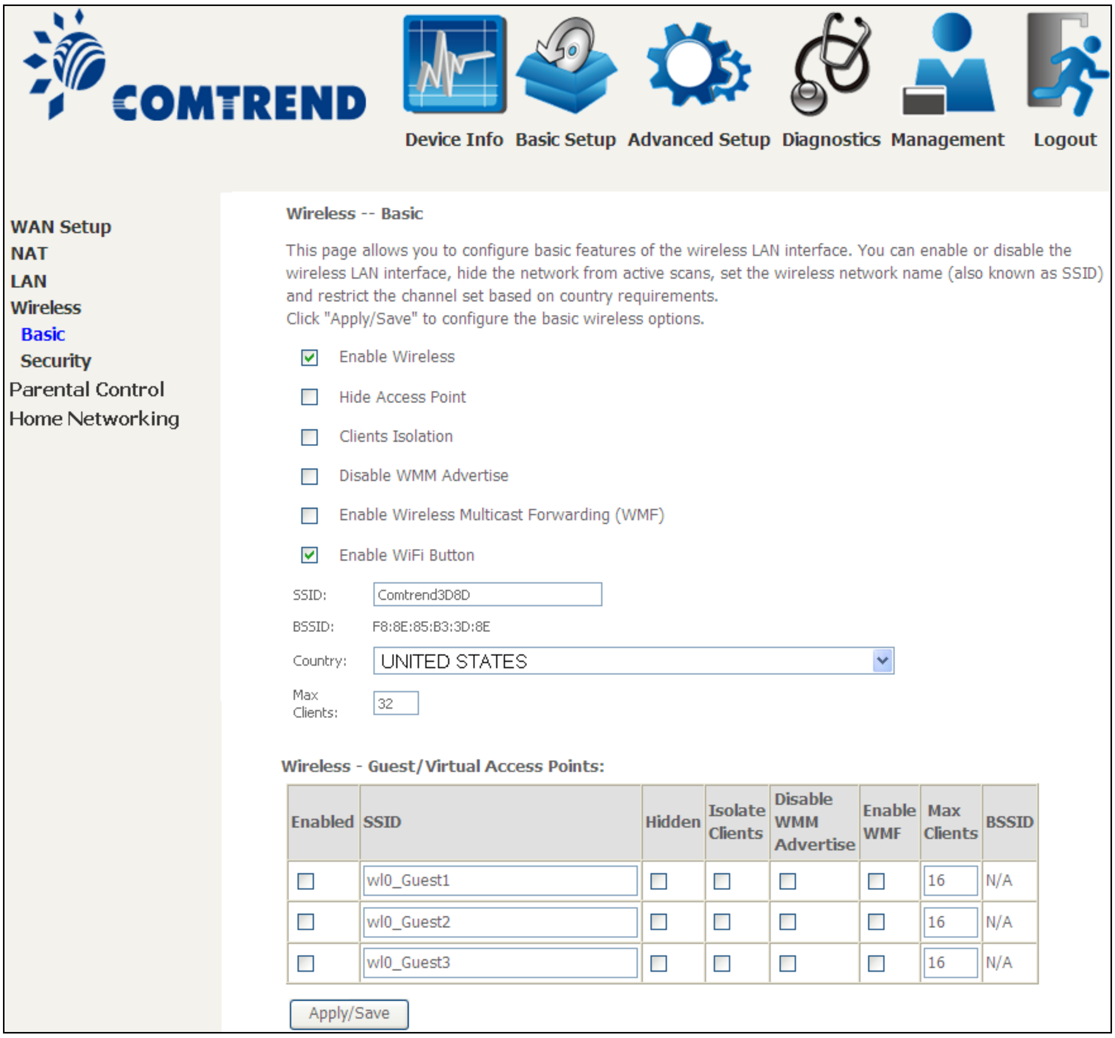
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ Enable UPnP

5.4 Wireless

5.4.1 Basic

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



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

☑ Enable WiFi Button

SSID: Comtrend3D8D

BSSID: F8:8E:85:B3:3D:8E

Country: UNITED STATES

Max Clients: 32

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	wl0_Guest1	□	□	□	□	16	N/A
□	wl0_Guest2	□	□	□	□	16	N/A
□	wl0_Guest3	□	□	□	□	16	N/A

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

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.

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

5.4.2 Security

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

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

WIRELESS SECURITY

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

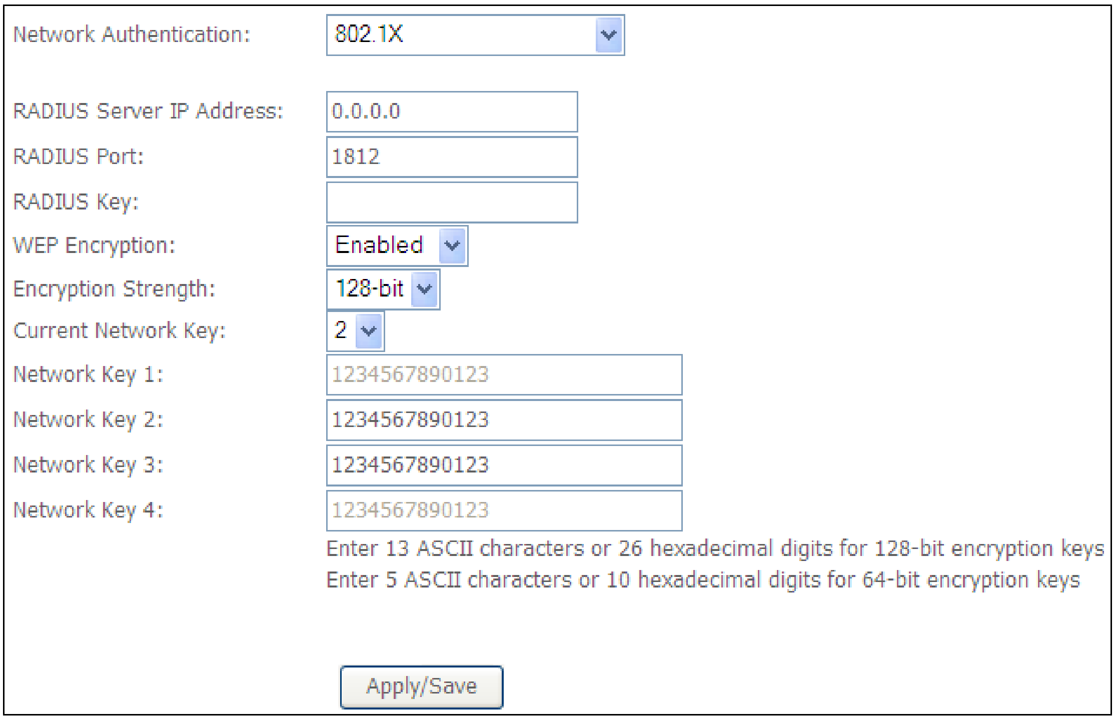
Select SSID

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

Network Authentication

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

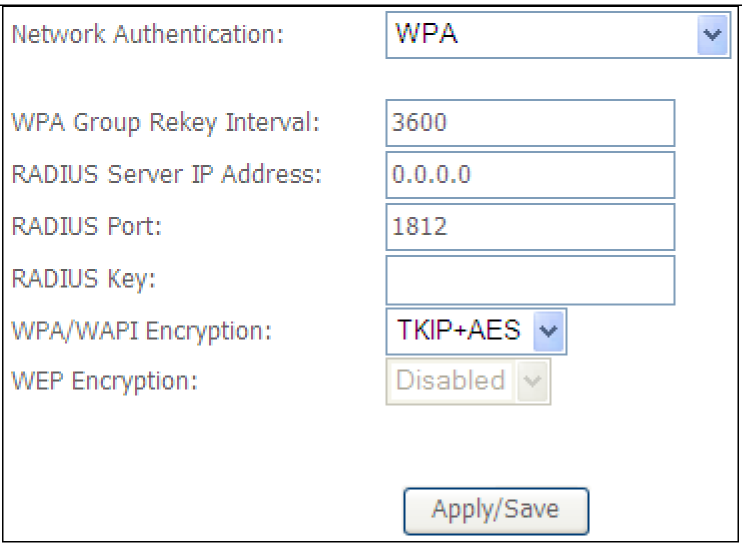
Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



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

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

The settings for WPA authentication are shown below.



Network Authentication: WPA

WPA Group Rekey Interval: 3600

RADIUS Server IP Address: 0.0.0.0

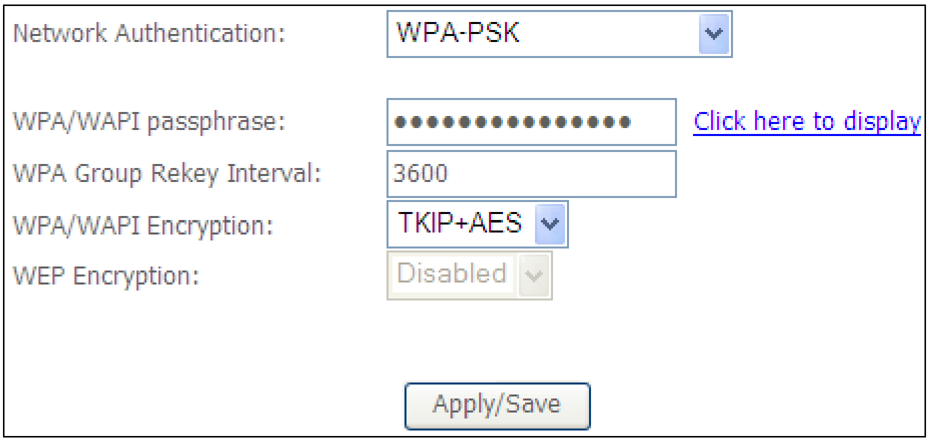
RADIUS Port: 1812

RADIUS Key:

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

The settings for WPA-PSK authentication are shown next.



Network Authentication: WPA-PSK

WPA/WAPI passphrase: ●●●●●●●●●●●●●●● Click here to display

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

WEP Encryption

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

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

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

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

Encryption Strength

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

Please see 6.13 for MAC Filter, Wireless Bridge and Advanced Wireless features.