VR-3033

Multi-DSL Wireless Router

User Manual

261099-037

Version A1.0, March 1, 2016

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.

FCC & ISED

User Information

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

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

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

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

This Class B digital apparatus complies with Canadian ICES-003.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.
This device complies with 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 choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.
Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s).

Son fonctionnement est soumis aux deux conditions suivantes:
1. Cet appareil ne peut pas provoquer d’interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

Radiation Exposure

FCC ID : L9VVR-3033U
IC : 4013C-VR3033U
US : 5SYDL01BVR-3033U

FCC

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

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

ISED

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

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

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 VR-3033 is an 802.11n compliant Multi-DSL router that supports both ADSL2+ and VDSL2 which is a brand new standard and technology perfect for triple play (Video, Voice and Data) applications. The VR-3033 comes with four 10/100 Base-T Ethernet ports, one USB host, combining wired LAN connectivity and an integrated high power802.11n WiFi WLAN Access Point (AP) for wireless connectivity.

The VR-3033 is a solution designed to meet the needs of ISPs and carriers planning on deploying a single DSL device for covering end users in different loop range areas. Deploying VR-3033 is cost effective for ISPs and carriers because deploying a single CPE DSL device with multiple profile support minimizes the number of required upgrades.

Antenna Information:

WLAN 2.4GHz Antenna-ANT-0	
Frequency Range	2412 MHz - 2462 MHz
Trade Name / Manufacturers	MAG. LAYERS SCIENTIFIC-TECHNICS CO., LTD
Model Name	EDA-1313-2G4C1-B4
Antenna Type	External Antenna
Antenna Gain	2.59 dBi
WLAN 2.4GHz Antenna-ANT-1	
Frequency Range	2412 MHz - 2462 MHz
Trade Name / Manufacturers	MAG. LAYERS SCIENTIFIC-TECHNICS CO., LTD
Model Name	EDA-1313-2G4C1-B3
Antenna Type	External Antenna
Antenna Gain	2.63 dBi

Chapter 2 Installation

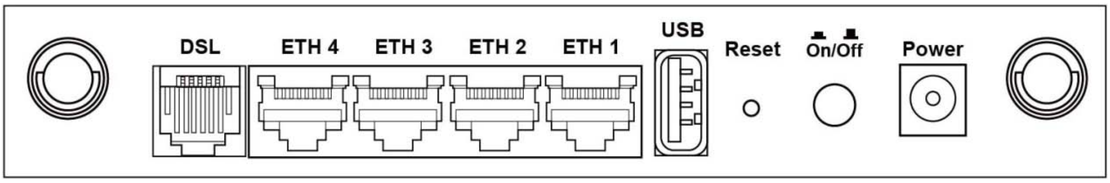
2.1 Hardware Setup

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.

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 VR-3033 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.

USB Host Port (Type A)

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

Ethernet (LAN) Ports

Use 10/100 BASE-T RJ-45 cables to connect up to four network devices. 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 RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

FRONT PANEL

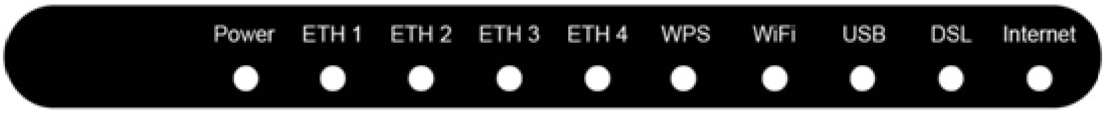
WiFi / WPS Button

Press and release WiFi-WPS button to activate WPS (make sure the WPS is enabled in Wireless->Security page).

Press and hold WiFi-WPS button more than 10 seconds to enable/disable WiFi.

2.2 LED Indicators

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



LED	Color	Mode	Function
POWER	GREEN	On	The device is powered up.
		Off	The device is powered down.
	RED	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
ETH 1 to 4	GREEN	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
WPS	GREEN	On	WPS enabled and PC connected to WLAN.
		Off	WPS disenabled when WPS configured. After clients are connected to router for about 5 minutes, LED is OFF.
		Blink	The router is searching for WPS clients or WPS is un-configured.
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.
USB	GREEN	On	USB mass storage, USB hub or USB printer is connected; or 3G USB dongle connection is UP.
		Off	No USB device connected.
DSL	GREEN	On	xDSL Link is established.
		Off	The device is powered down.
		Blink	fast: xDSL Link is training or data transmitting. slow: xDSL training failed.
INTERNET	GREEN	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
		Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.

	🟩	Blink	IP connected and IP Traffic is passing thru the device (either direction)
	RED	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

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

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the VR-3033 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.

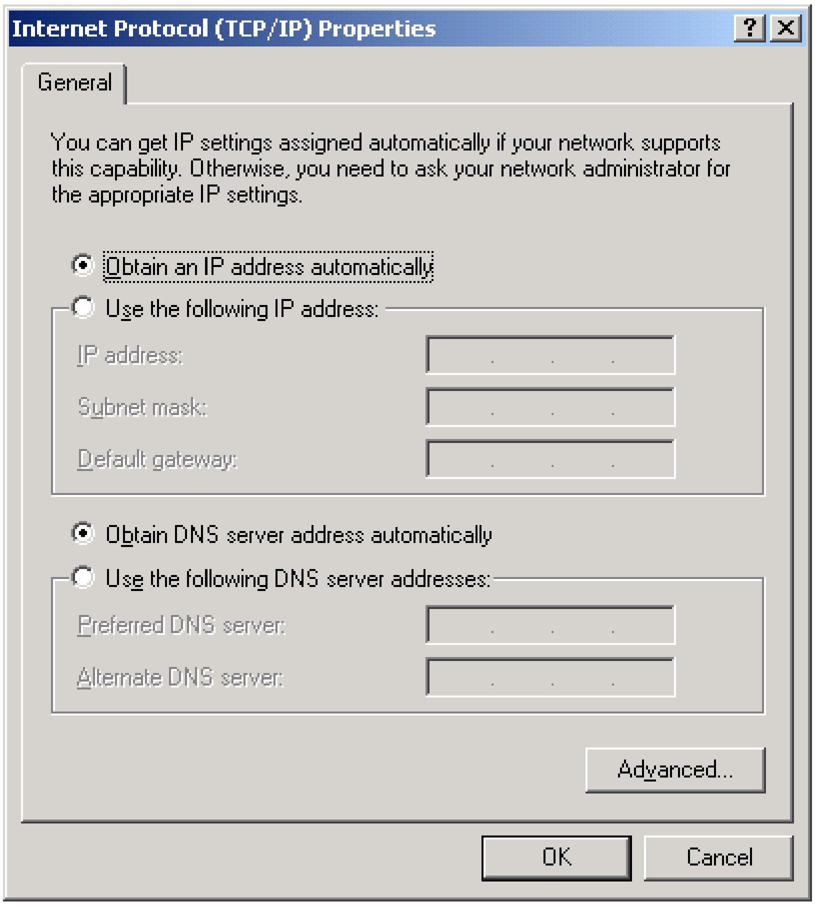
To obtain an IP address from the DCHP server, follow the steps provided below.

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.

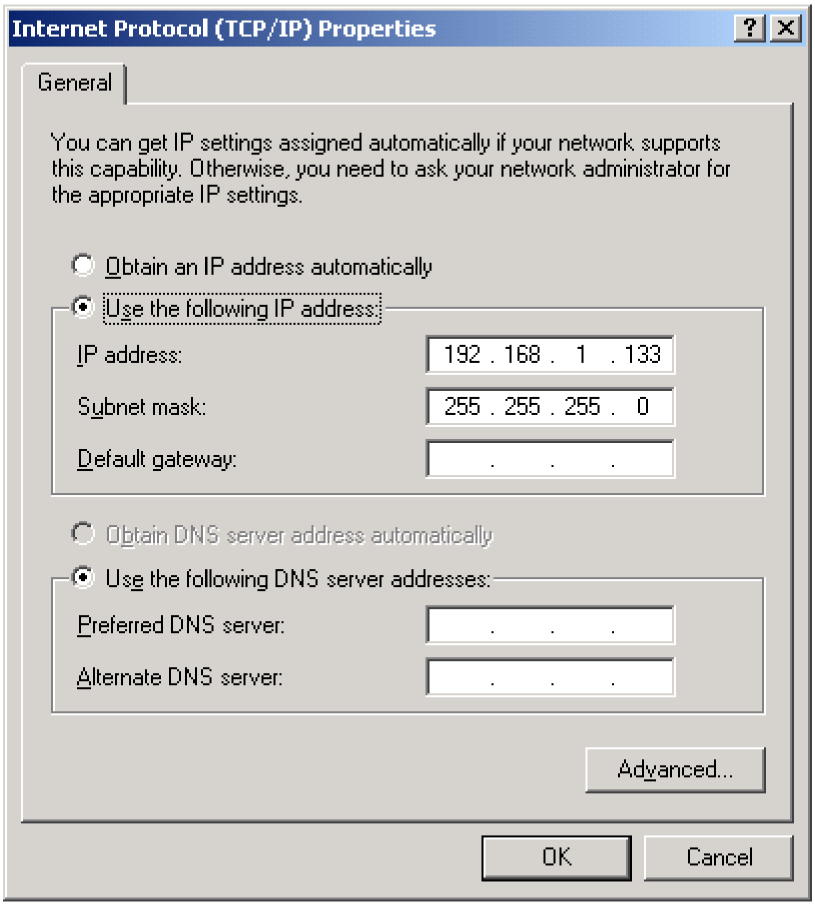
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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.



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

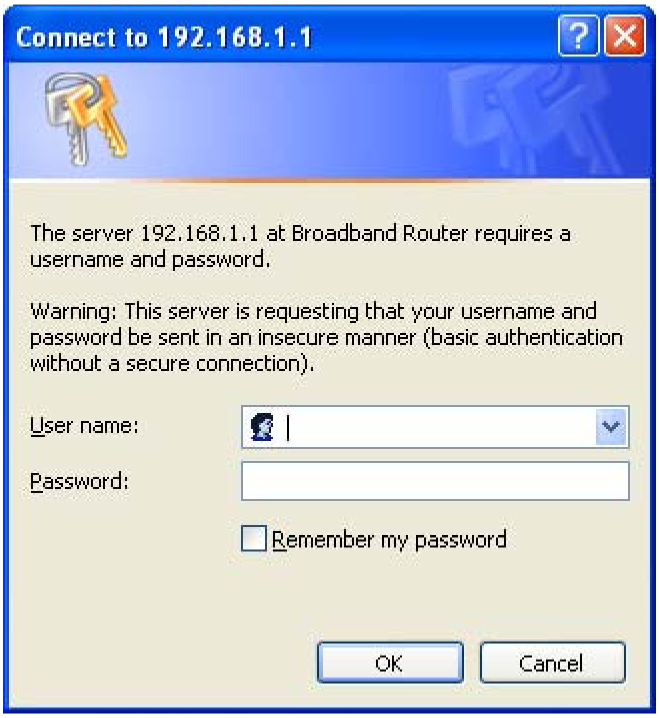
Perform the following steps to login to the web user interface.

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:

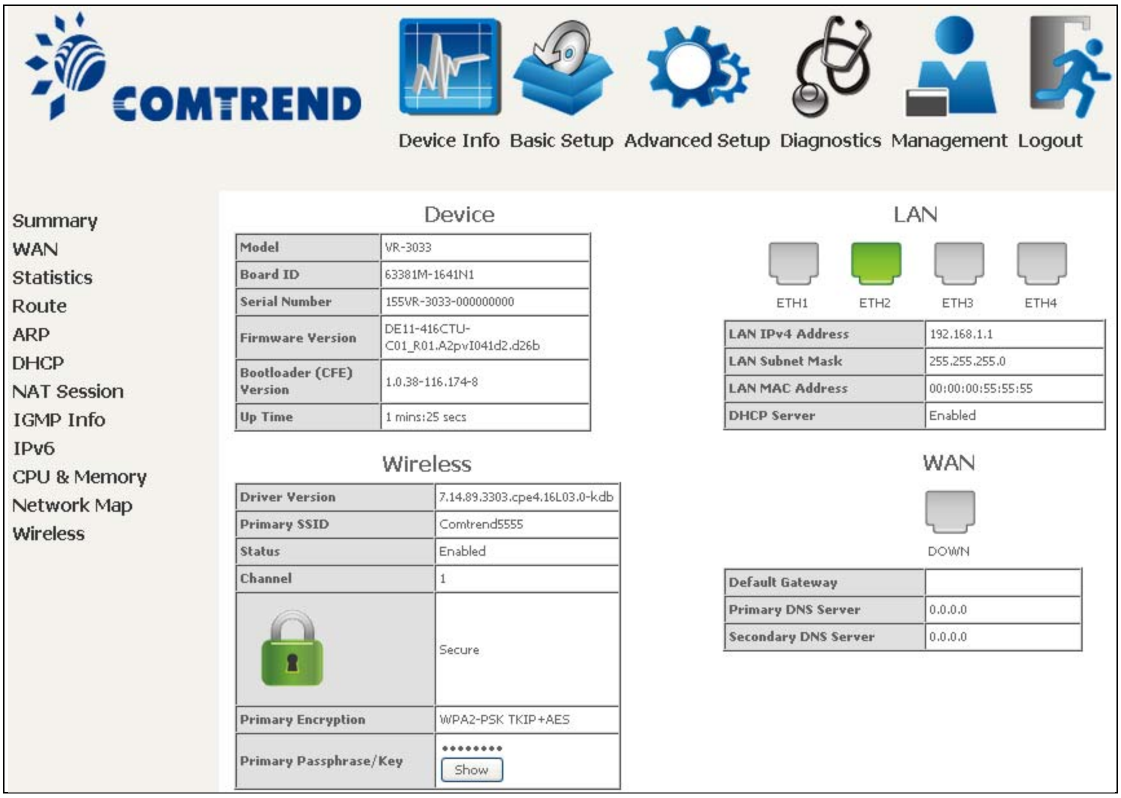
Password:

□ 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	VR-3033
Board ID	63381M-1641N1
Serial Number	155VR-3033-000000000
Firmware Version	DE11-416CTU-C01_R01.A2pvI041d2.d26b
Bootloader (CFE) Version	1.0.38-116.174-8
Up Time	1 mins:25 secs

Wireless

Driver Version	7.14.89.3303.cpe4.16L03.0-kdb
Primary SSID	Comtrend5555
Status	Enabled
Channel	1
	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	••••••••

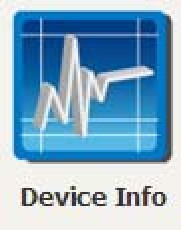
LAN

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

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

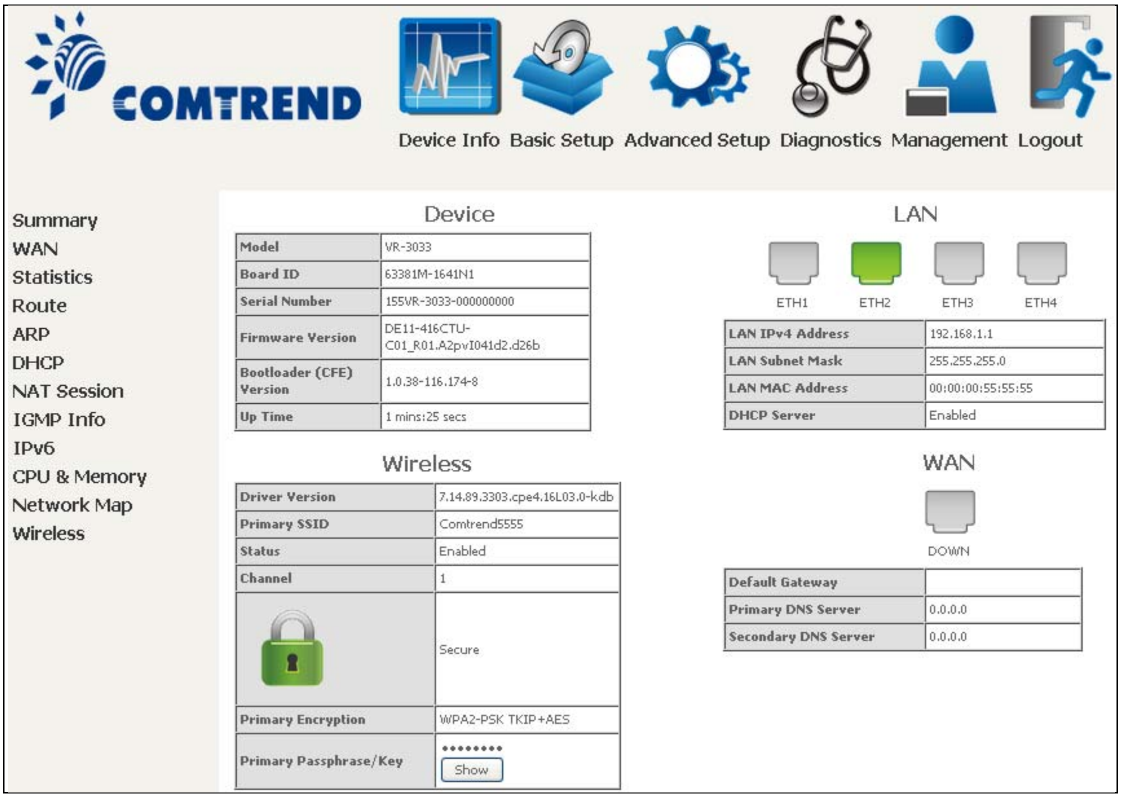
You can reach this page by clicking on the following icon located at the top of the screen.

The web user interface window is divided into two frames, the main menu (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	VR-3033
Board ID	63381M-1641N1
Serial Number	155VR-3033-000000000
Firmware Version	DE11-416CTU-C01_R01.A2pvI041d2.d26b
Bootloader (CFE) Version	1.0.38-116.174-8
Up Time	1 mins:25 secs

LAN

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

Wireless

Driver Version	7.14.89.3303.cpe4.16L03.0-kdb
Primary SSID	Comtrend5555
Status	Enabled
Channel	1
	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	••••••••

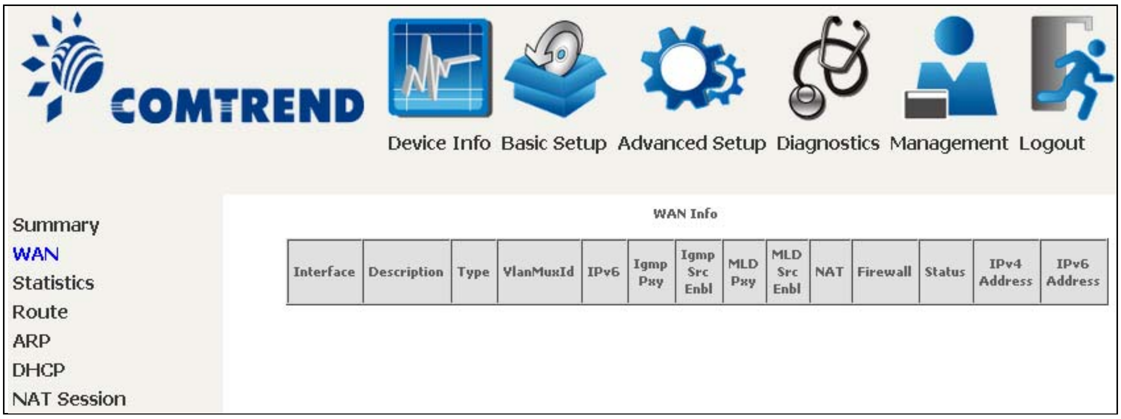
WAN

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).



WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	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 Pxy	Shows Internet Group Management Protocol (IGMP) proxy status
Igmp Src Enbl	Shows the status of WAN interface used as IGMP source
MLD Pxy	Shows Multicast Listener Discovery (MLD) proxy status
MLD Src Enbl	Shows the status of WAN interface used as MLD source
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address
IPv6 Address	Shows WAN IPv6 address

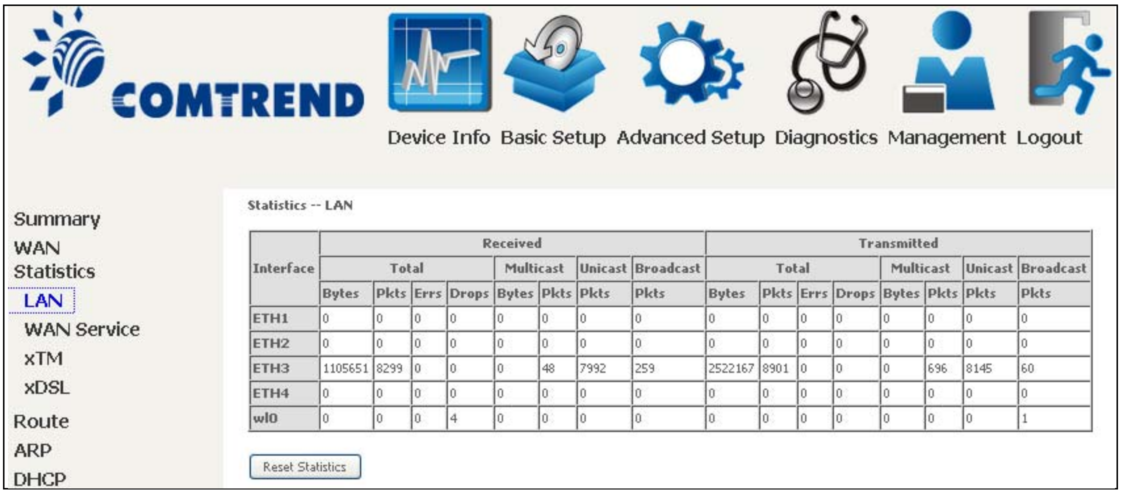
4.2 Statistics

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

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

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



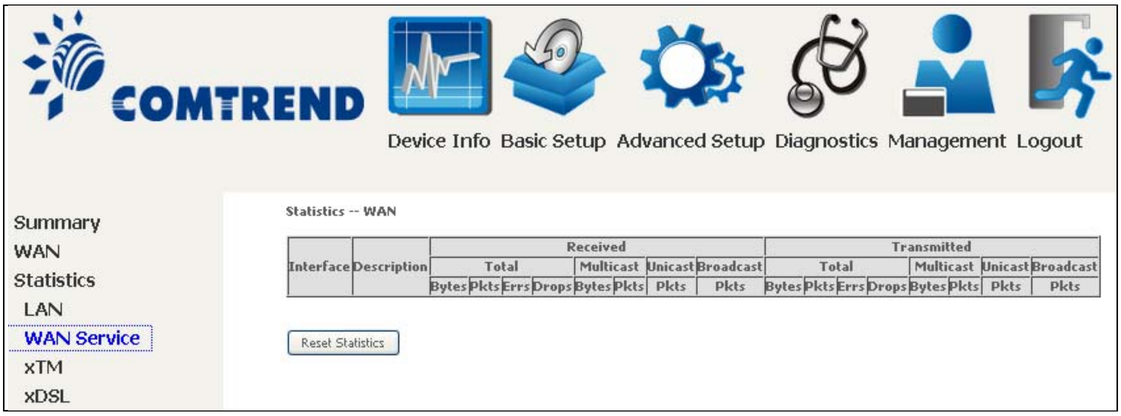
Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ETH1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH3	1105651	8299	0	0	0	48	7992	259	2522167	8901	0	0	0	696	8145	60
ETH4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	1

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.



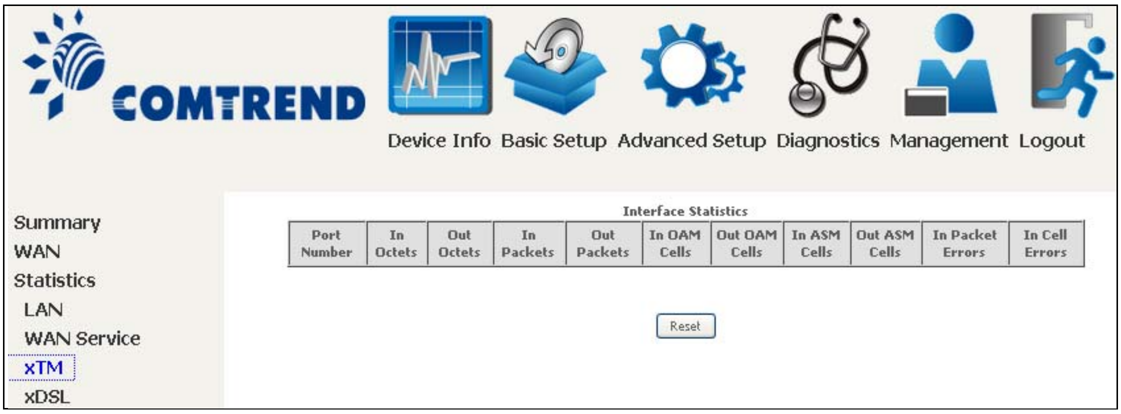
Statistics -- WAN

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

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

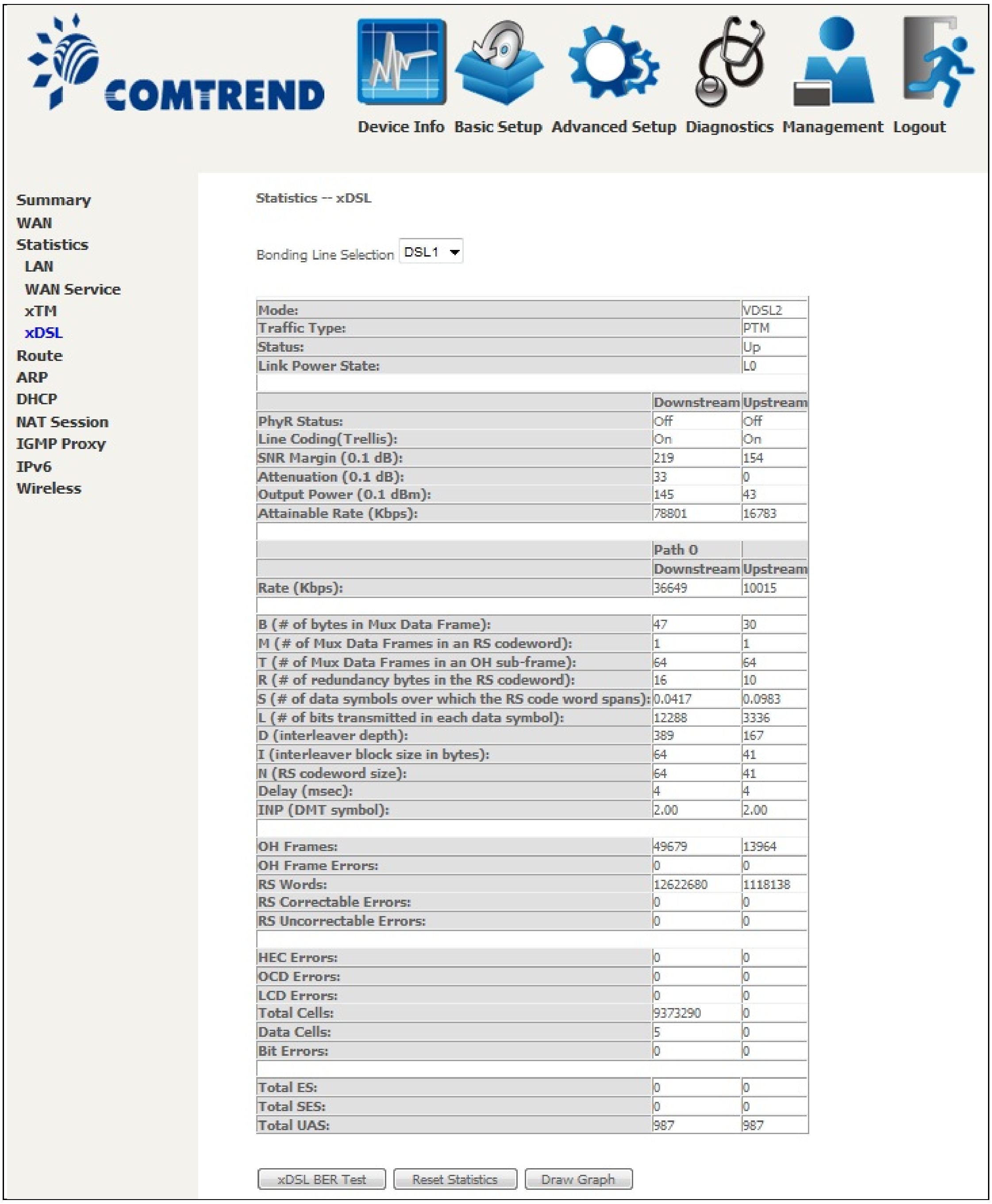
XTM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-1)
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

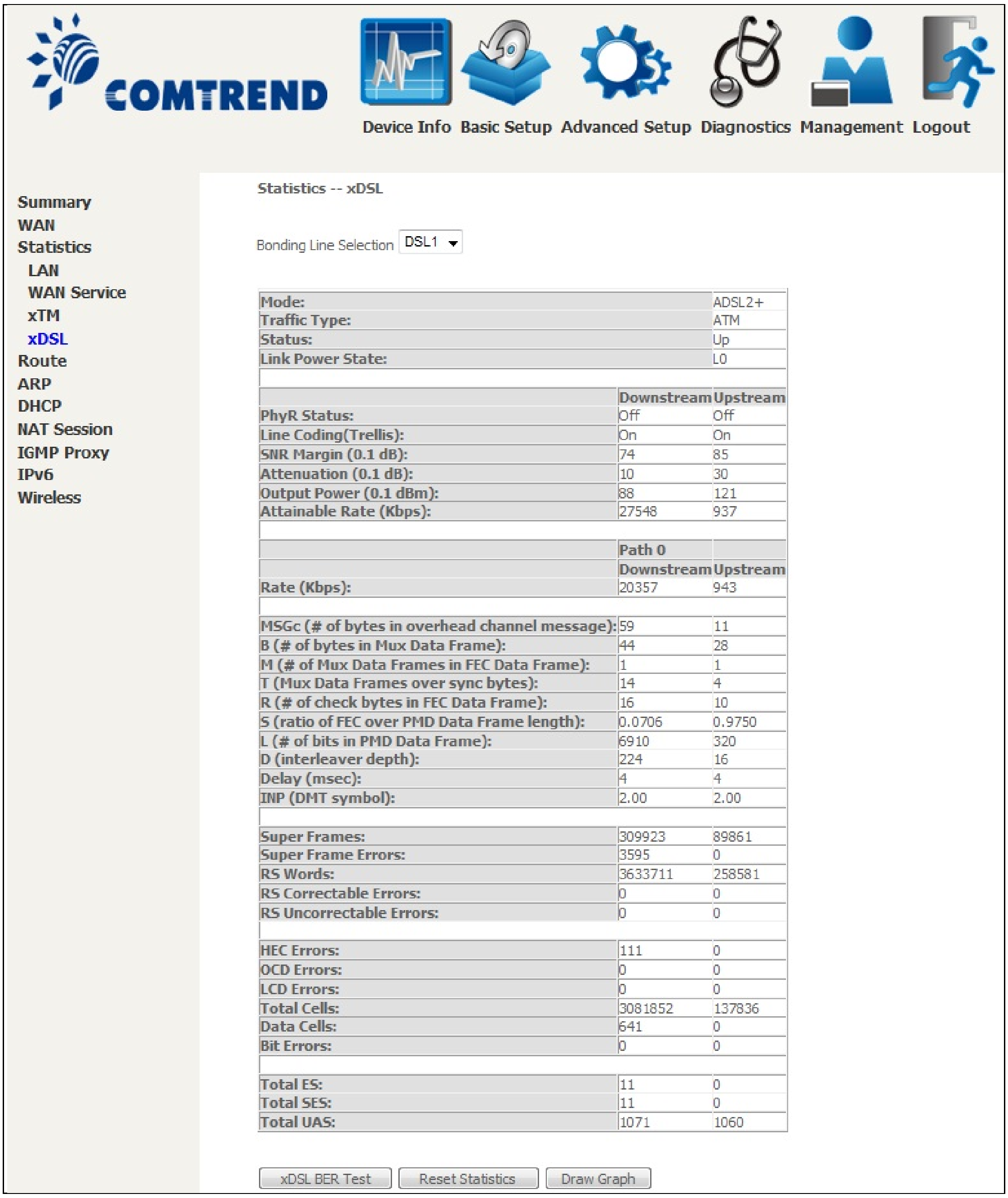


Statistics -- xDSL

Bonding Line Selection 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):	219	154
Attenuation (0.1 dB):	33	0
Output Power (0.1 dBm):	145	43
Attainable Rate (Kbps):	78801	16783
	Path 0	
	Downstream	Upstream
Rate (Kbps):	36649	10015
B (# of bytes in Mux Data Frame):	47	30
M (# of Mux Data Frames in an RS codeword):	1	1
T (# of Mux Data Frames in an OH sub-frame):	64	64
R (# of redundancy bytes in the RS codeword):	16	10
S (# of data symbols over which the RS code word spans):	0.0417	0.0983
L (# of bits transmitted in each data symbol):	12288	3336
D (interleaver depth):	389	167
I (interleaver block size in bytes):	64	41
N (RS codeword size):	64	41
Delay (msec):	4	4
INP (DMT symbol):	2.00	2.00
OH Frames:	49679	13964
OH Frame Errors:	0	0
RS Words:	12622680	1118138
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	9373290	0
Data Cells:	5	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	987	987

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):	74	85
Attenuation (0.1 dB):	10	30
Output Power (0.1 dBm):	88	121
Attainable Rate (Kbps):	27548	937
	Path 0	
	Downstream	Upstream
Rate (Kbps):	20357	943
MSGc (# of bytes in overhead channel message):	59	11
B (# of bytes in Mux Data Frame):	44	28
M (# of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	14	4
R (# of check bytes in FEC Data Frame):	16	10
S (ratio of FEC over PMD Data Frame length):	0.0706	0.9750
L (# of bits in PMD Data Frame):	6910	320
D (interleaver depth):	224	16
Delay (msec):	4	4
INP (DMT symbol):	2.00	2.00
Super Frames:	309923	89861
Super Frame Errors:	3595	0
RS Words:	3633711	258581
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	111	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	3081852	137836
Data Cells:	641	0
Bit Errors:	0	0
Total ES:	11	0
Total SES:	11	0
Total UAS:	1071	1060

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

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

Field	Description
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

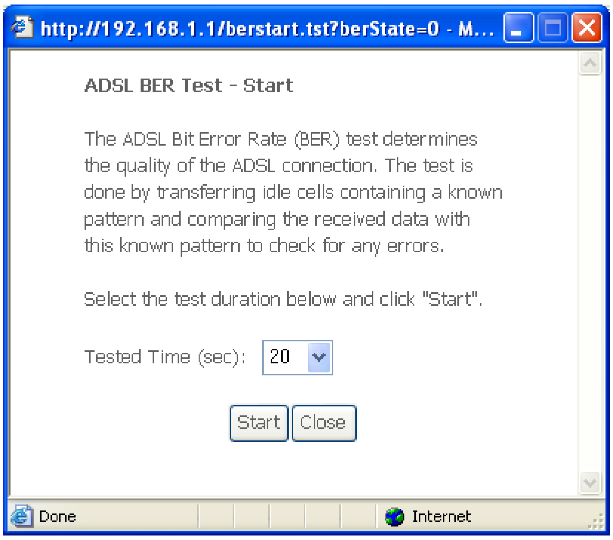
OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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.



http://192.168.1.1/berstart.tst?berState=0 - M...

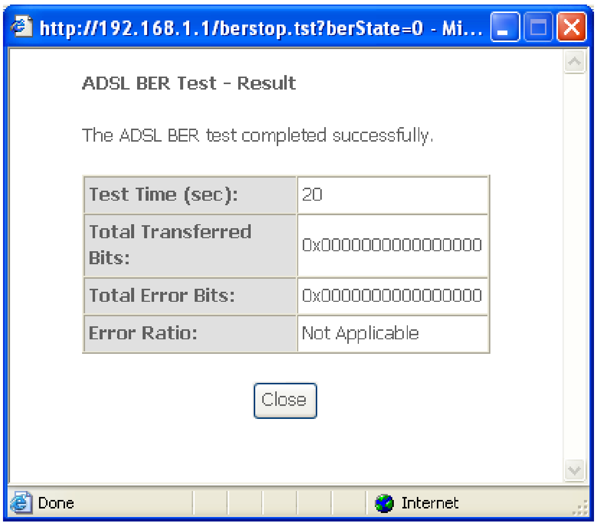
ADSL BER Test - Start

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.



http://192.168.1.1/berstop.tst?berState=0 - Mi...

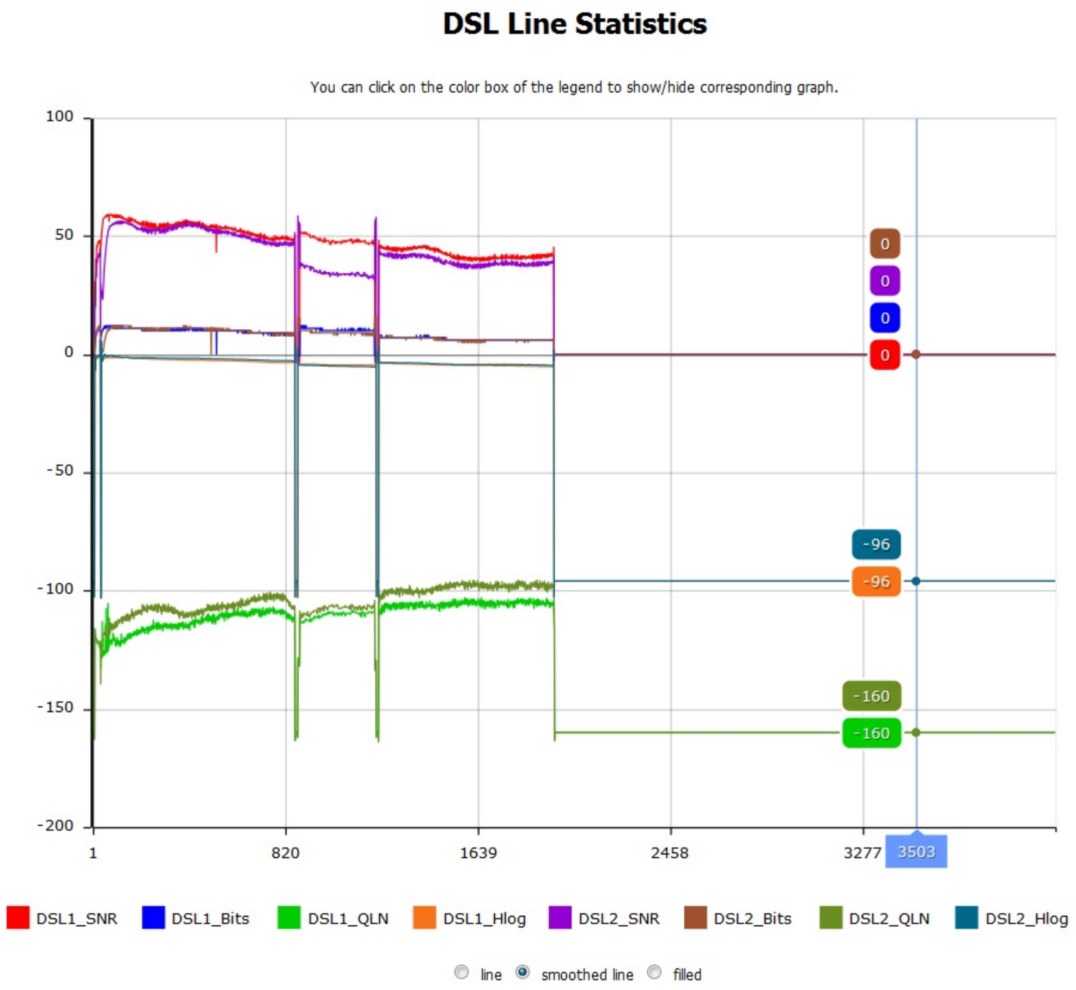
ADSL BER Test - Result

The ADSL BER test completed successfully.

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

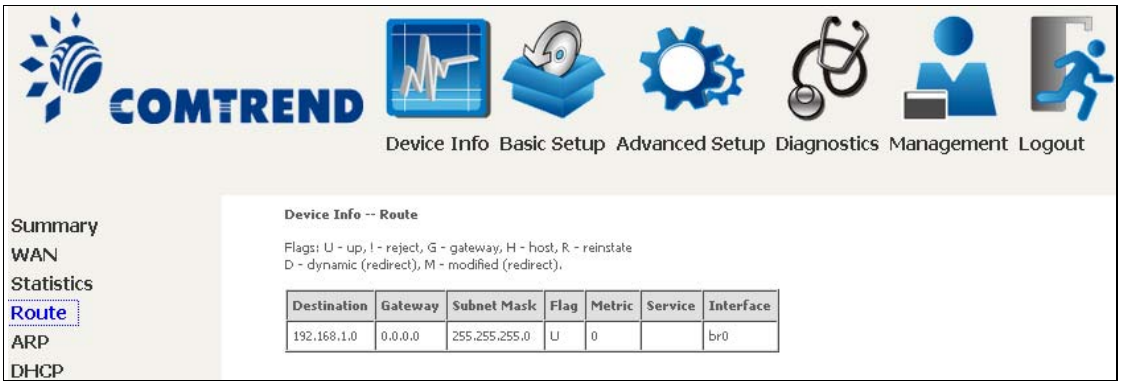
xDSL TONE GRAPH

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



4.3 Route

Choose **Route** to display the routes that the VR-3033 has found.



Device Info -- Route

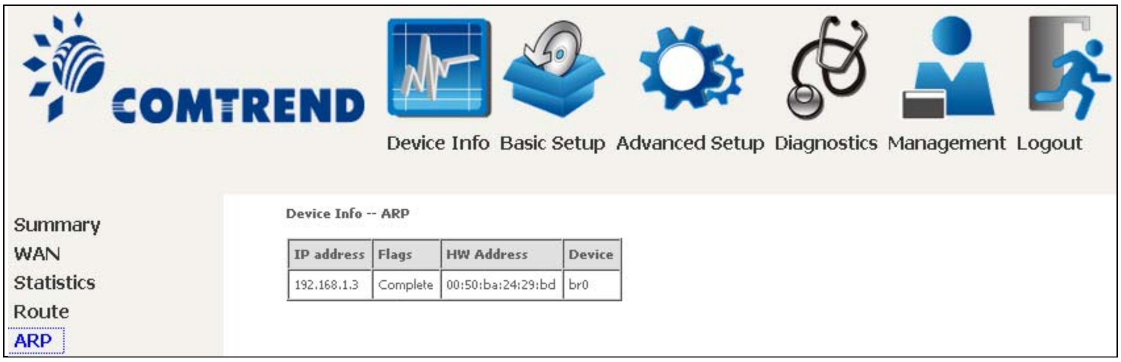
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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.



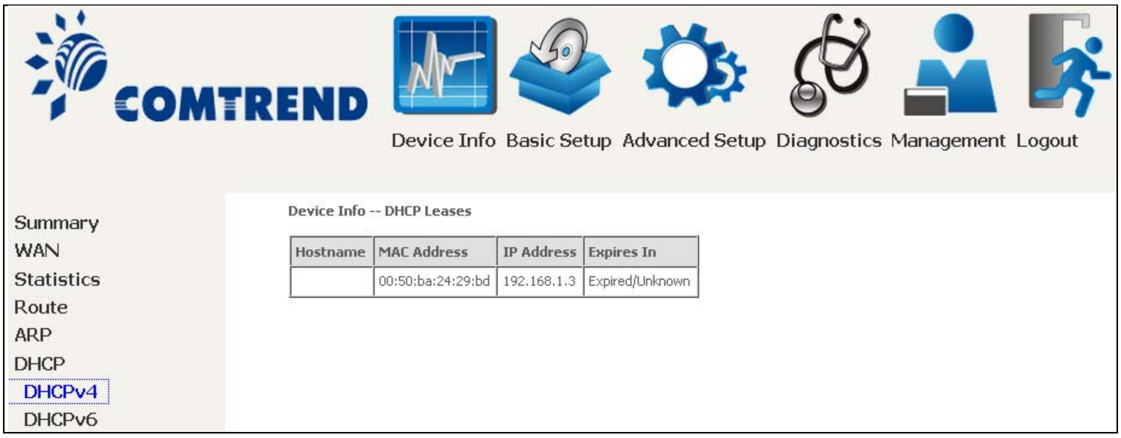
Device Info -- ARP

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

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

4.5 DHCP

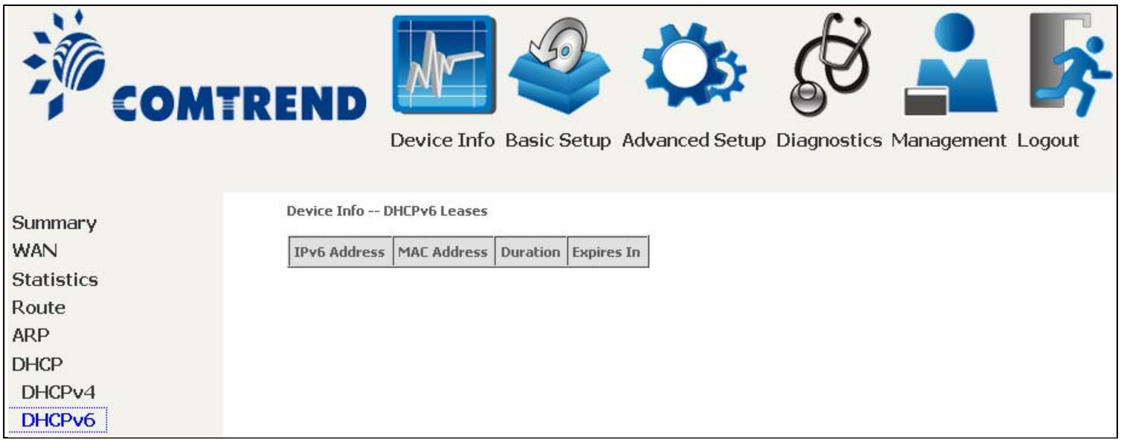
Click **DHCP** to display all DHCP Leases.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
	00:50:ba:24:29:bd	192.168.1.3	Expired/Unknown

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

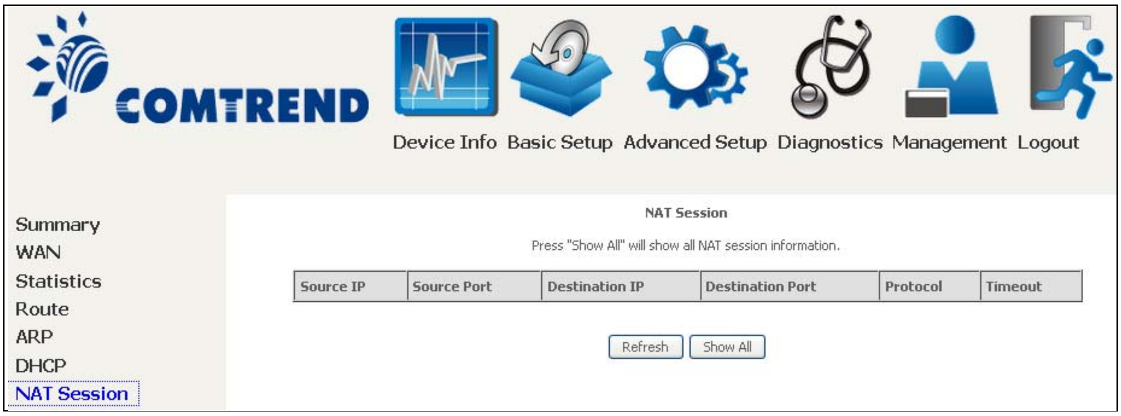


Device Info -- DHCPv6 Leases

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

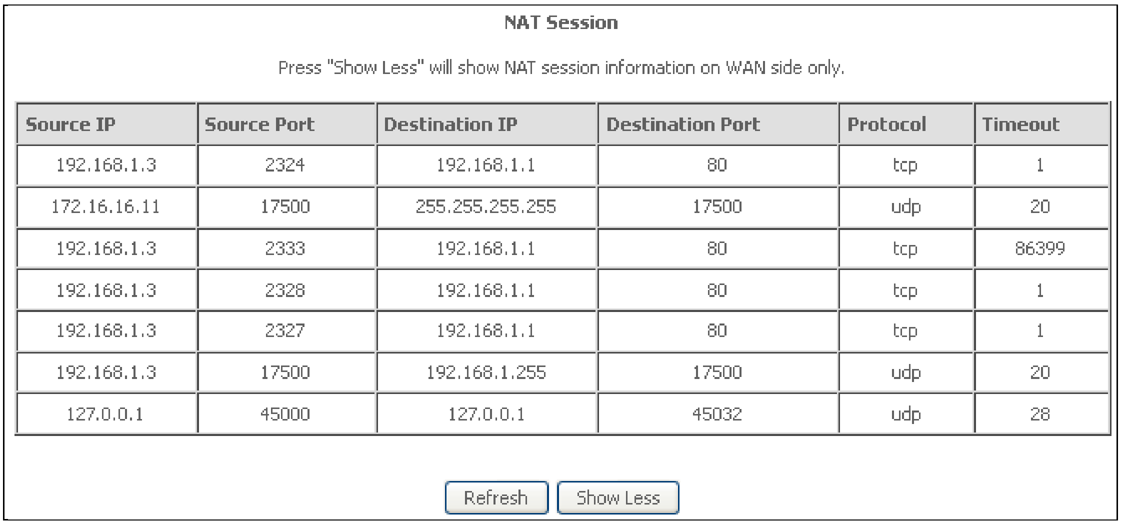


NAT Session

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.



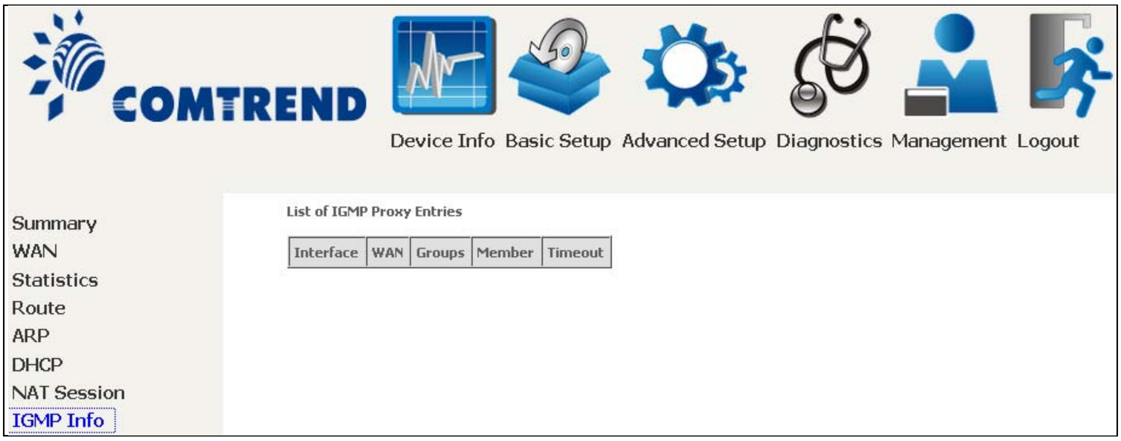
NAT Session

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	2324	192.168.1.1	80	tcp	1
172.16.16.11	17500	255.255.255.255	17500	udp	20
192.168.1.3	2333	192.168.1.1	80	tcp	86399
192.168.1.3	2328	192.168.1.1	80	tcp	1
192.168.1.3	2327	192.168.1.1	80	tcp	1
192.168.1.3	17500	192.168.1.255	17500	udp	20
127.0.0.1	45000	127.0.0.1	45032	udp	28

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

4.7 IGMP Info



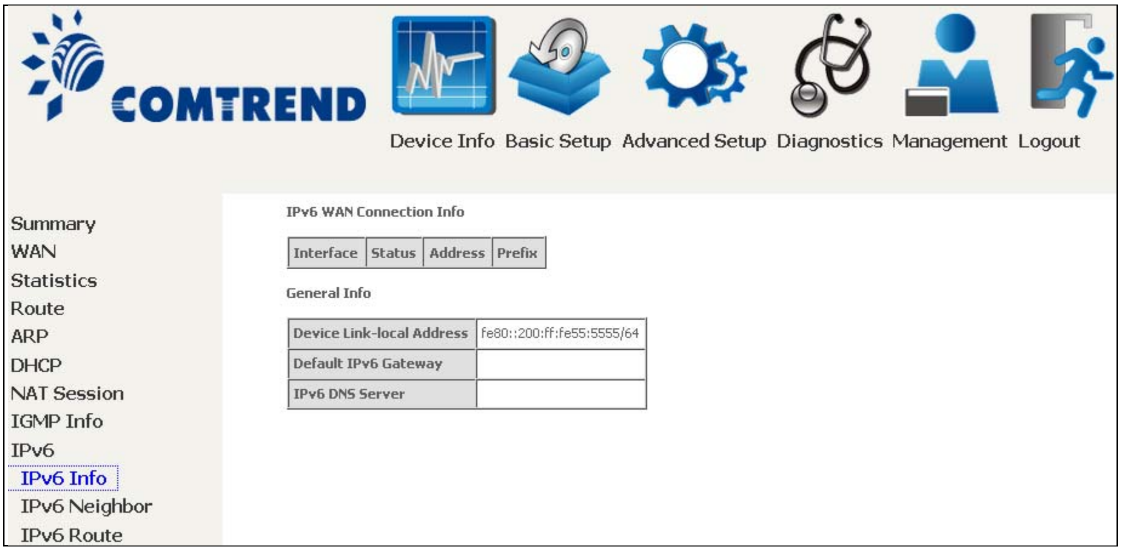
List of IGMP Proxy Entries

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

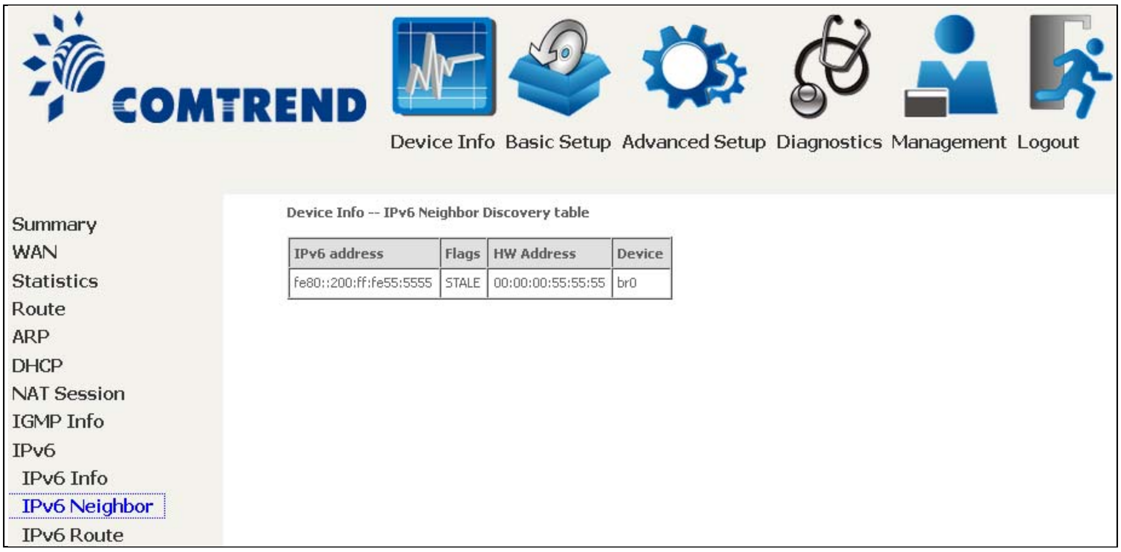
Interface	Status	Address	Prefix

General Info

Device Link-local Address	fe80::200:ff:fe55:5555/64
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

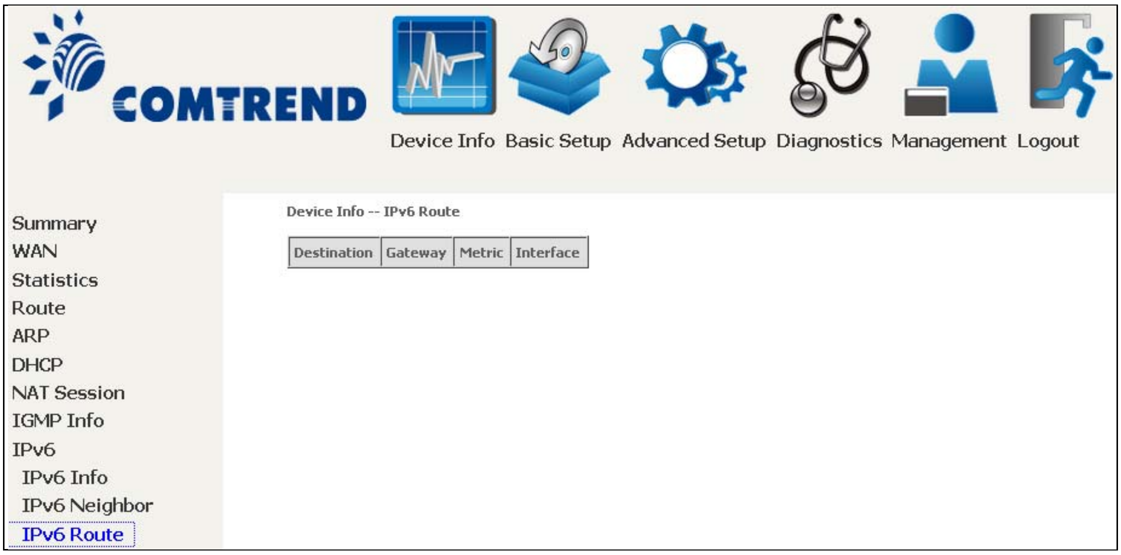


Device Info -- IPv6 Neighbor Discovery table

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

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

4.8.3 IPv6 Route



Device Info -- IPv6 Route

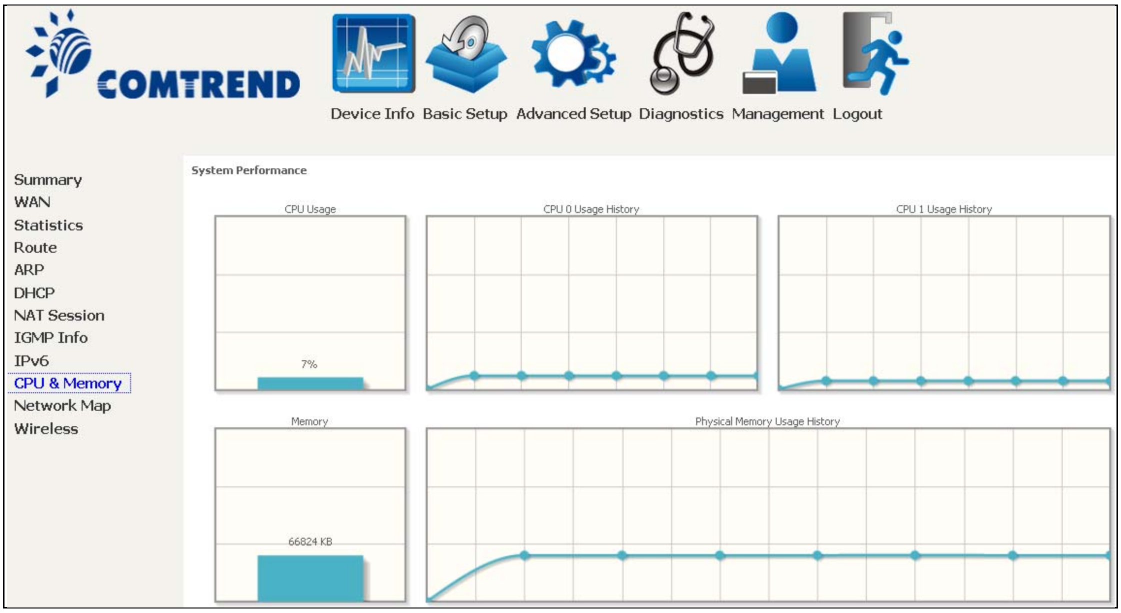
Destination	Gateway	Metric	Interface

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 CPU & Memory

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

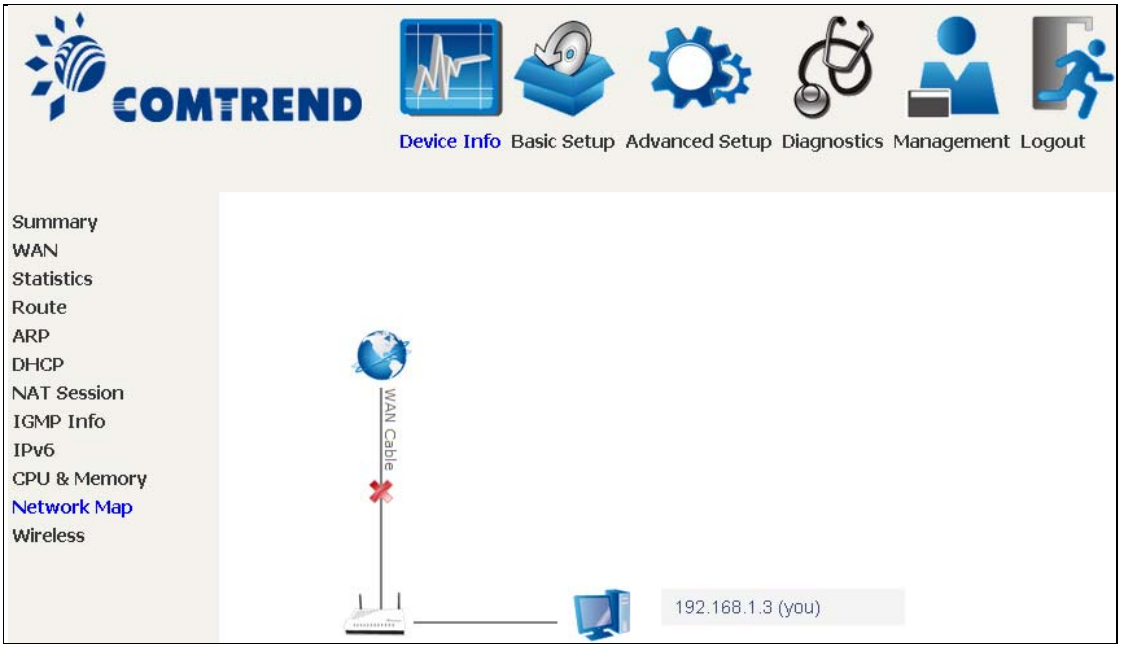
Note: This graph is unavailable for Internet Explorer users.



4.10 Network Map

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

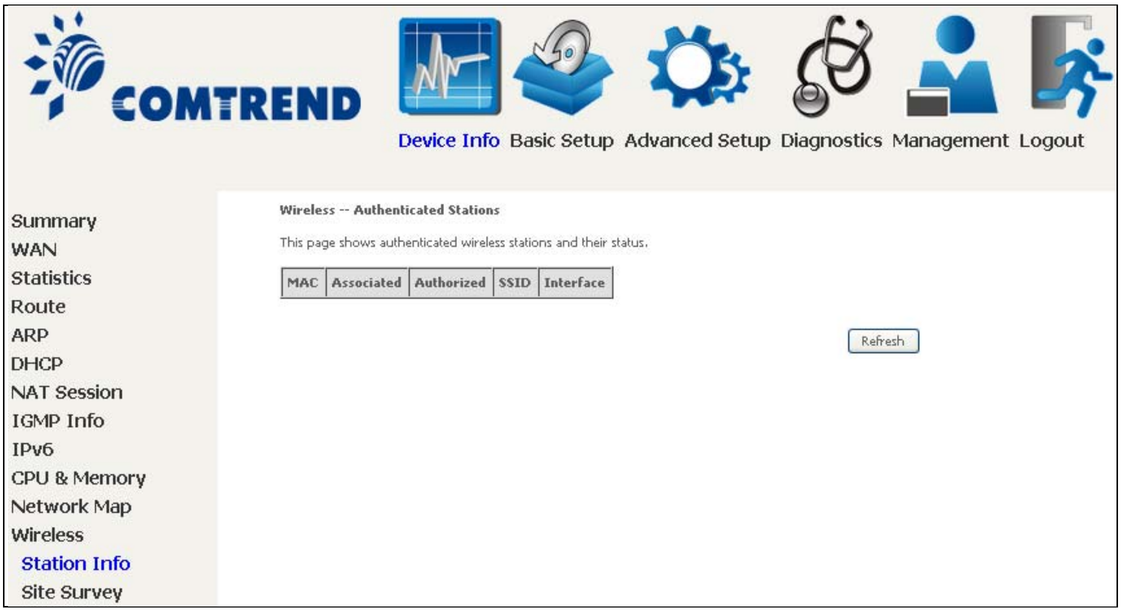
Note: This graph is unavailable for Internet Explorer users.



4.11 Wireless

4.11.1 Station Info

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



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

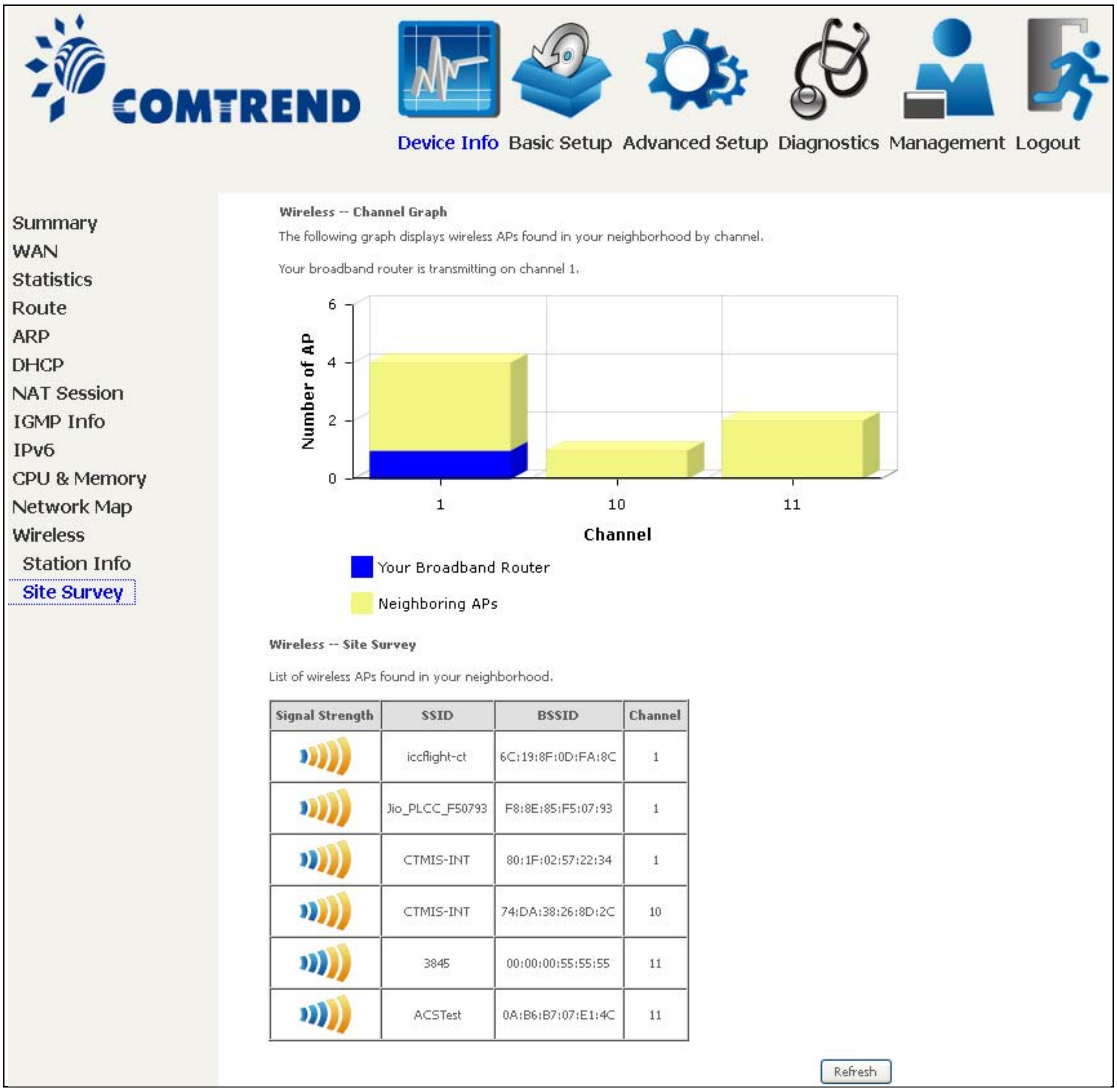
MAC	Associated	Authorized	SSID	Interface

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.

4.11.2 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 1.

Wireless -- Site Survey

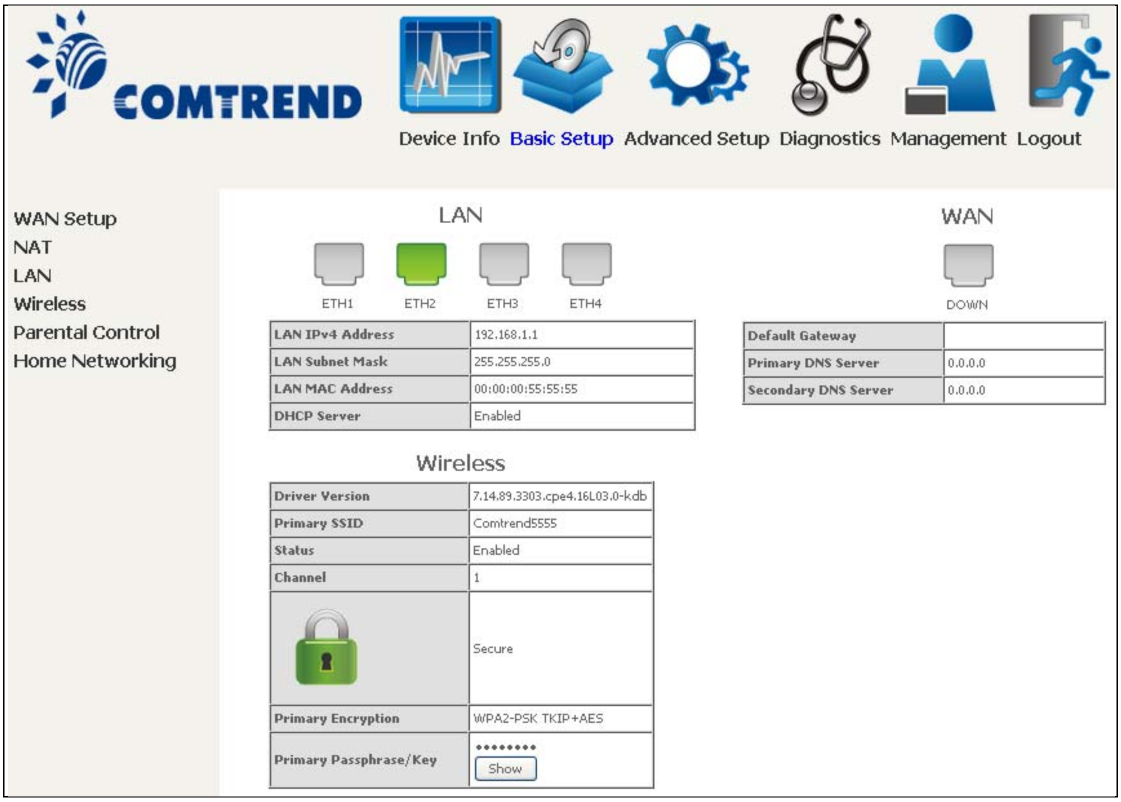
List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
📶	iccflight-ct	6C:19:8F:0D:FA:8C	1
📶	Jio_PLCC_F50793	F8:8E:85:F5:07:93	1
📶	CTMIS-INT	80:1F:02:57:22:34	1
📶	CTMIS-INT	74:DA:38:26:8D:2C	10
📶	3845	00:00:00:55:55:55	11
📶	ACSTest	0A:B6:B7:07:E1:4C	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.



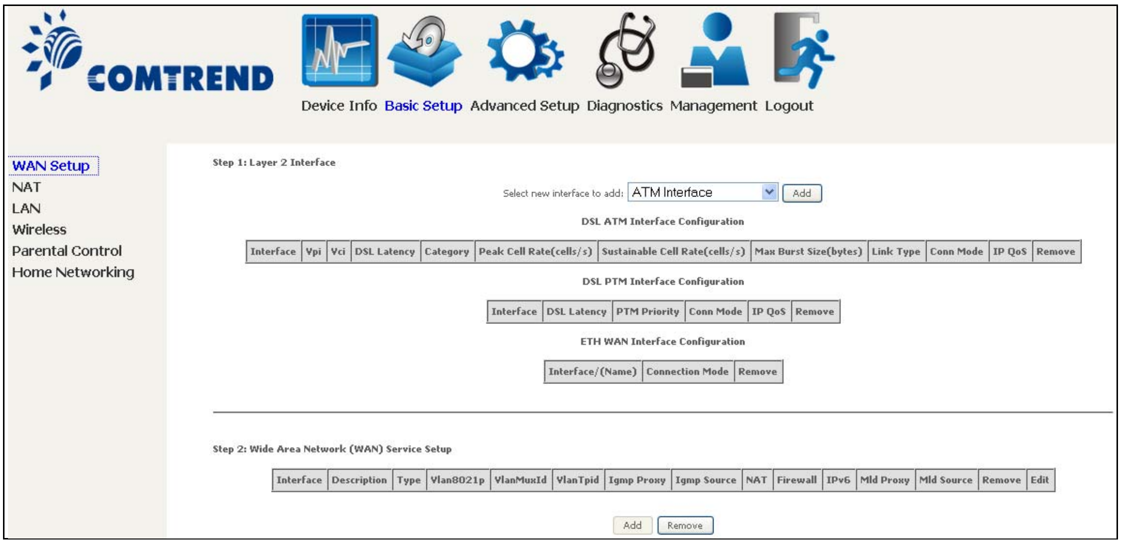
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:00:00:55:55:55
DHCP Server	Enabled

Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Driver Version	7.14.89.3303.cpe4.16L03.0-kdb
Primary SSID	Comtrend5555
Status	Enabled
Channel	1
🔒	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	•••••••• Show

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 [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]

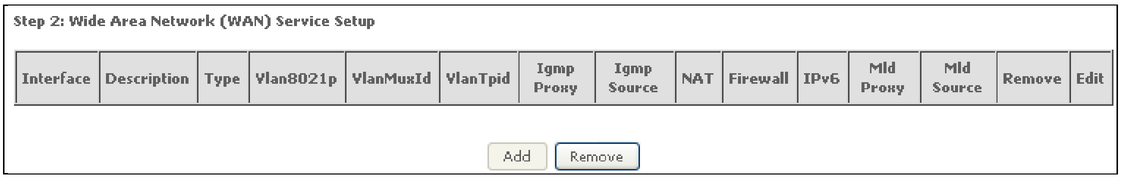
Click **Add** to create a new Layer 2 Interface (see Appendix F - Connection Setup).

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.

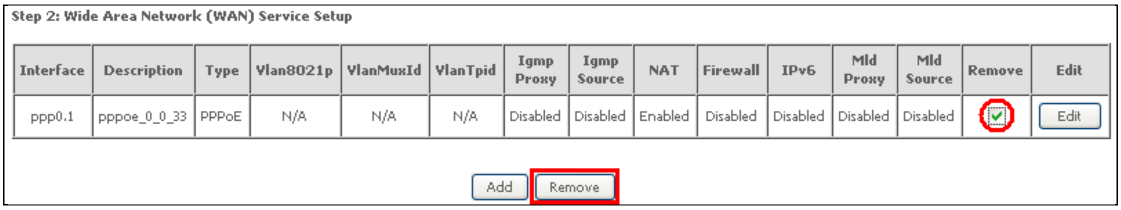


Step 2: Wide Area Network (WAN) Service Setup

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

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_33	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	☑	Edit

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

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

NOTE: 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.

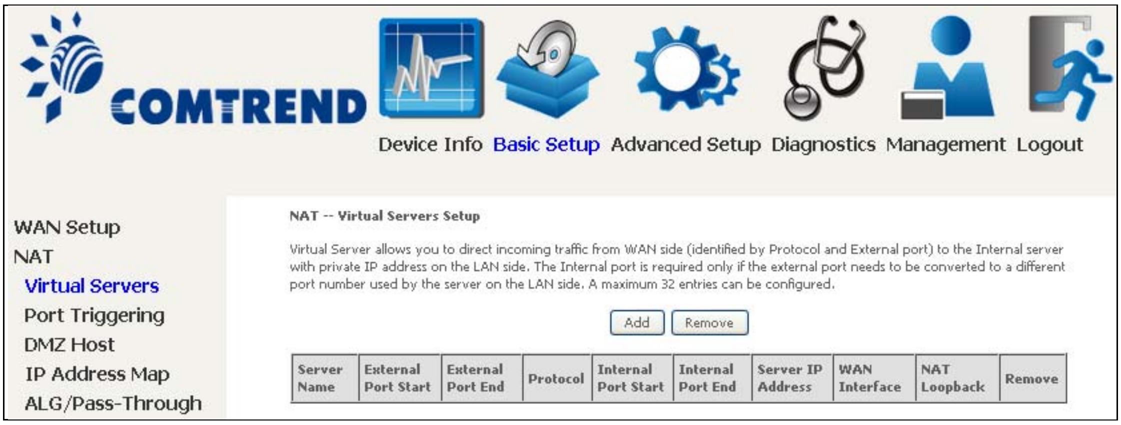
NOTE: Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist.

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.

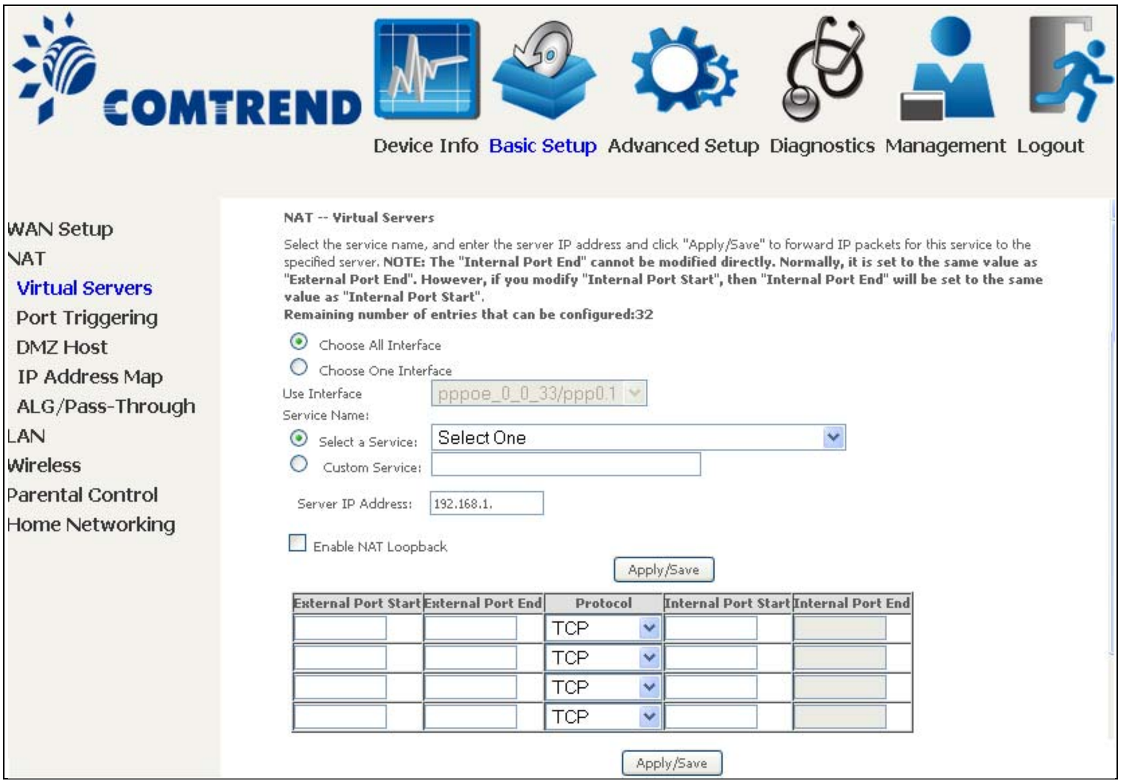


NAT -- Virtual Servers Setup

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.



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_33/ppp0.1
Service Name:
● Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.1.

□ Enable NAT Loopback

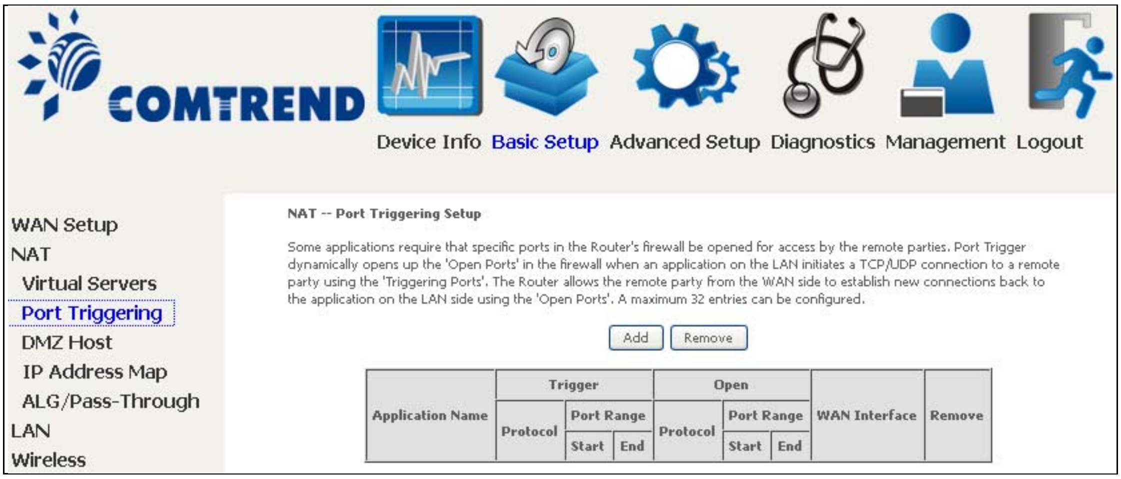
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		

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 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.



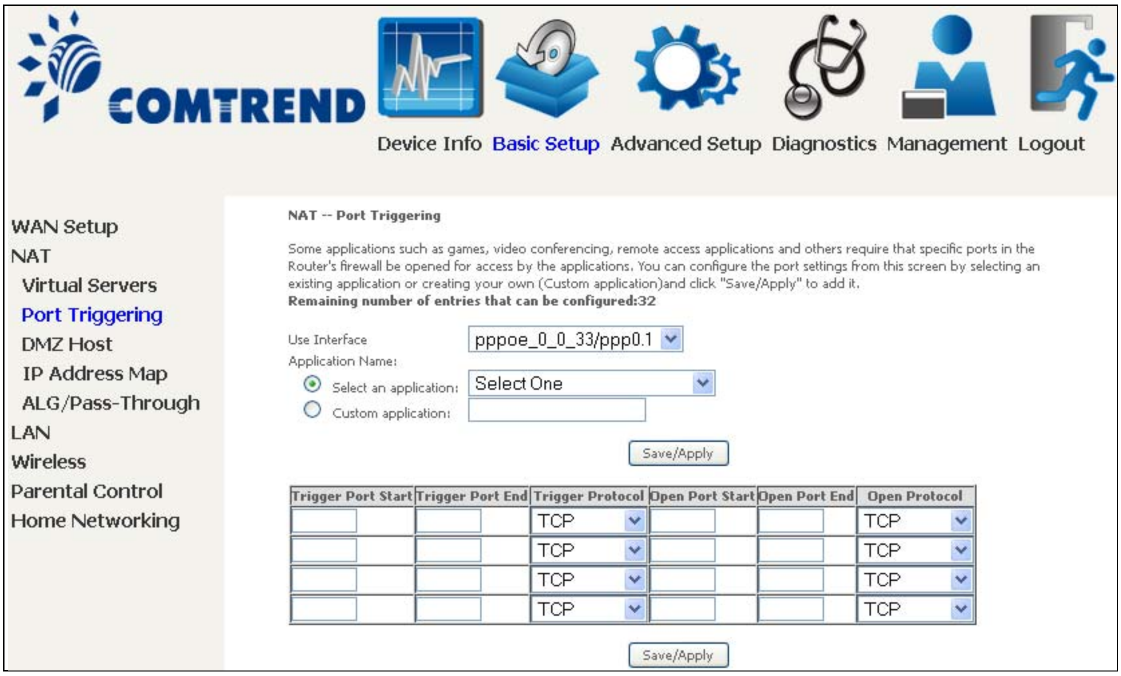
NAT -- Port Triggering Setup

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.

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_33/ppp0.1
Application Name:
● Select an application: Select One
○ Custom application:

Save/Apply

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

Save/Apply

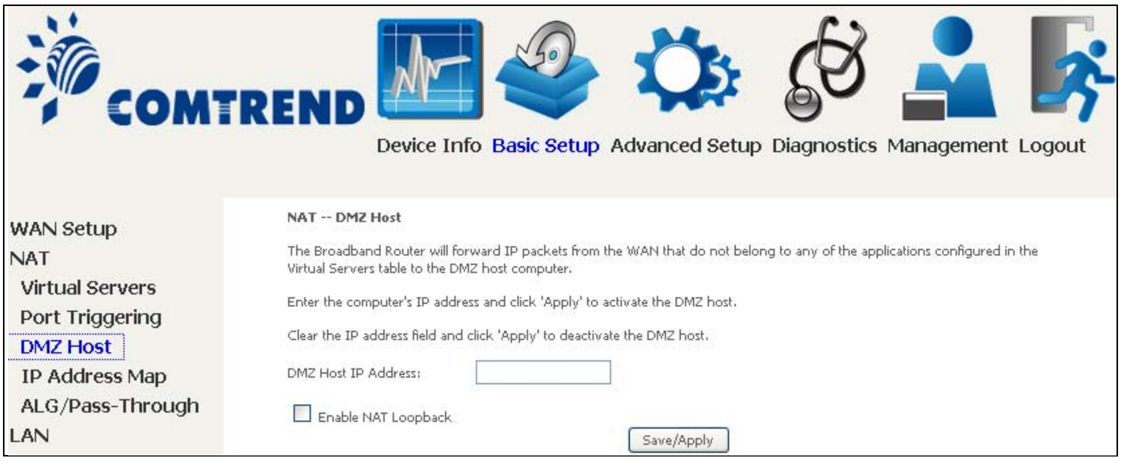
Click Save/Apply to save and apply the settings.

Consult the table below for field and header descriptions.

Field / Header	**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.



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

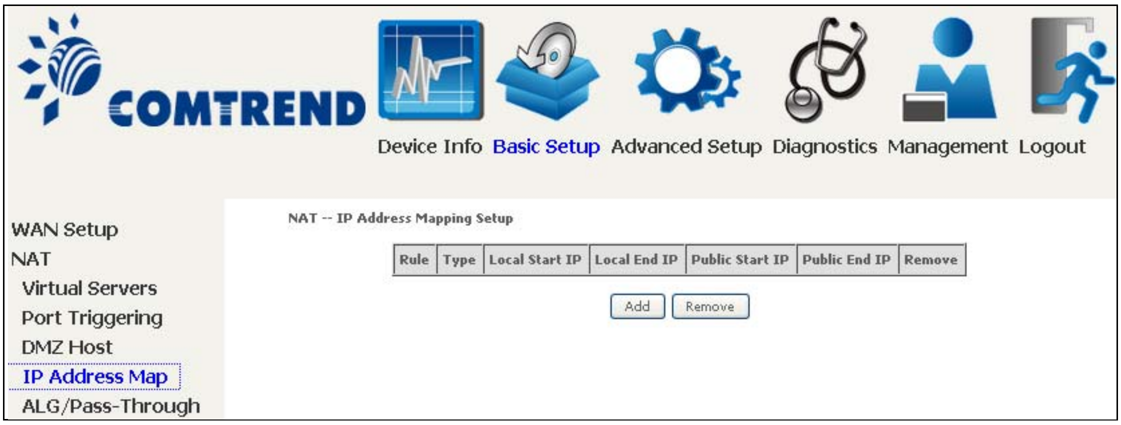
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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).

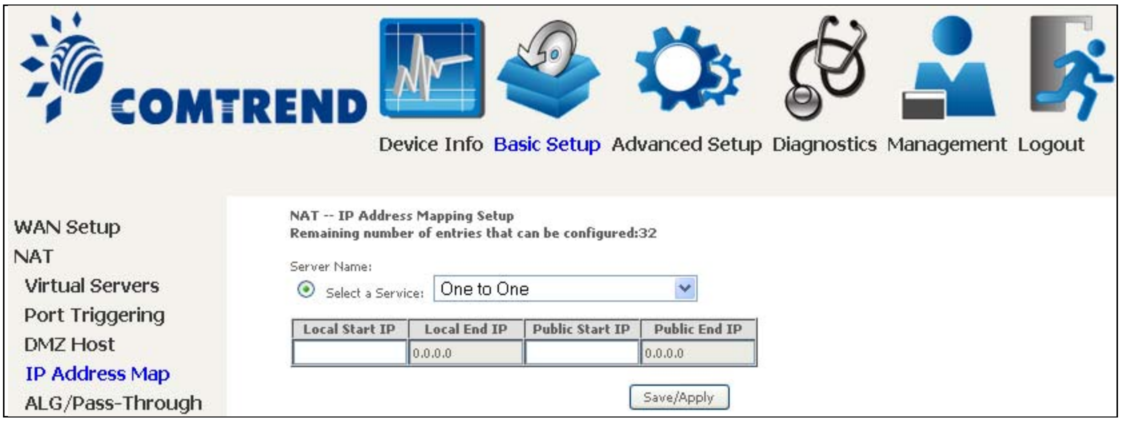


NAT -- IP Address Mapping Setup

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

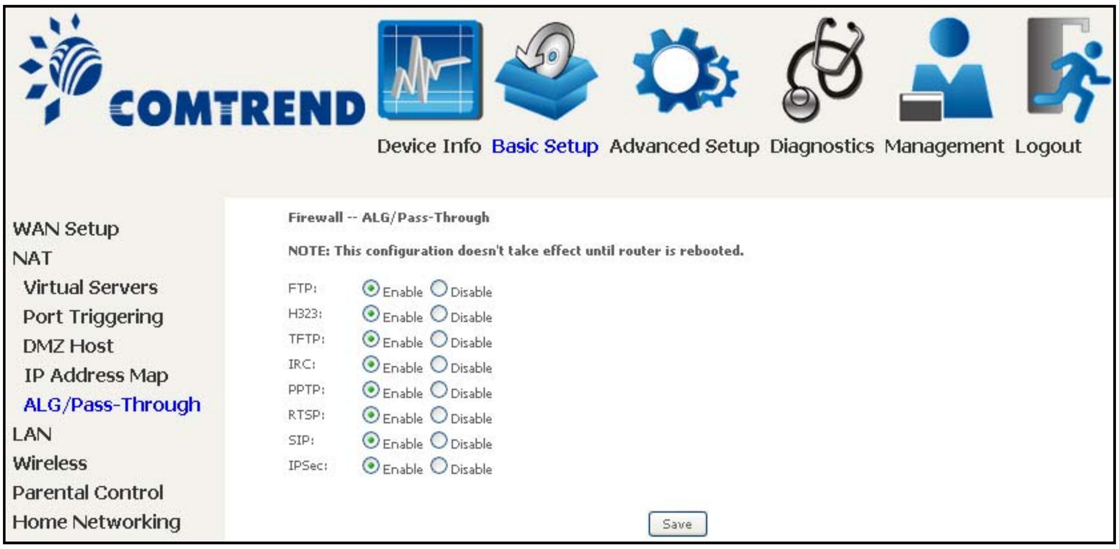
Many to one: mapping a range of local IP to a specific public IP

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 ALG/Pass-Through

Support ALG Pass-through for the listed protocols.



Firewall -- ALG/Pass-Through

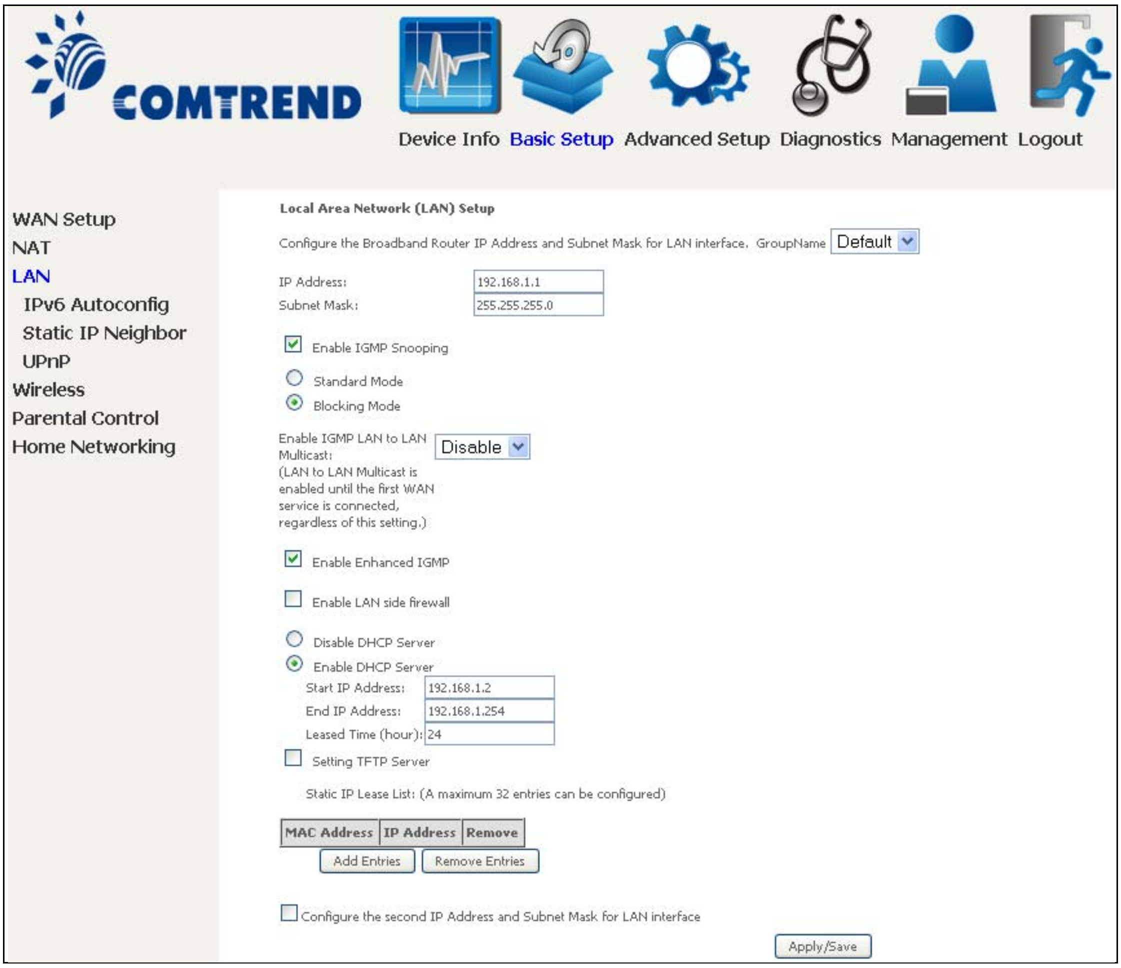
NOTE: This configuration doesn't take effect until router is rebooted.

FTP:	● Enable	○ Disable
H323:	● Enable	○ Disable
TFTP:	● Enable	○ Disable
IRC:	● Enable	○ Disable
PPTP:	● Enable	○ Disable
RTSP:	● Enable	○ Disable
SIP:	● Enable	○ Disable
IPSec:	● Enable	○ Disable

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

5.3 LAN

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



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode
● Blocking Mode

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

☑ Enable 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

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

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

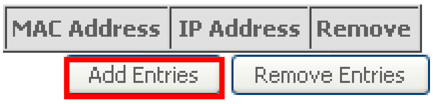
Enable Enhanced IGMP: Enable by ticking the checkbox ☑. IGMP packets between LAN ports will be blocked.

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.

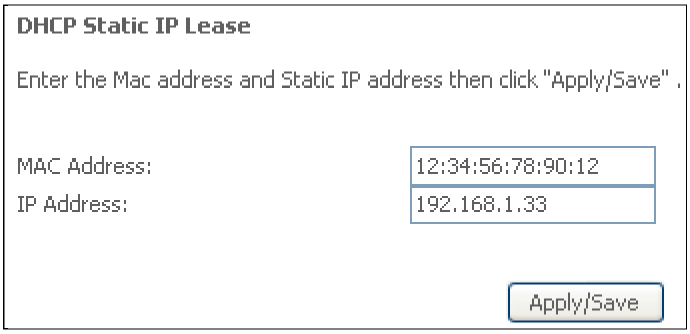
Setting TFTP Server: Enable by ticking the checkbox ☑. Then, input the TFTP server address or an IP address.

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



MAC Address	IP Address	Remove

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

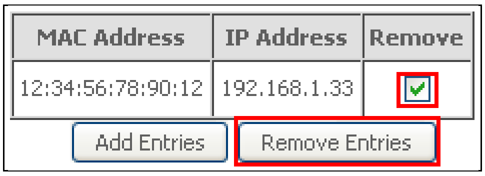


DHCP Static IP Lease

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

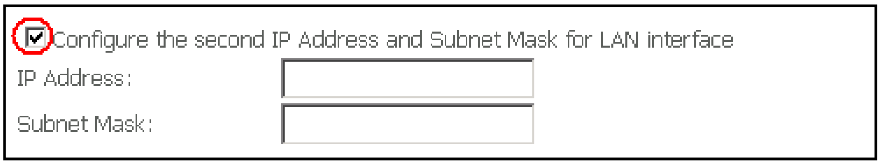
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



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

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

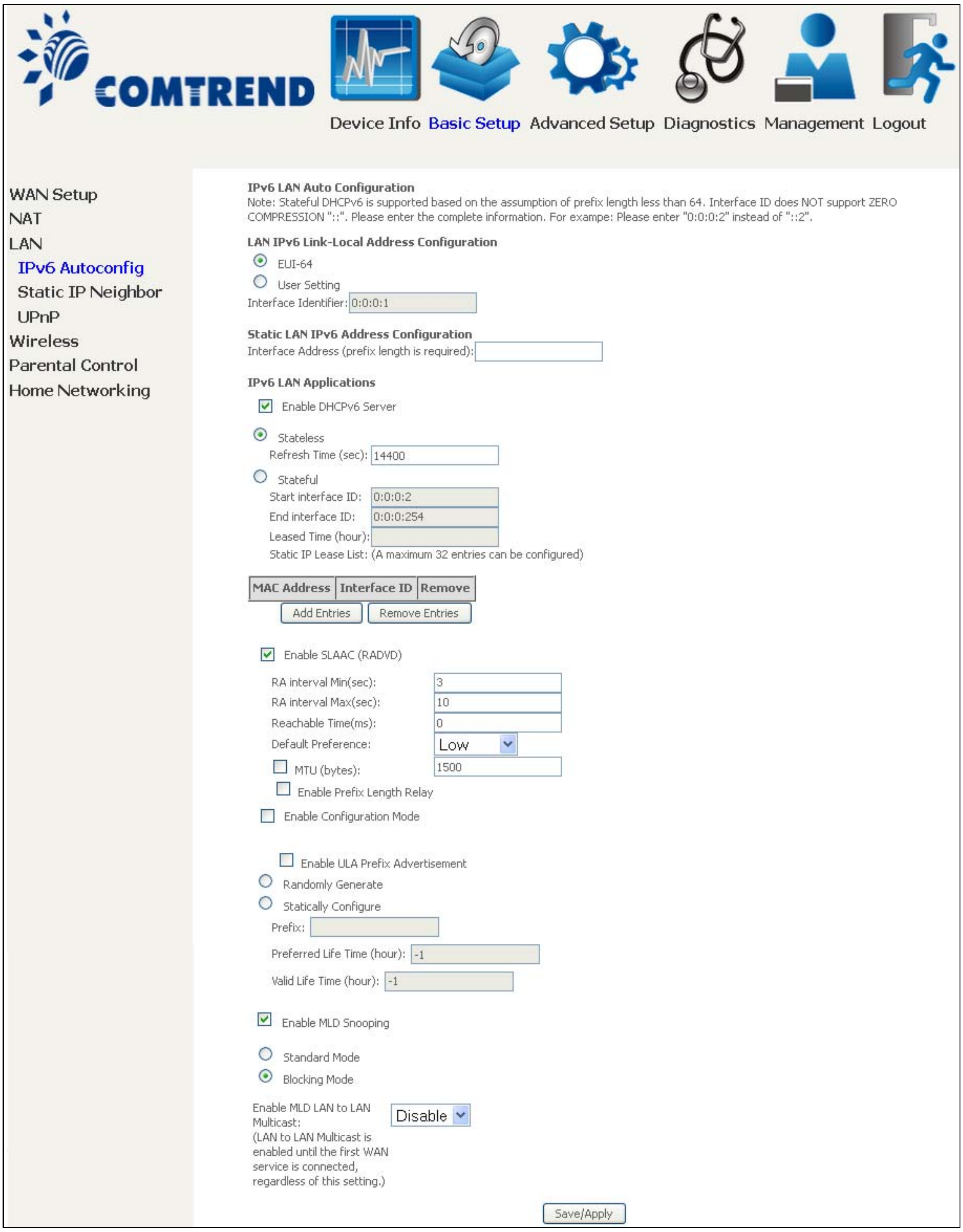
IP Address:

Subnet Mask:

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

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

☑ Enable SLAAC (RADVD)

RA interval Min(sec): 3

RA interval Max(sec): 10

Reachable Time(ms): 0

Default Preference: Low

□ MTU (bytes): 1500

□ Enable Prefix Length Relay

□ Enable Configuration Mode

□ Enable ULA Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Prefix:

Preferred Life Time (hour): -1

Valid Life Time (hour): -1

☑ Enable MLD Snooping

○ Standard Mode

● Blocking Mode

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

Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

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

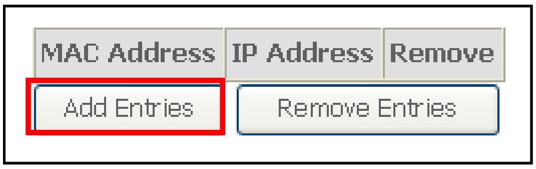
Static LAN IPv6 Address Configuration

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

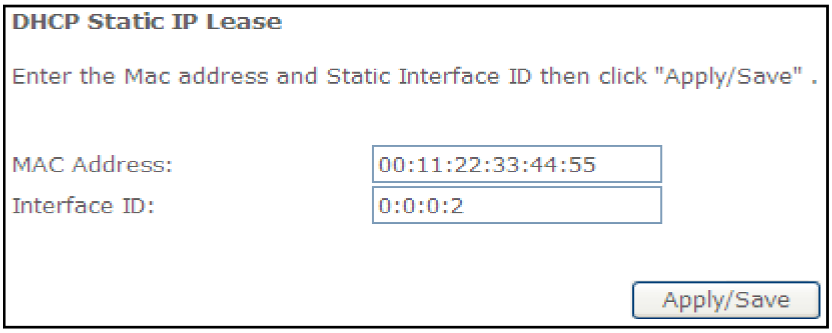
IPv6 LAN Applications

Heading	Description
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.



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



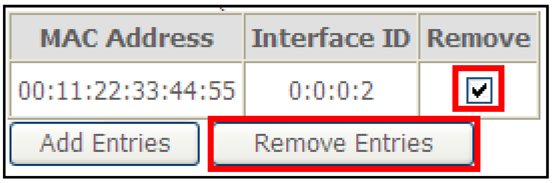
DHCP Static IP Lease

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

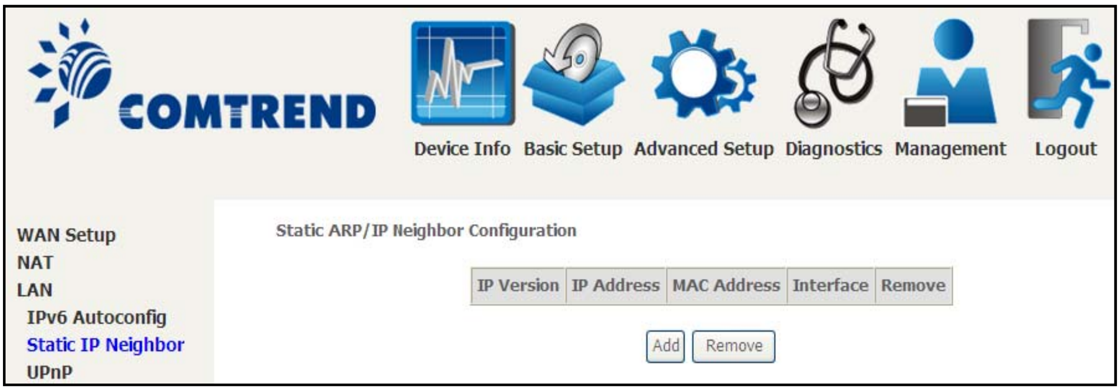
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



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
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

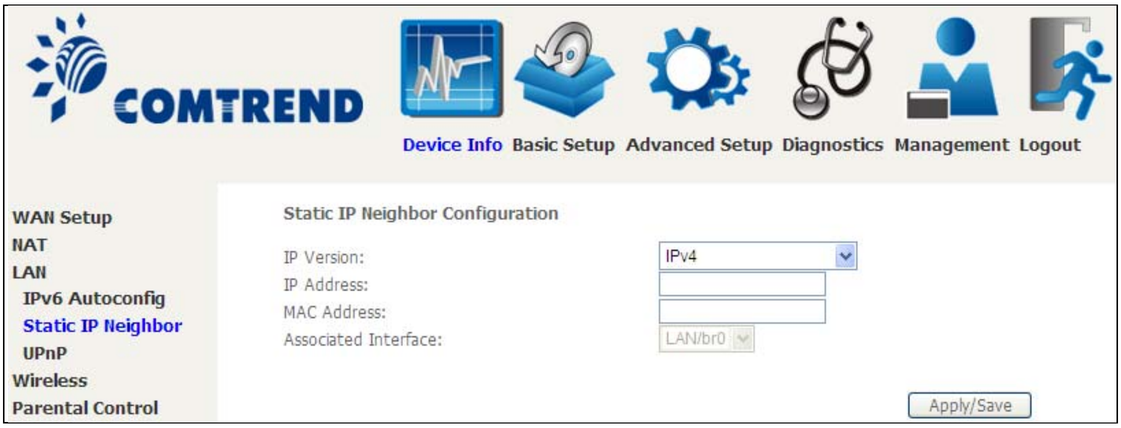
5.3.2 Static IP Neighbor



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:

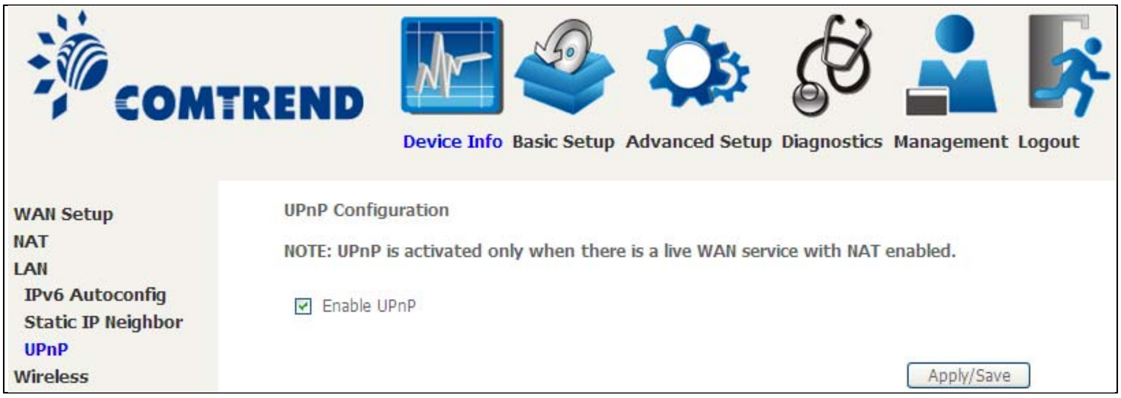
Associated Interface: LAN/br0

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

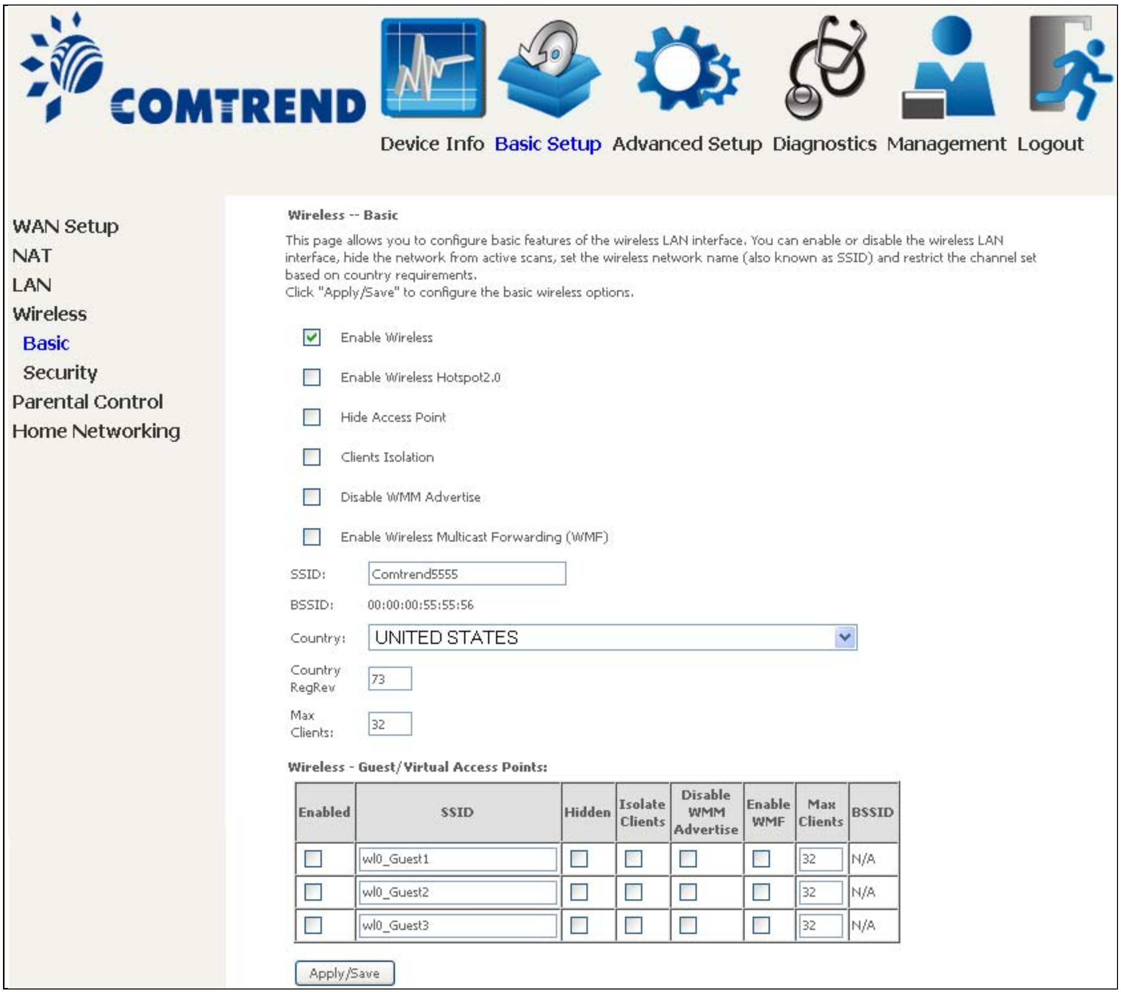
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ 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

□ Enable Wireless Hotspot2.0

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: Comtrend5555

BSSID: 00:00:00:55:55:56

Country: UNITED STATES

Country RegRev: 73

Max Clients: 32

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	wl0_Guest1	□	□	□	□	32	N/A
□	wl0_Guest2	□	□	□	□	32	N/A
□	wl0_Guest3	□	□	□	□	32	N/A

Apply/Save

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

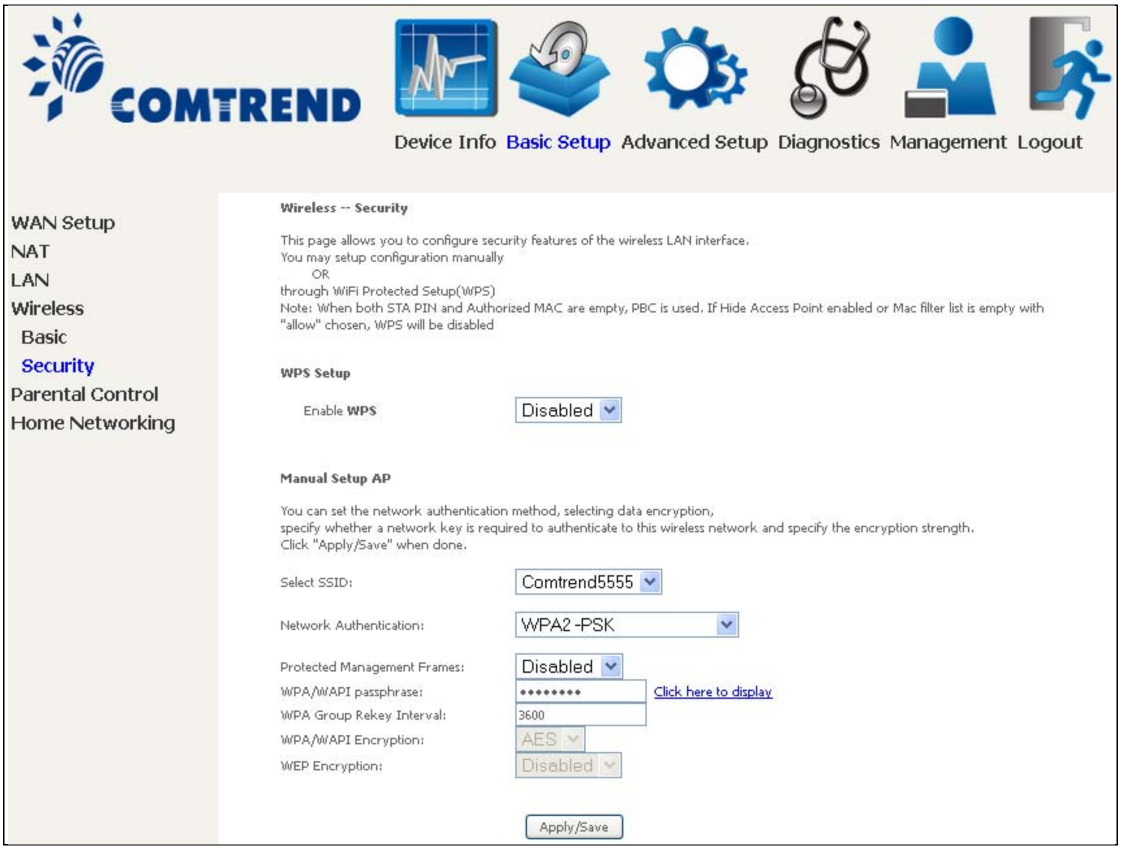
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Enable Wireless Hotspot2.0	Enable Wireless Hotspot 2.0 (Wi-Fi Certified Passpoint) on the wireless interface.

Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **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.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Country RegRev	Wireless country code for transmit power limit.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	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.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

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

Select SSID:	Comtrend5555
Network Authentication:	WPA2 -PSK
Protected Management Frames:	Disabled
WPA/WAPI passphrase:	•••••••• Click here to display
WPA Group Rekey Interval:	3600
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

Please see 6.11.3 for WPS setup instructions.

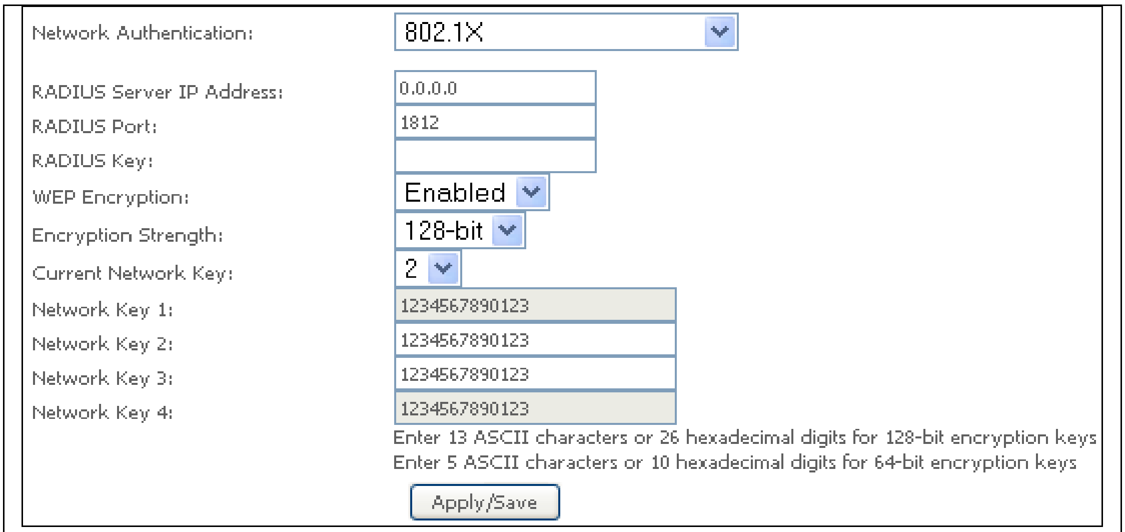
Click **Apply/Save** to implement new configuration settings.

WIRELESS SECURITY

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

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

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1: 1234567890123

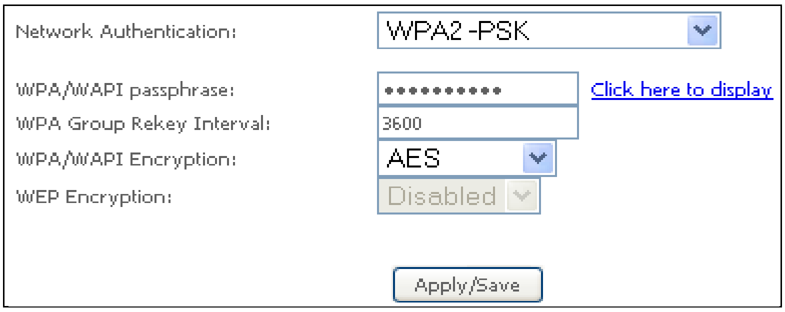
Network Key 2: 1234567890123

Network Key 3: 1234567890123

Network Key 4: 1234567890123

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

The settings for WPA2-PSK authentication are shown next.



Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ●●●●●●●●●●●

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: 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 6.11 for MAC Filter, Wireless Bridge and Advanced Wireless features.

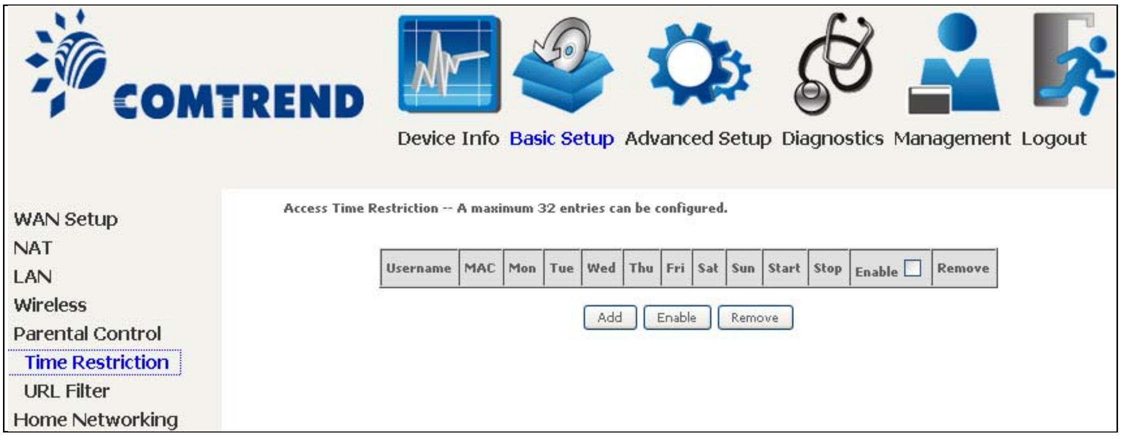
5.5 Parental Control

This selection provides WAN access control functionality.

5.5.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.5 Internet Time, so that the scheduled times match your local time.

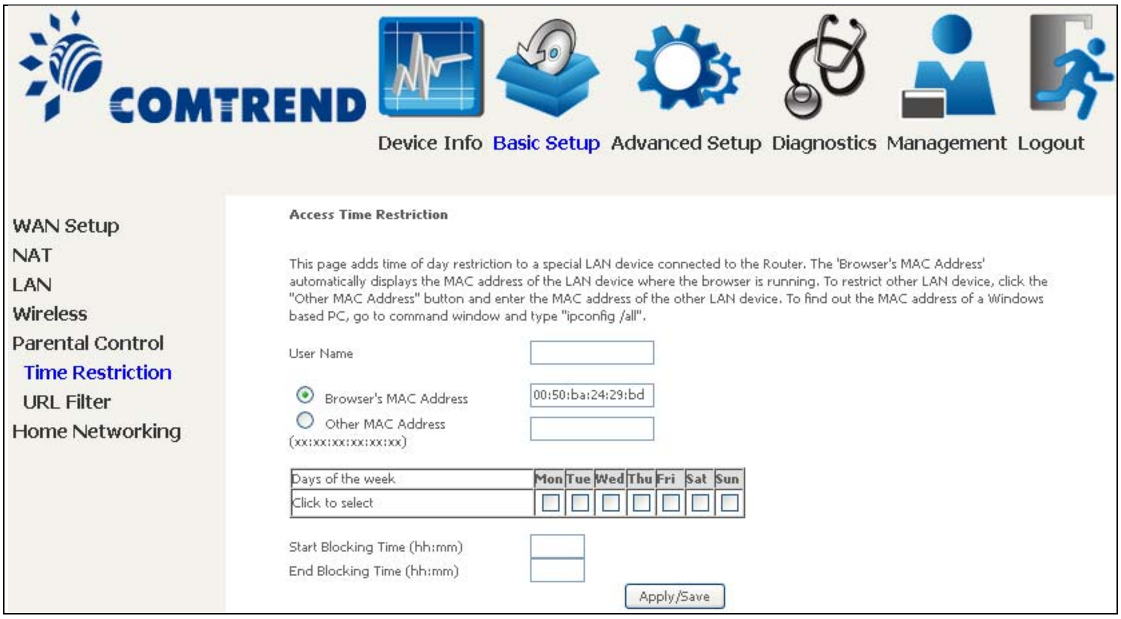
Clicking on the checkbox in the Enable field allows the user to select all / none entries for Enabling/Disabling.



Access Time Restriction -- A maximum 32 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Enable □	Remove

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



Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

● Browser's MAC Address 00:50:ba:24:29:bd

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

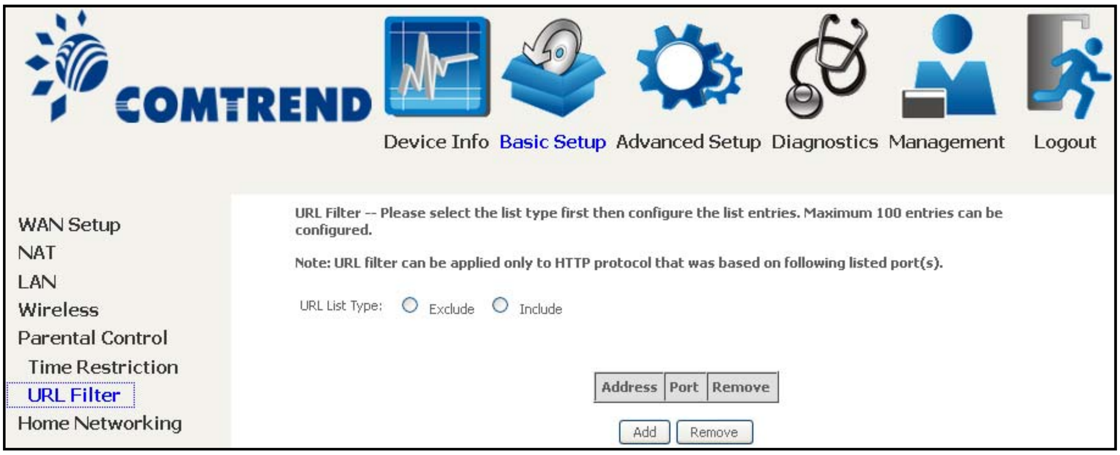
End Blocking Time (hh:mm)

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

User Name: A user-defined label for this restriction.
Browser's MAC Address: MAC address of the PC running the browser.
Other MAC Address: MAC address of another LAN device.
Days of the Week: The days the restrictions apply.
Start Blocking Time: The time the restrictions start.
End Blocking Time: The time the restrictions end.

5.5.2 URL Filter

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



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

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

URL List Type: ○ Exclude ○ Include

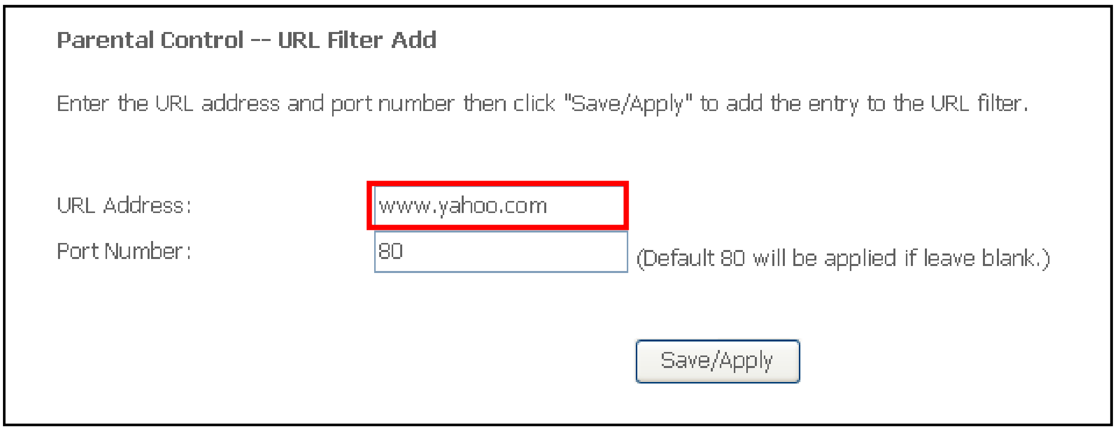
Address	Port	Remove

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.



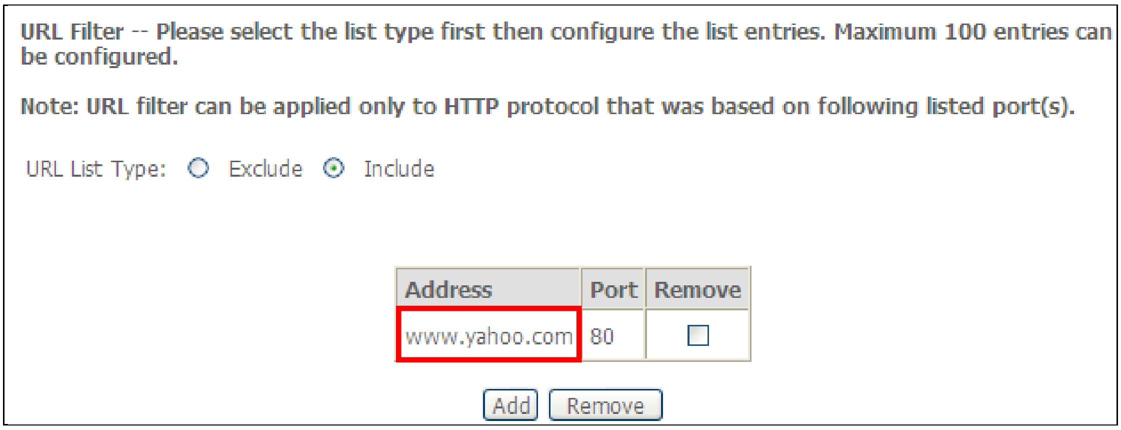
Parental Control -- URL Filter Add

Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.

URL Address: www.yahoo.com

Port Number: 80 (Default 80 will be applied if leave blank.)

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



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

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

URL List Type: ○ Exclude ● Include

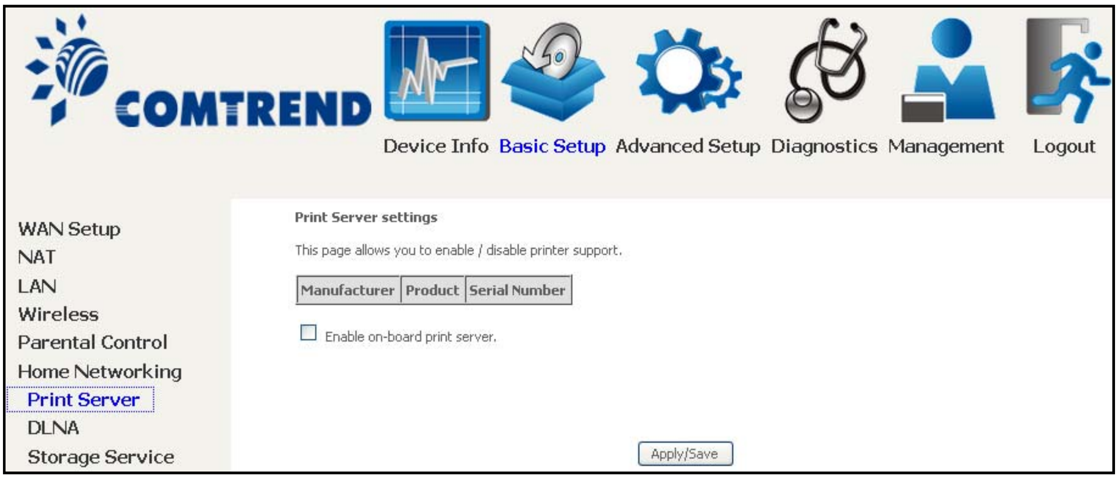
Address	Port	Remove
www.yahoo.com	80	□

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

5.6 Home networking

5.6.1 Print Server

This page allows you to enable or disable printer support.



Print Server settings

This page allows you to enable / disable printer support.

Manufacturer	Product	Serial Number

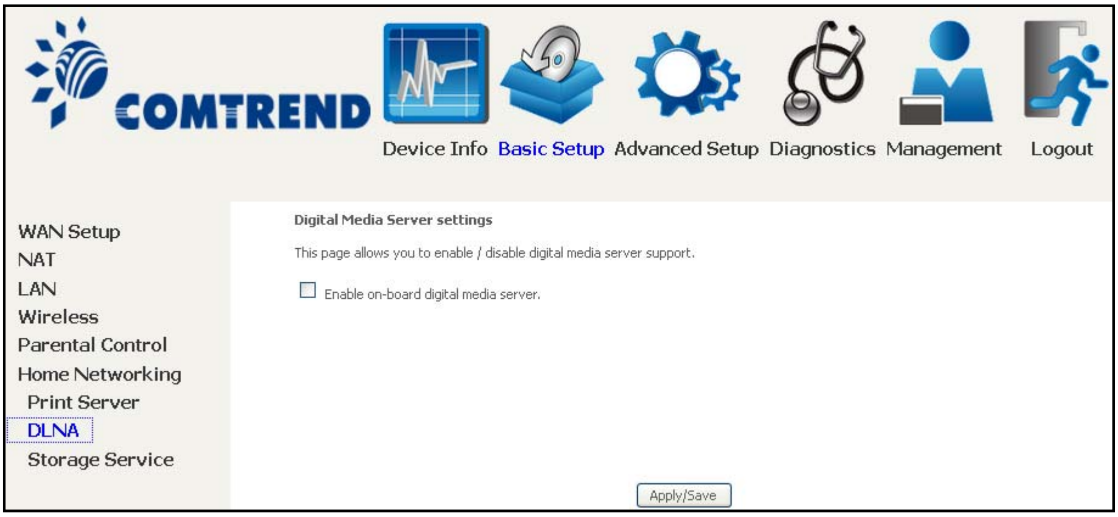
□ Enable on-board print server.

Please reference **Appendix E** to see the procedure for enabling the Printer Server.

5.6.2 DLNA

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

Insert USB drive to the USB host port on the back of router. Modify media library path to the corresponding path of the USB drive and click Apply/Save to enable the DLNA media server.



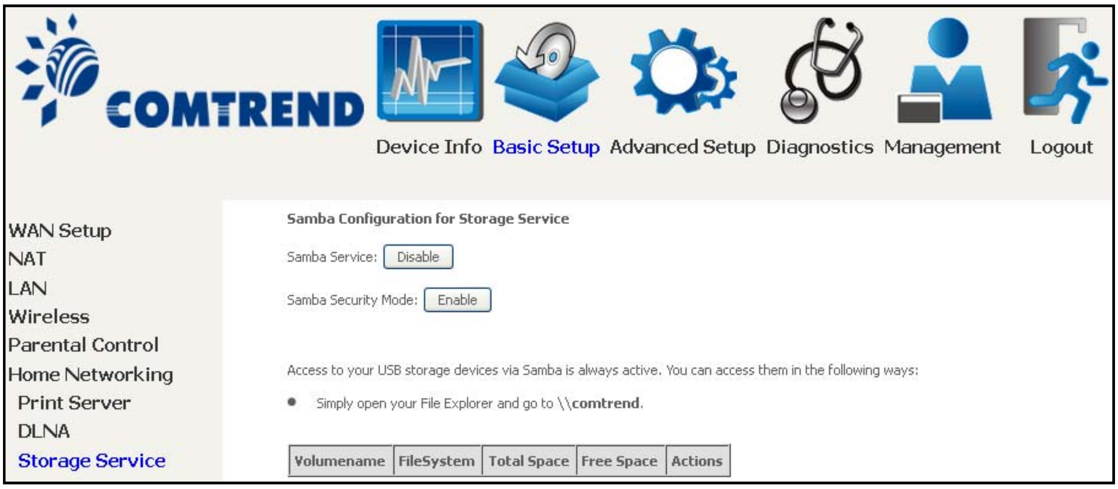
Digital Media Server settings

This page allows you to enable / disable digital media server support.

□ Enable on-board digital media server.

5.6.3 Storage Service

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



Samba Configuration for Storage Service

Samba Service: [Disable]

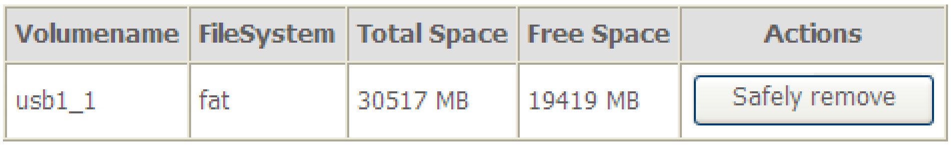
Samba Security Mode: [Enable]

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

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

Volumename	FileSystem	Total Space	Free Space	Actions

Display after storage device attached (for your reference).



Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	30517 MB	19419 MB	[Safely remove]

Chapter 6 Advanced Setup

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

6.1 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A - Firewall.

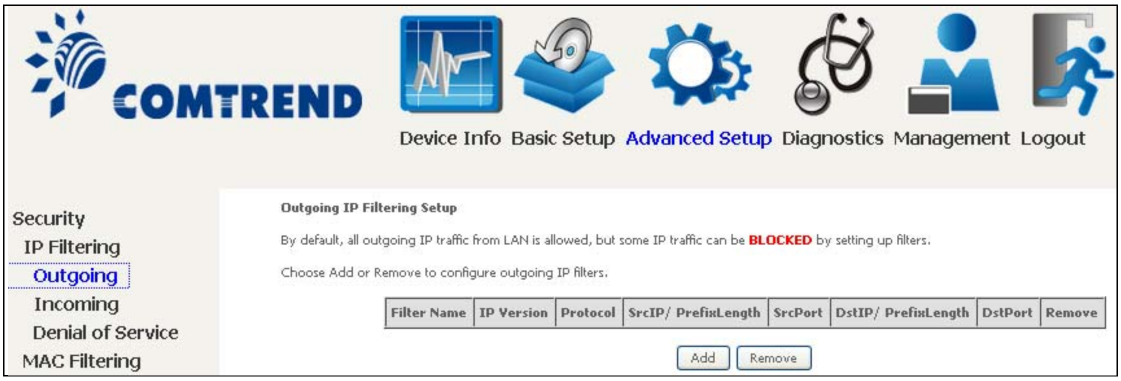
6.1.1 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering performs a similar function.

OUTGOING IP FILTER

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



Outgoing IP Filtering Setup

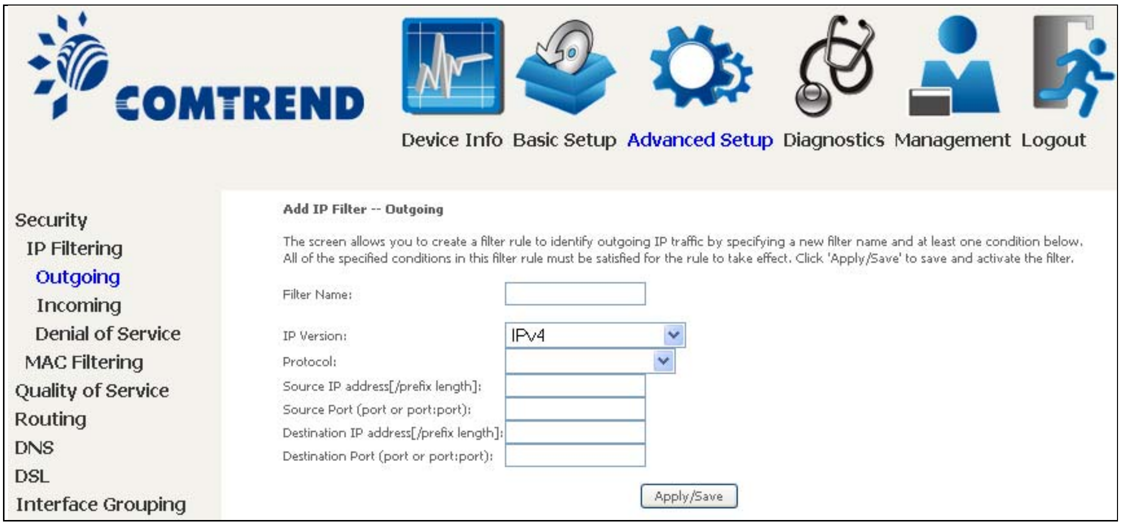
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

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

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



Add IP Filter -- Outgoing

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

Filter Name:

IP Version: IPv4

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

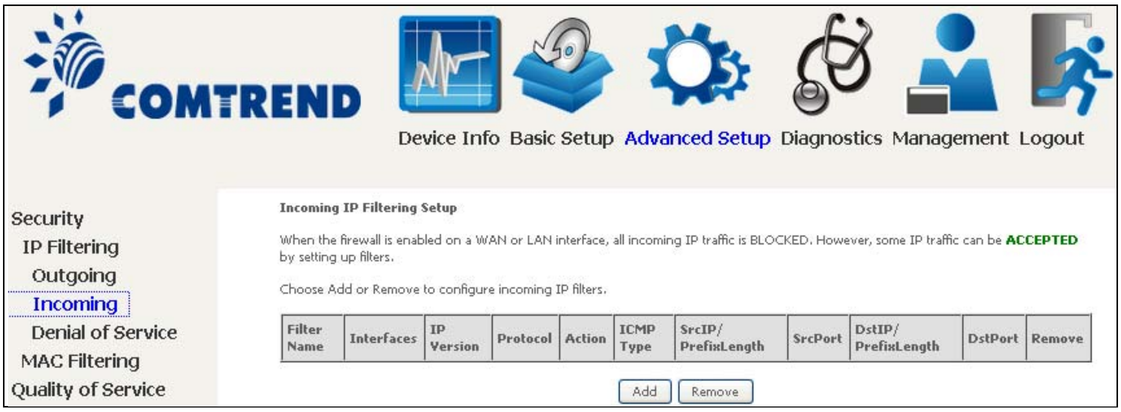
Destination Port (port or port:port):

Consult the table below for field descriptions.

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

INCOMING IP FILTER

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



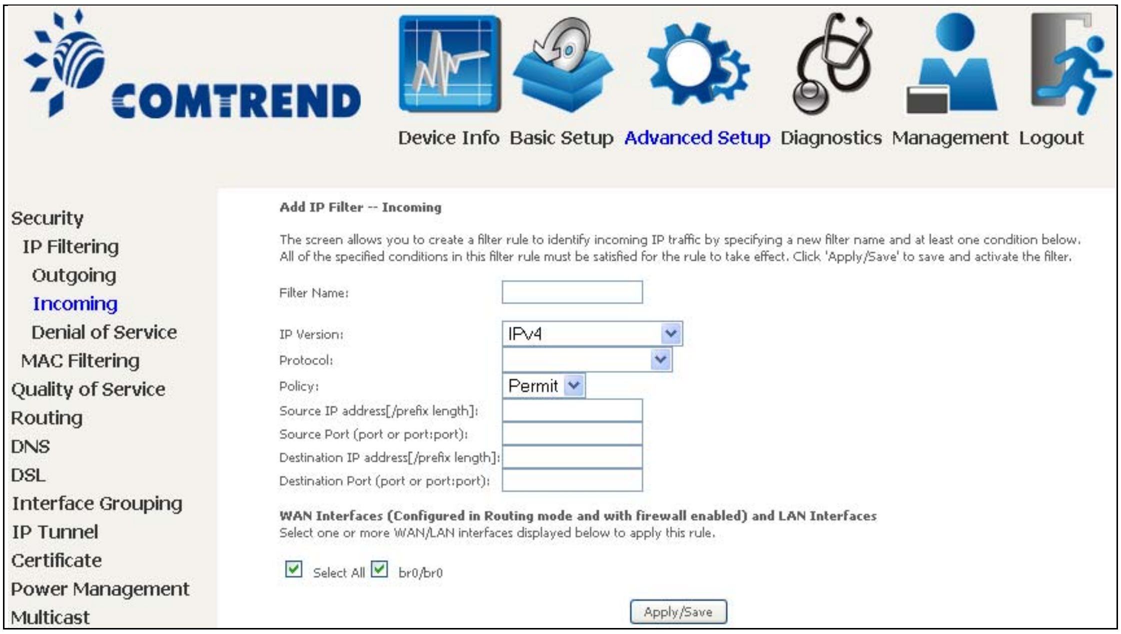
Incoming IP Filtering Setup

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

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	Action	ICMP Type	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

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**.



Add IP Filter -- Incoming

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

Filter Name:	
IP Version:	IPv4
Protocol:	
Policy:	Permit
Source IP address[/prefix length]:	
Source Port (port or port:port):	
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

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

☑ Select All ☑ br0/br0

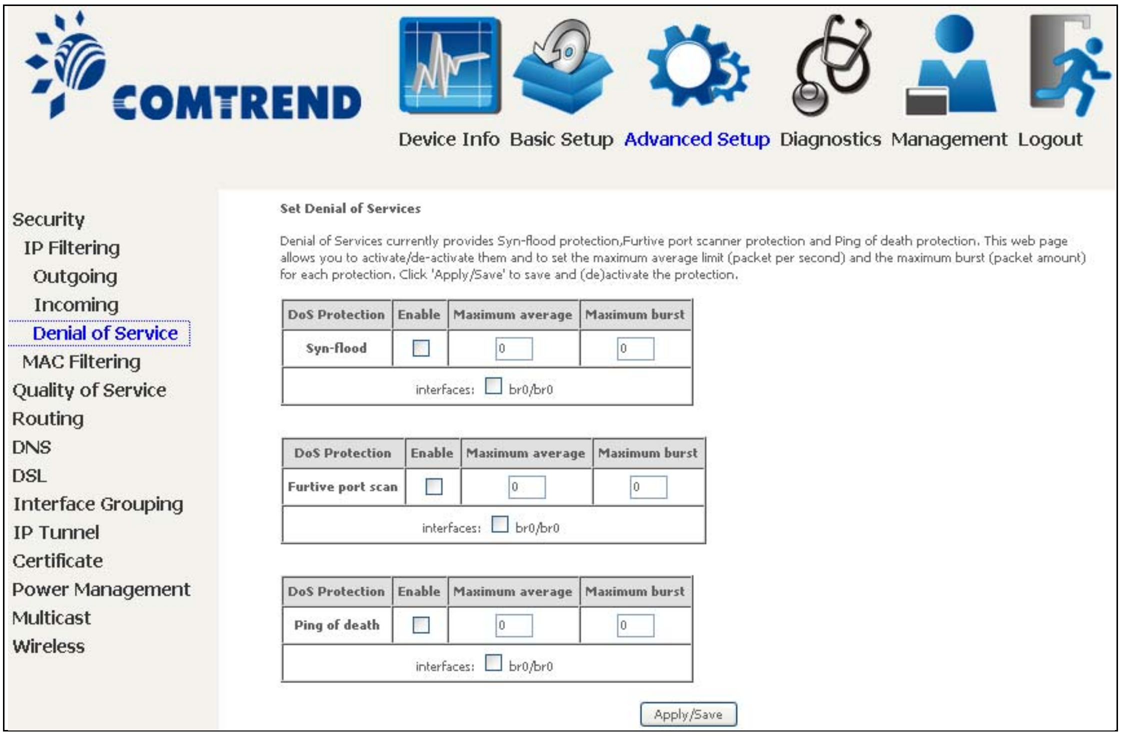
Consult the table below for field descriptions.

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

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

6.1.2 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.



Set Denial of Services

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

DoS Protection	Enable	Maximum average	Maximum burst
Syn-flood	□	0	0
interfaces: □ br0/br0			

DoS Protection	Enable	Maximum average	Maximum burst
Furtive port scan	□	0	0
interfaces: □ br0/br0			

DoS Protection	Enable	Maximum average	Maximum burst
Ping of death	□	0	0
interfaces: □ br0/br0			

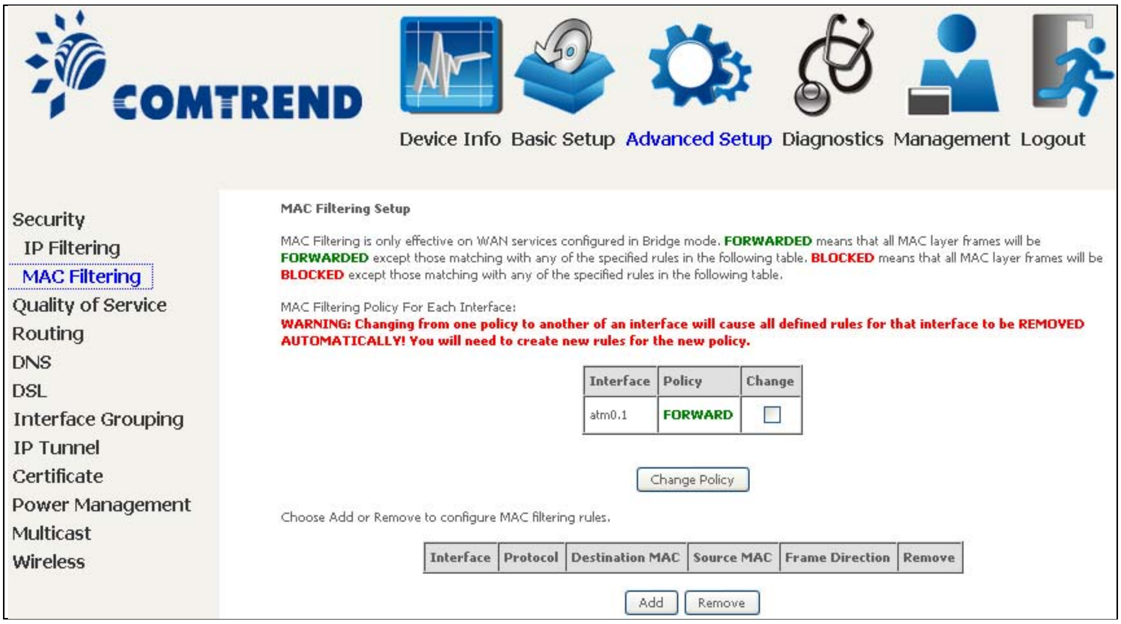
Click the **Apply/Save** button to save and (de)activate the protection.

6.1.3 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 VR-3033 can be set according to the following procedure.

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



MAC Filtering Setup

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

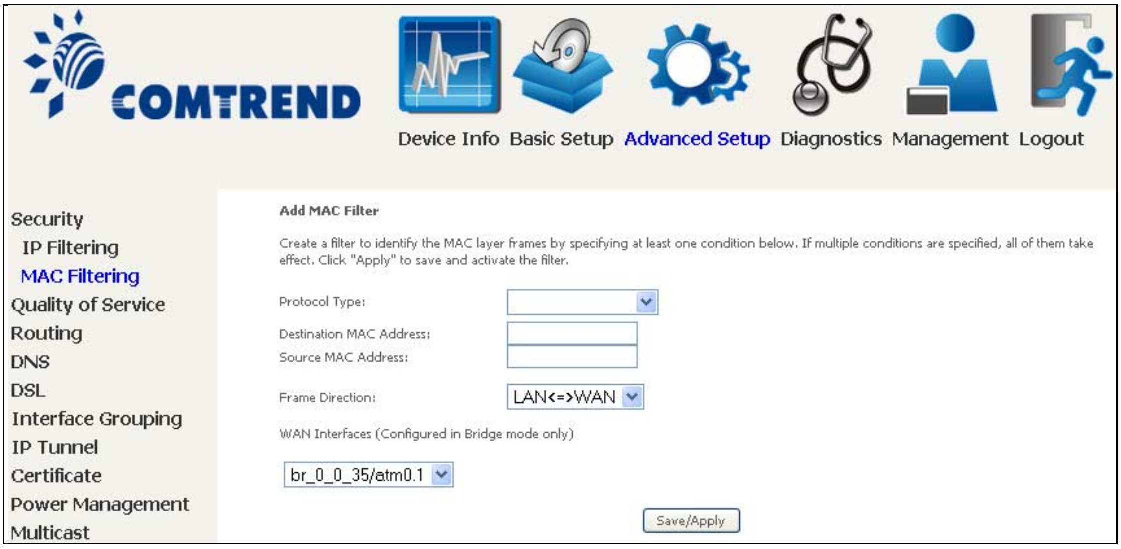
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm0.1	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	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.



Add MAC Filter

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_35/atm0.1

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

Consult the table below for detailed field descriptions.

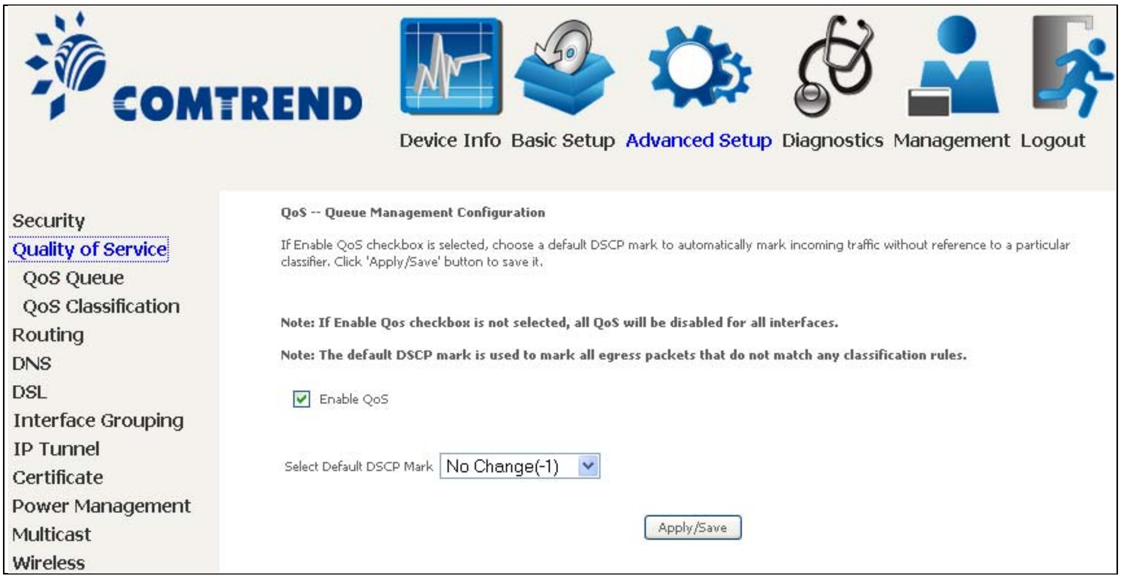
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

6.2 Quality of Service (QoS)

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

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

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



QoS -- Queue Management Configuration

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

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

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

☑ Enable QoS

Select Default DSCP Mark No Change(-1)

Apply/Save

QoS and DSCP Mark are defined as follows:

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

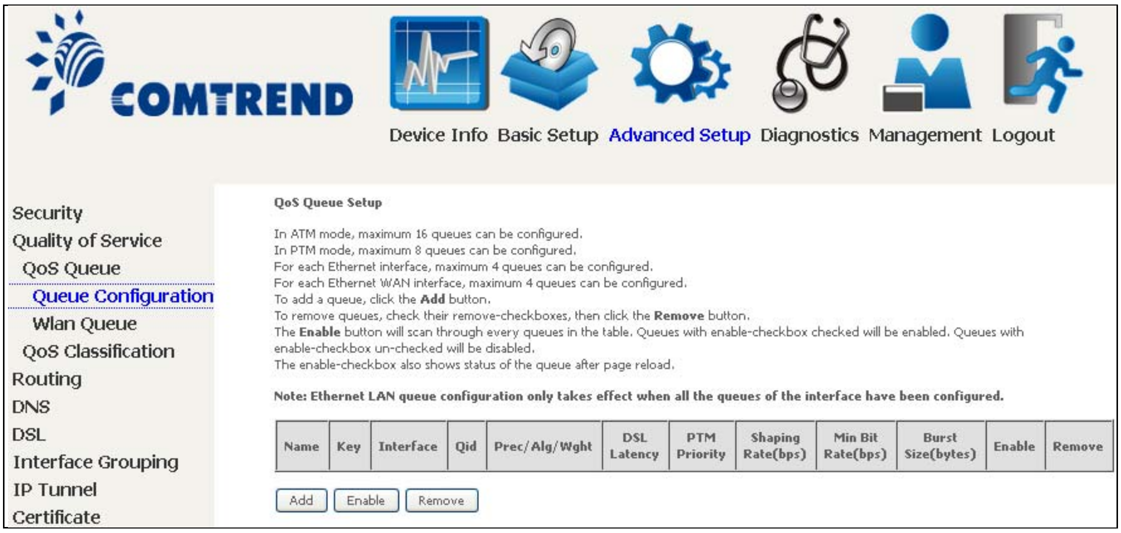
Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

6.2.1 QoS Queue

6.2.1.1 QoS Queue Configuration

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

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 3 queues can be configured.



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 4 queues can be configured.
For each Ethernet WAN interface, maximum 4 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.

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

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bps)	Min Bit Rate(bps)	Burst Size(bytes)	Enable	Remove

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

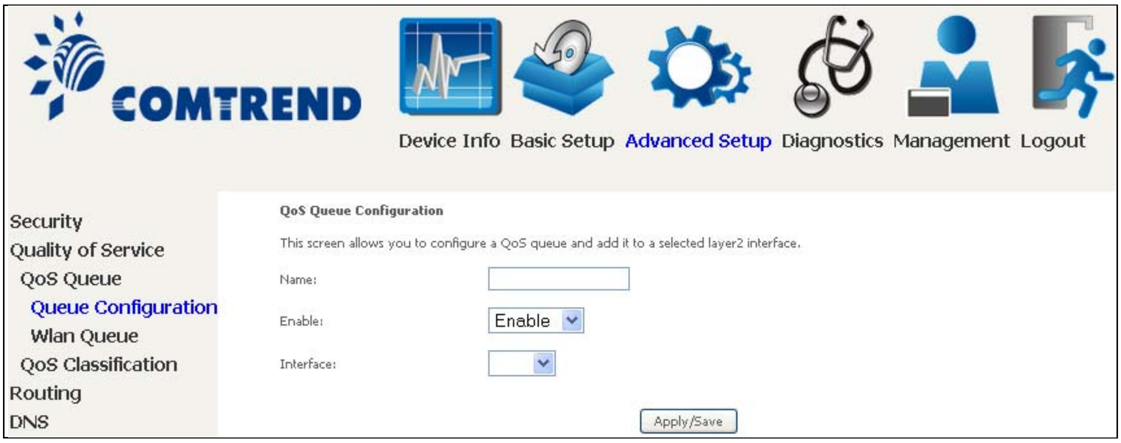
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

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

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button.

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

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



QoS Queue Configuration

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

Name:

Enable: Enable

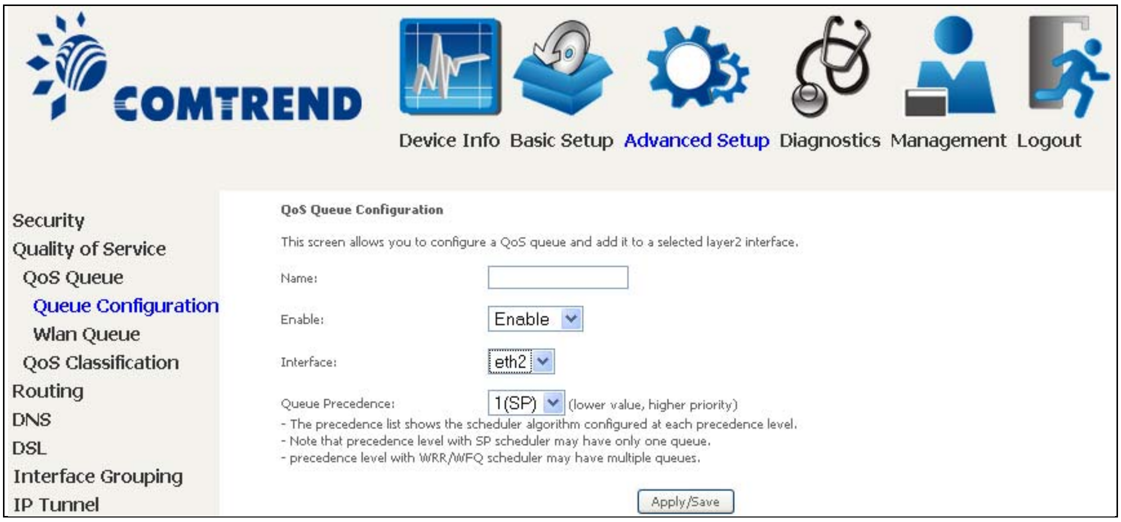
Interface:

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.



QoS Queue Configuration

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

Name:

Enable: Enable

Interface: eth2

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

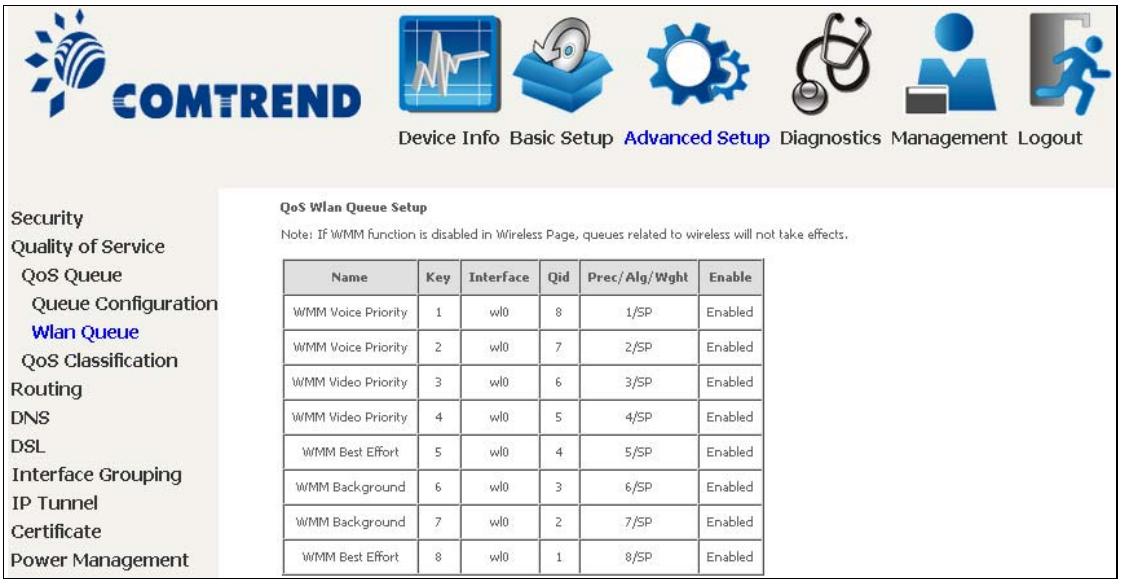
- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

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.

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

6.2.1.2 Wlan Queue

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



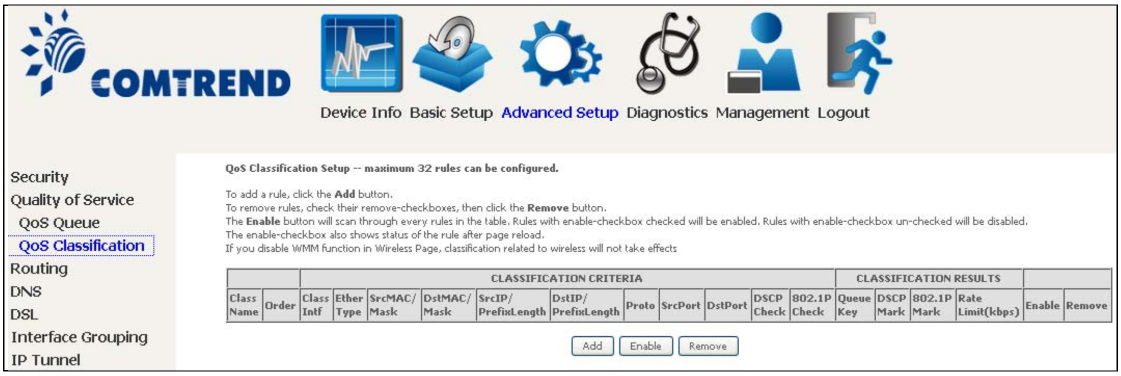
QoS Wlan Queue Setup

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

Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
WMM Voice Priority	1	wl0	8	1/SP	Enabled
WMM Voice Priority	2	wl0	7	2/SP	Enabled
WMM Video Priority	3	wl0	6	3/SP	Enabled
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled

6.2.2 QoS Classification

The network traffic classes are listed in the following table.



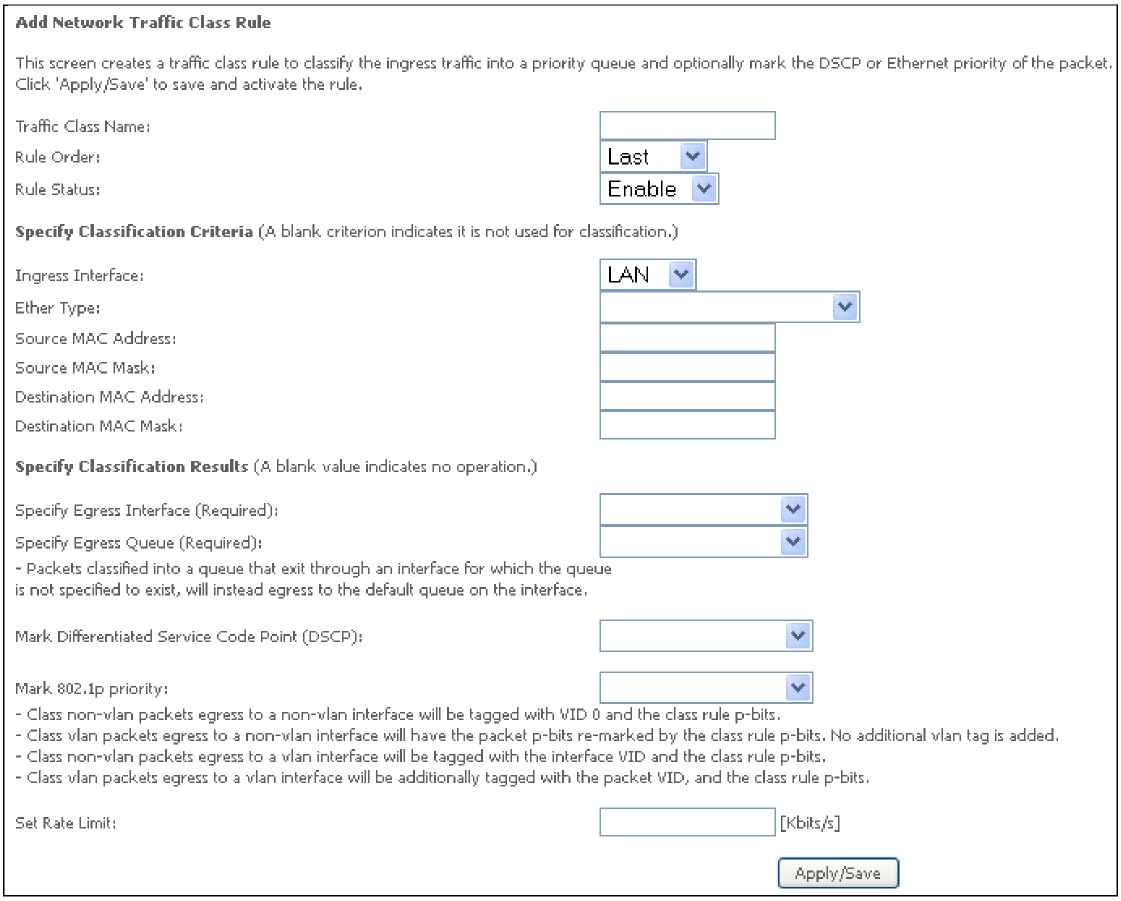
QoS Classification Setup -- maximum 32 rules can be configured.

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

		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

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:	Last
Rule Status:	Enable

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

Ingress Interface:	LAN
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, wl0)
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 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.
Set Rate Limit	The data transmission rate limit in kbps.

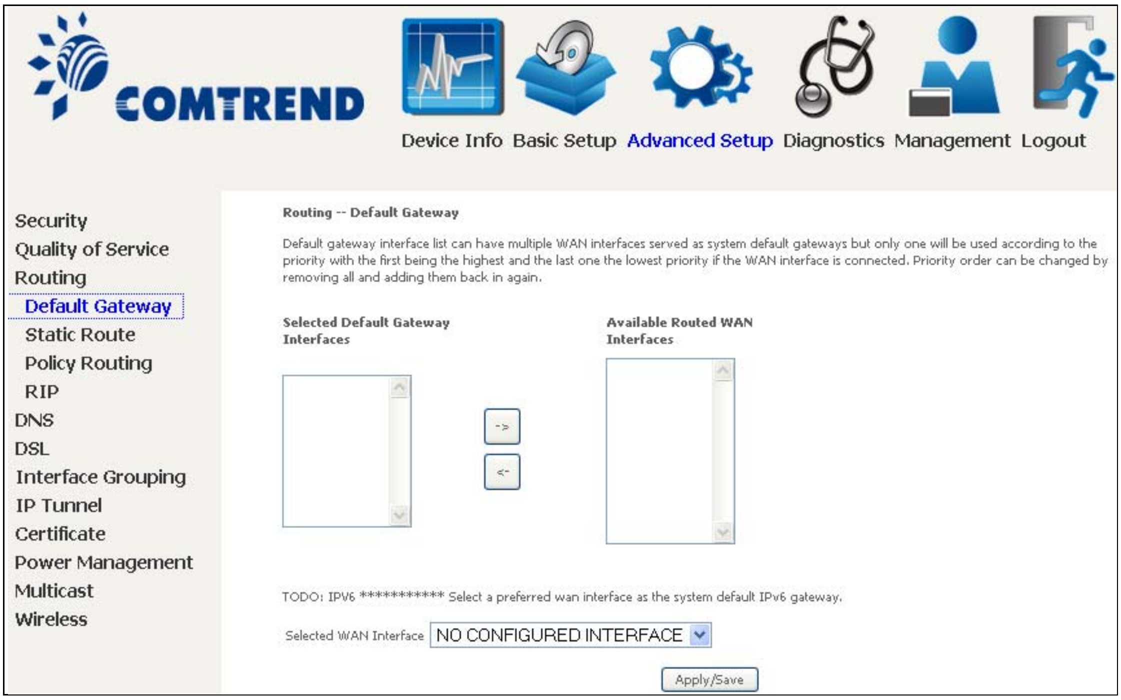
6.3 Routing

The following routing functions are accessed from this menu:
Default Gateway, Static Route, Policy Routing, RIP and **IPv6 Static Route**.

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

6.3.1 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.



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

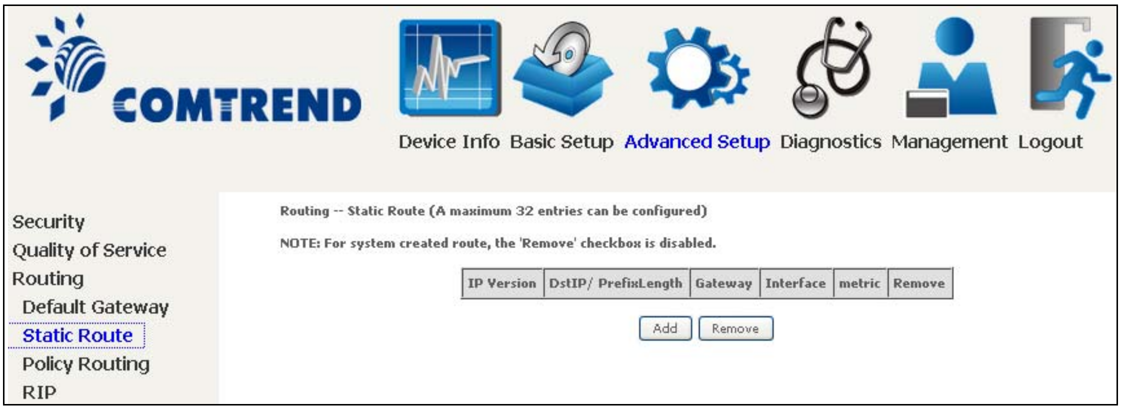
Available Routed WAN Interfaces

TODO: IPV6 *********** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: NO CONFIGURED INTERFACE

6.3.2 Static Route

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

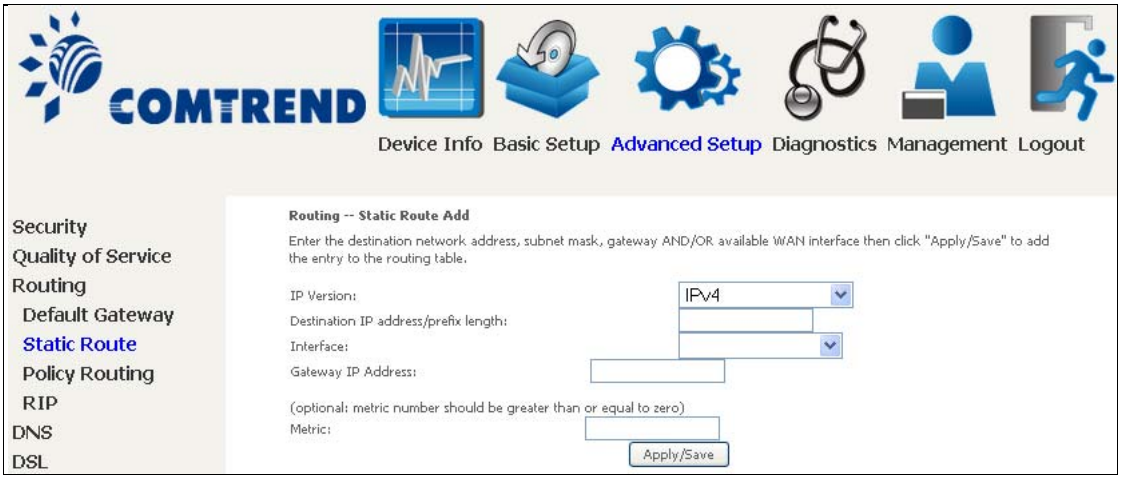


Routing -- Static Route (A maximum 32 entries can be configured)

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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

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



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

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

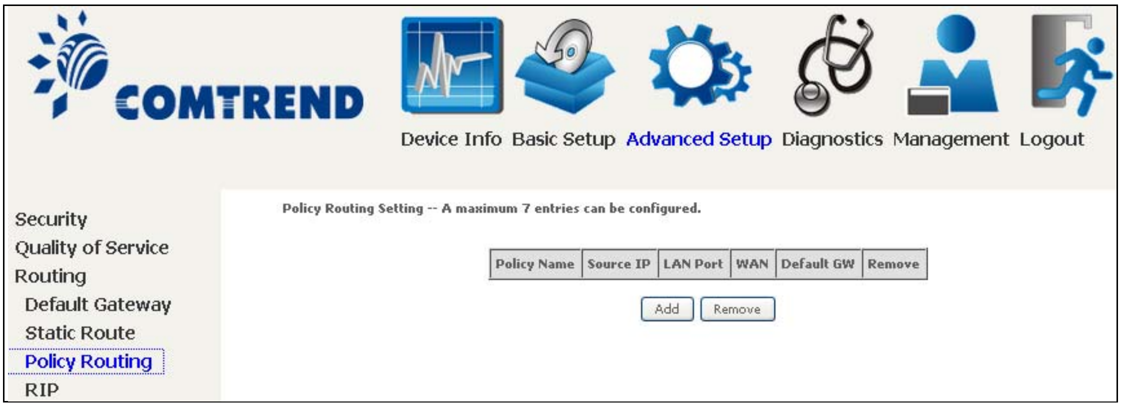
Metric:

- **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.

6.3.3 Policy Routing

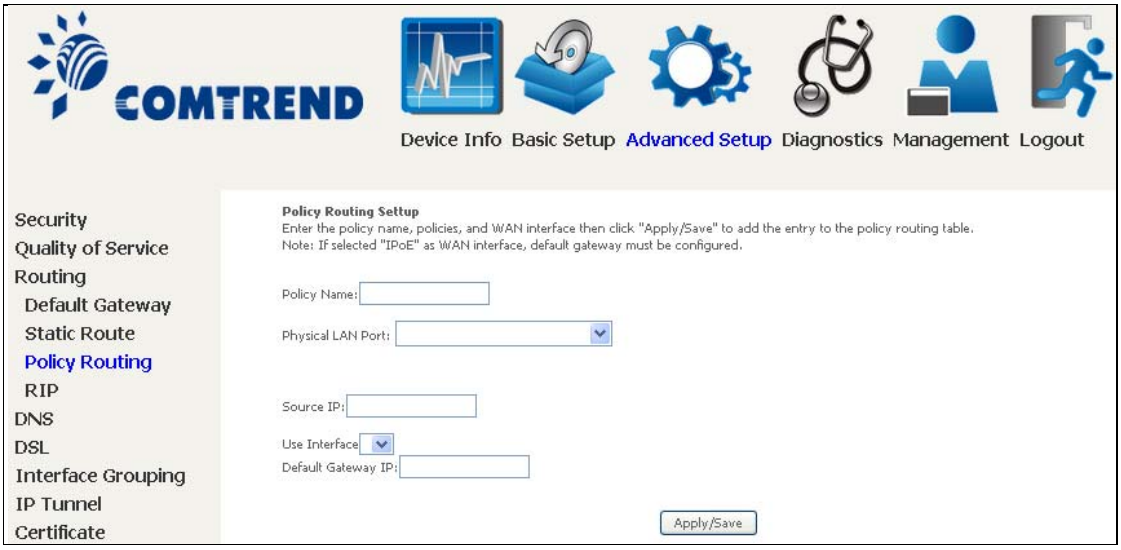
This option allows for the configuration of static routes by policy.
Click **Add** to create a routing policy or **Remove** to delete one.



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

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

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



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:

Physical LAN Port:

Source IP:

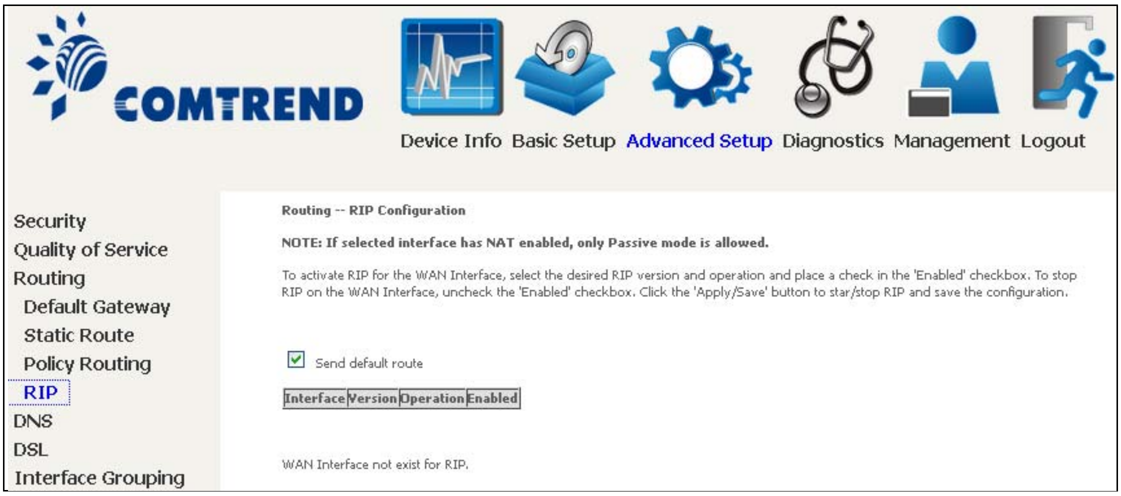
Use Interface

Default Gateway IP:

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

6.3.4 RIP

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



Routing -- RIP Configuration

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

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

☑ Send default route

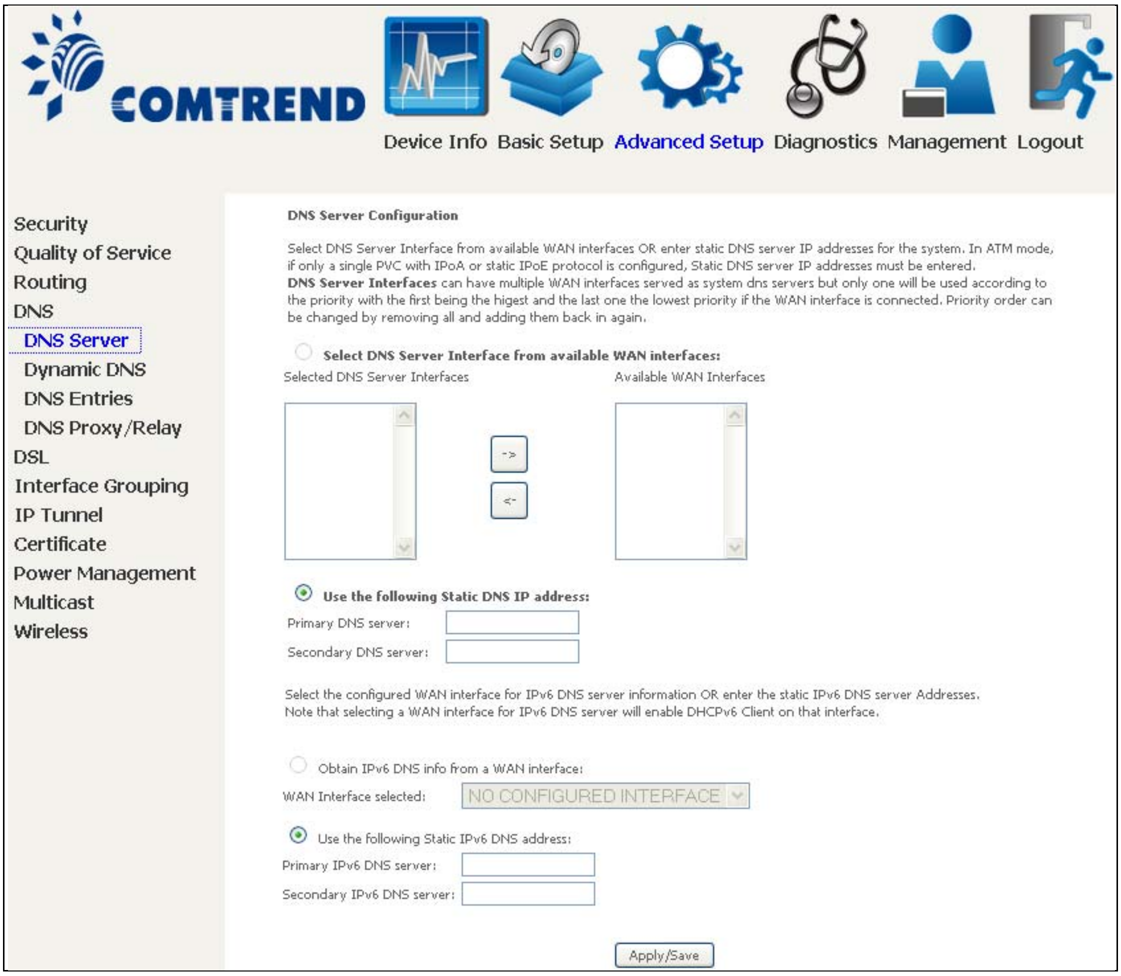
Interface	Version	Operation	Enabled

WAN Interface not exist for RIP.

6.4 DNS

6.4.1 DNS Server

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



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 higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

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

Selected DNS Server Interfaces | Available WAN Interfaces

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

Primary DNS server:

Secondary DNS server:

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

○ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: NO CONFIGURED INTERFACE

● Use the following Static IPv6 DNS address:

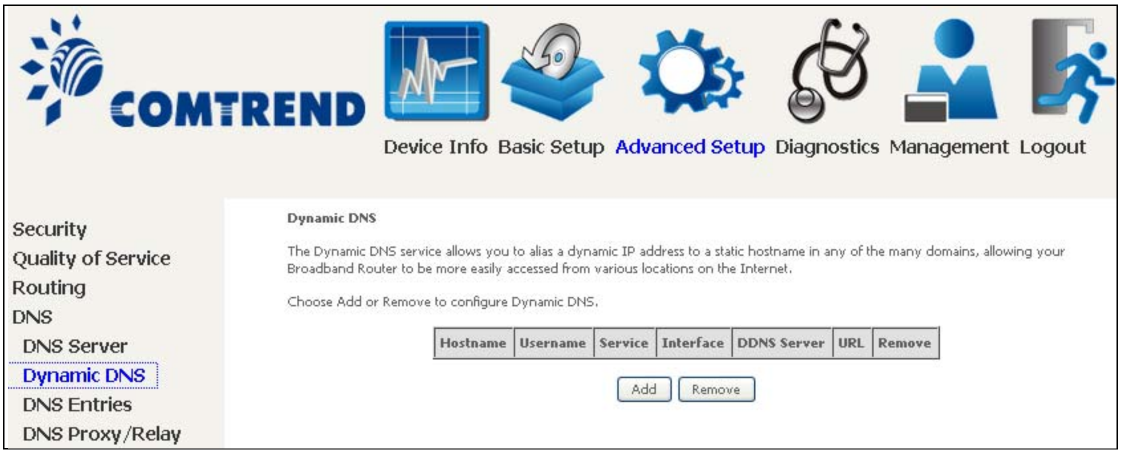
Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

6.4.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the VR-3033 to be more easily accessed from various locations on the Internet.



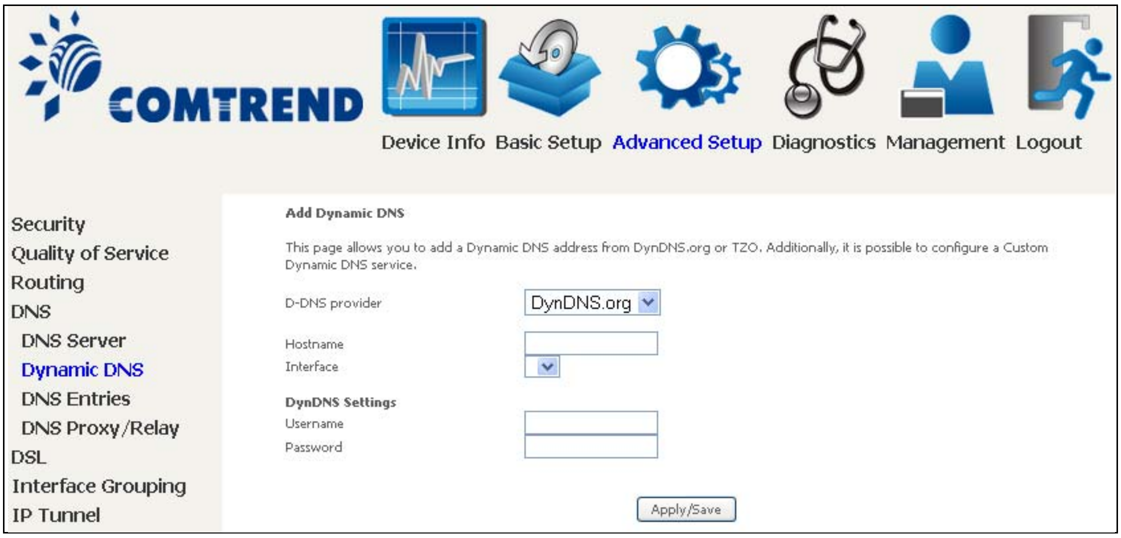
Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	DDNS Server	URL	Remove

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



Add Dynamic DNS

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

D-DNS provider: DynDNS.org

Hostname:

Interface:

DynDNS Settings

Username:

Password:

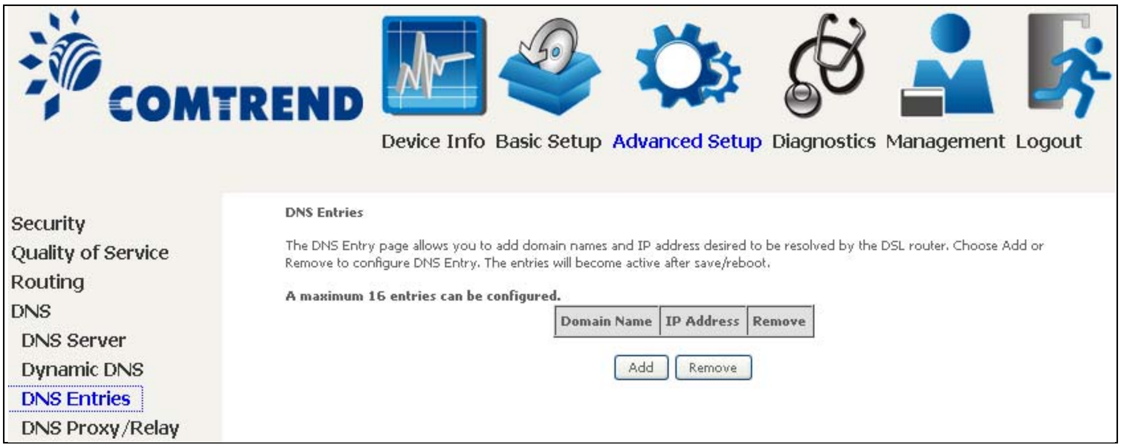
Click **Apply/Save** to save your settings.

Consult the table below for field descriptions.

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

6.4.3 DNS Entries

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



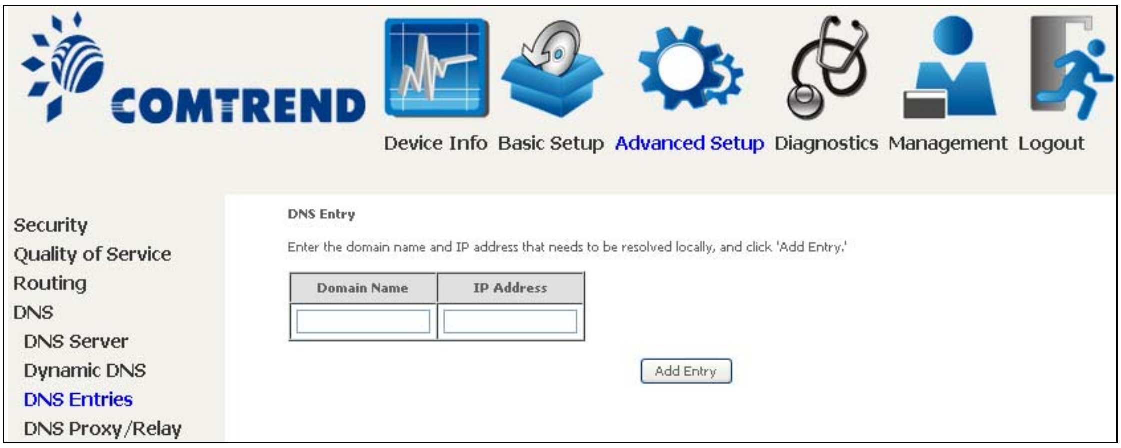
DNS Entries

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

A maximum 16 entries can be configured.

Domain Name	IP Address	Remove

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



DNS Entry

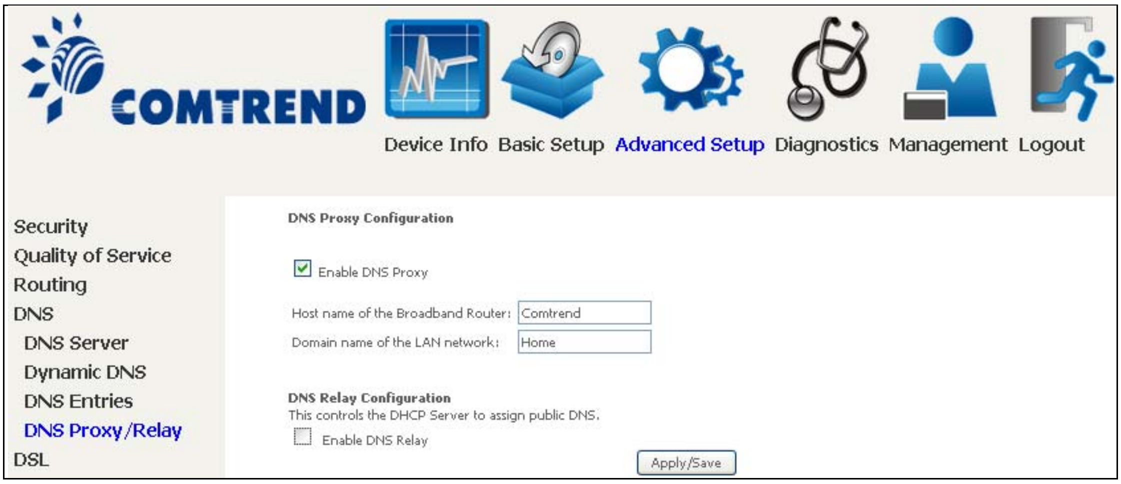
Enter the domain name and IP address that needs to be resolved locally, and click 'Add Entry.'

Domain Name	IP Address

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

6.4.4 DNS Proxy / Relay

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



DNS Proxy Configuration

☑ Enable DNS Proxy

Host name of the Broadband Router: Comtrend

Domain name of the LAN network: Home

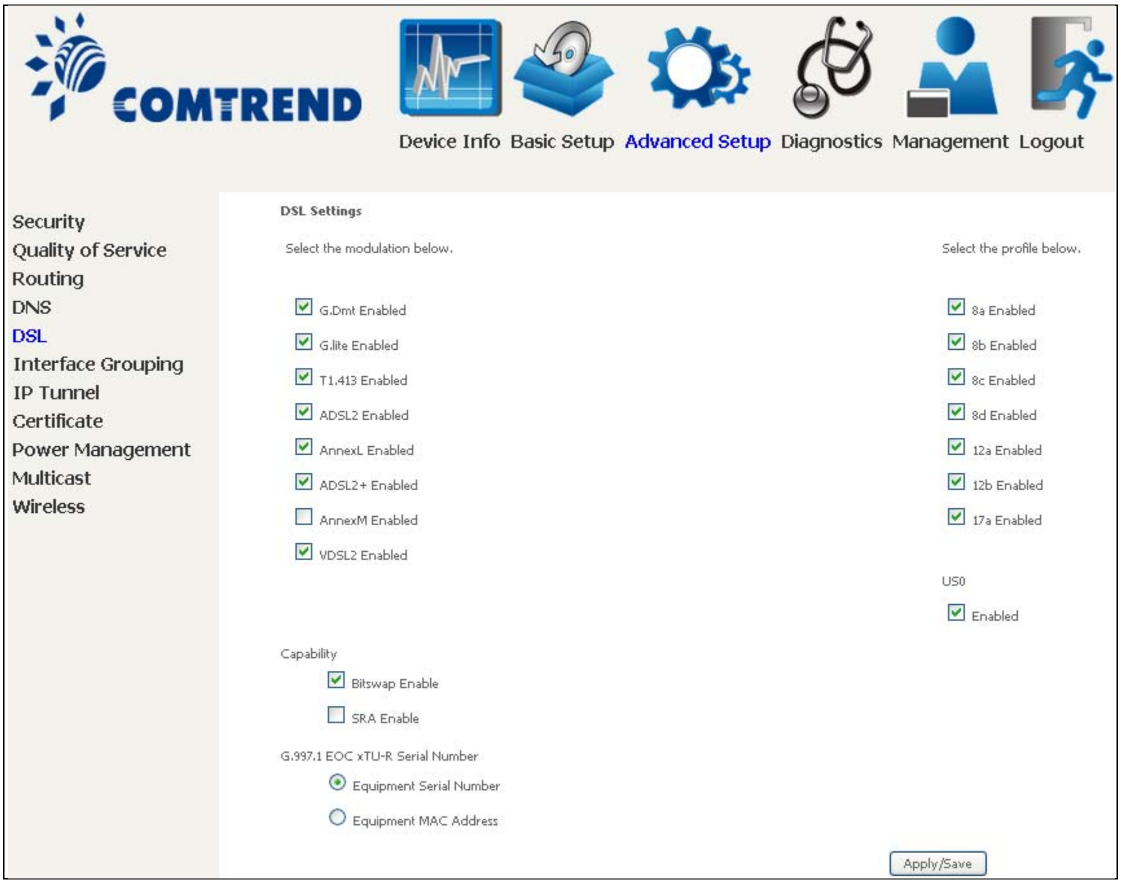
DNS Relay Configuration

This controls the DHCP Server to assign public DNS.

□ Enable DNS Relay

6.5 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 Settings

Select the modulation below.

☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
☐ AnnexM Enabled
☑ VDSL2 Enabled

Select the profile below.

☑ 8a Enabled
☑ 8b Enabled
☑ 8c Enabled
☑ 8d Enabled
☑ 12a Enabled
☑ 12b Enabled
☑ 17a Enabled

US0

☑ Enabled

Capability

☑ Bitswap Enable
☐ SRA Enable

G.997.1 EOC xTU-R Serial Number

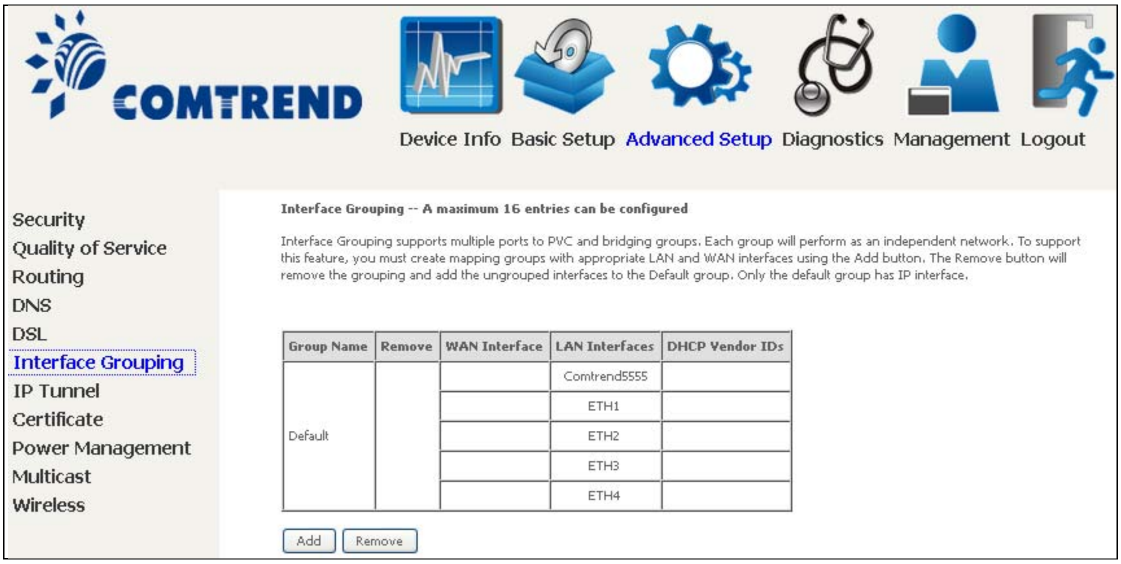
● Equipment Serial Number
○ Equipment MAC Address

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

VDSL Profile	Maximum Downstream Throughput- Mbps (Megabits per second)
8a	Downstream 50
8b	Downstream 50
8c	Downstream: 50
8d	Downstream: 50
12a	Downstream: 68
12b	Downstream: 68
17a	Downstream: 100
Options	**Description**
US0	Band between 20 and 138 kHz for long loops to upstream
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
G997.1 EOC 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

6.6 Interface Grouping

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

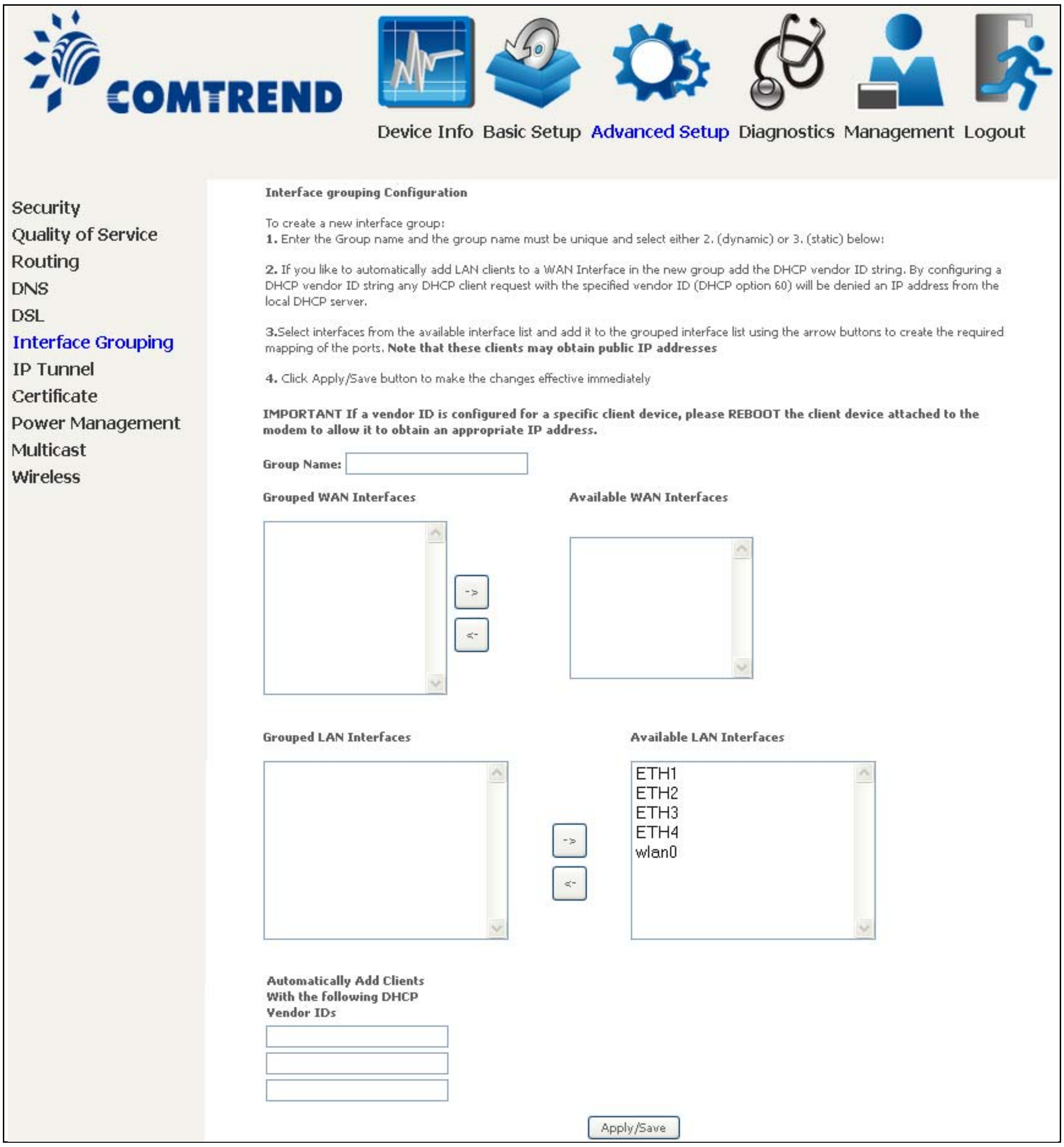


Interface Grouping -- A maximum 16 entries can be configured

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	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			Comtrend5555	
			ETH1	
			ETH2	
			ETH3	
			ETH4	

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.



Interface grouping Configuration

To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

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

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

Group Name:

Grouped WAN Interfaces | **Available WAN Interfaces**

Grouped LAN Interfaces | **Available LAN Interfaces**

ETH1
ETH2
ETH3
ETH4
wlan0

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients With Following DHCP Vendor IDs:

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

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

The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and ETH4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

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

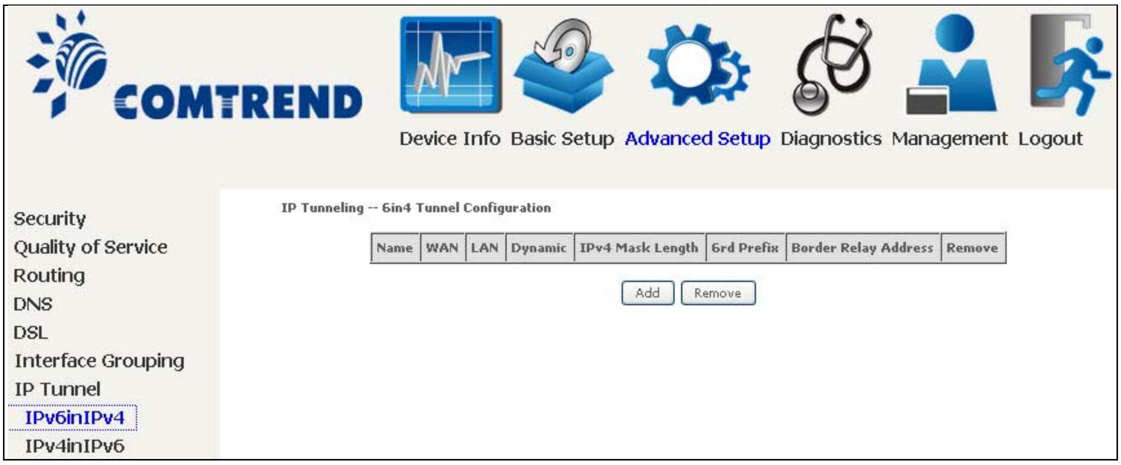
If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ETH2, ETH3, and ETH4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ETH1.

6.7 IP Tunnel

6.7.1 IPv6inIPv4

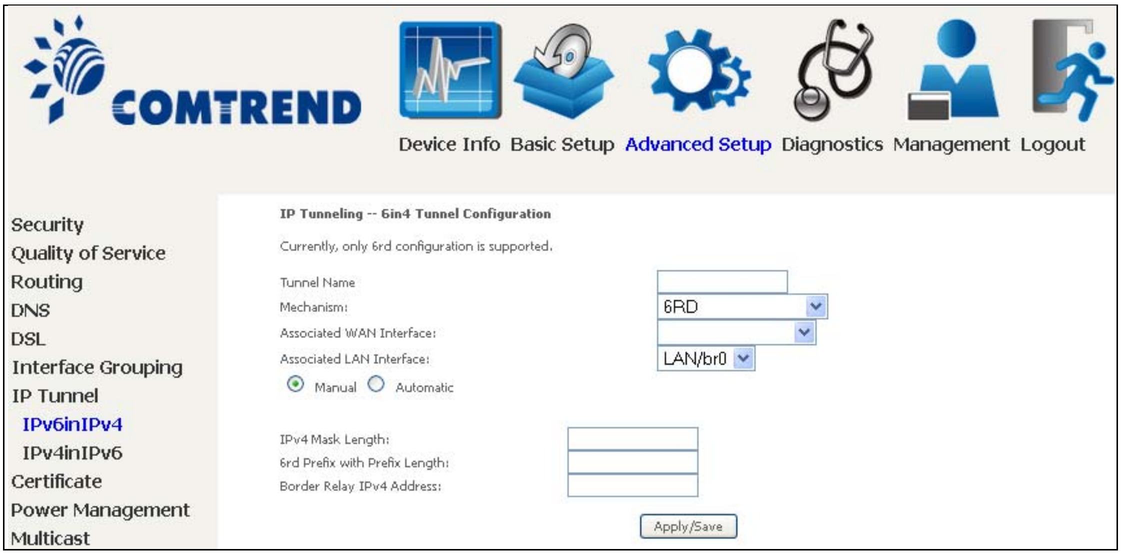
Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.



IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

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



IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name

Mechanism: 6RD

Associated WAN Interface:

Associated LAN Interface: LAN/br0

● Manual ○ Automatic

IPv4 Mask Length:

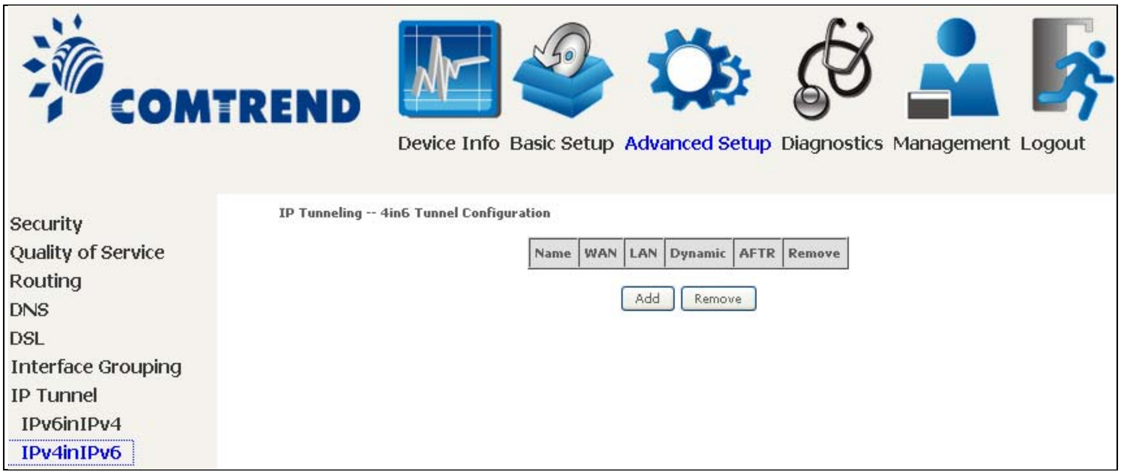
6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

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

6.7.2 IPv4inIPv6

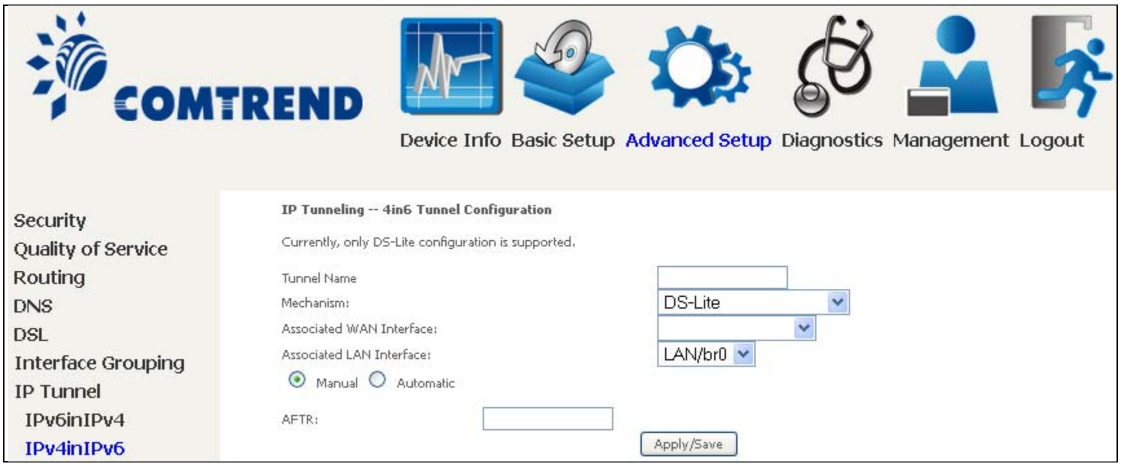
Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.



IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove

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



IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

● Manual ○ Automatic

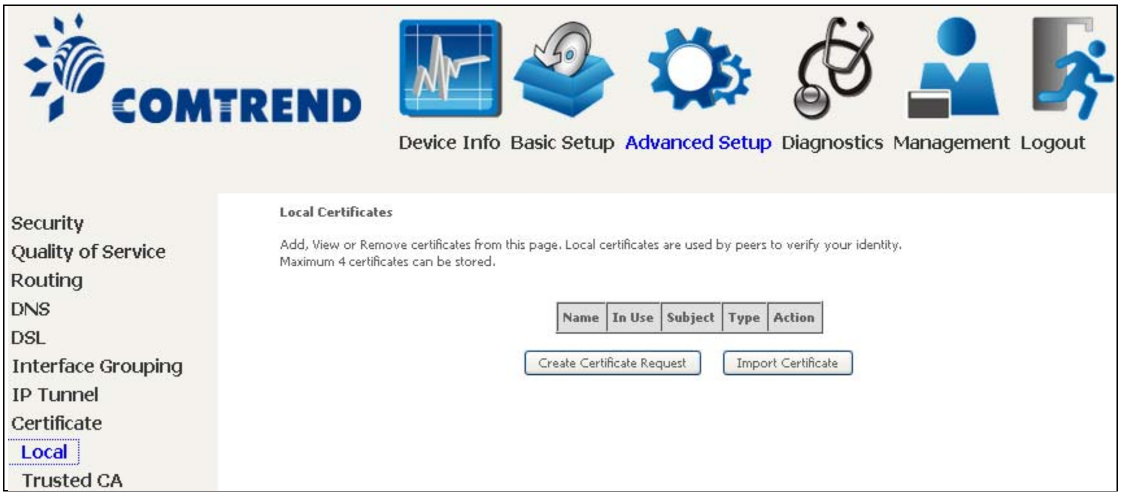
AFTR:

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

6.8 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.

6.8.1 Local



Local Certificates

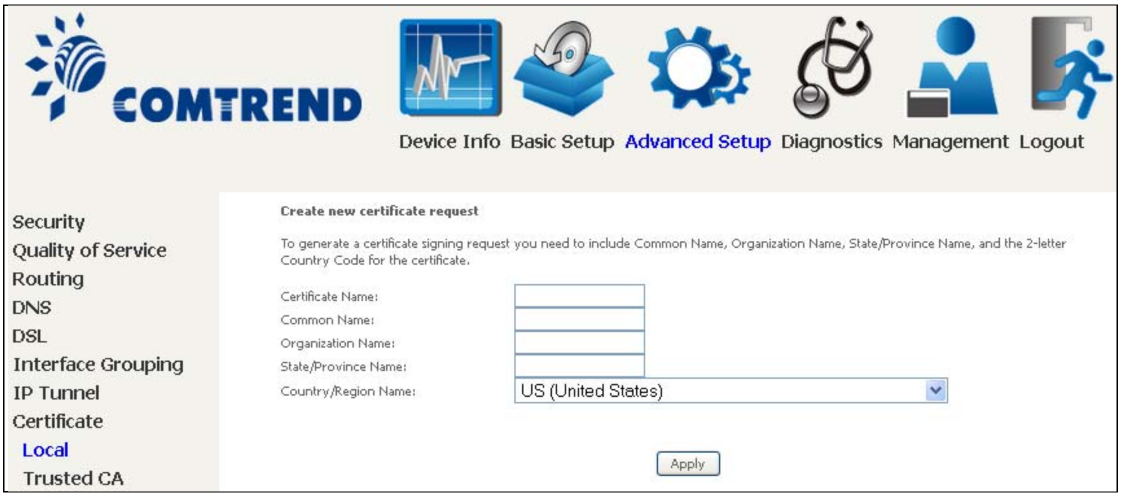
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

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.



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name: US (United States)

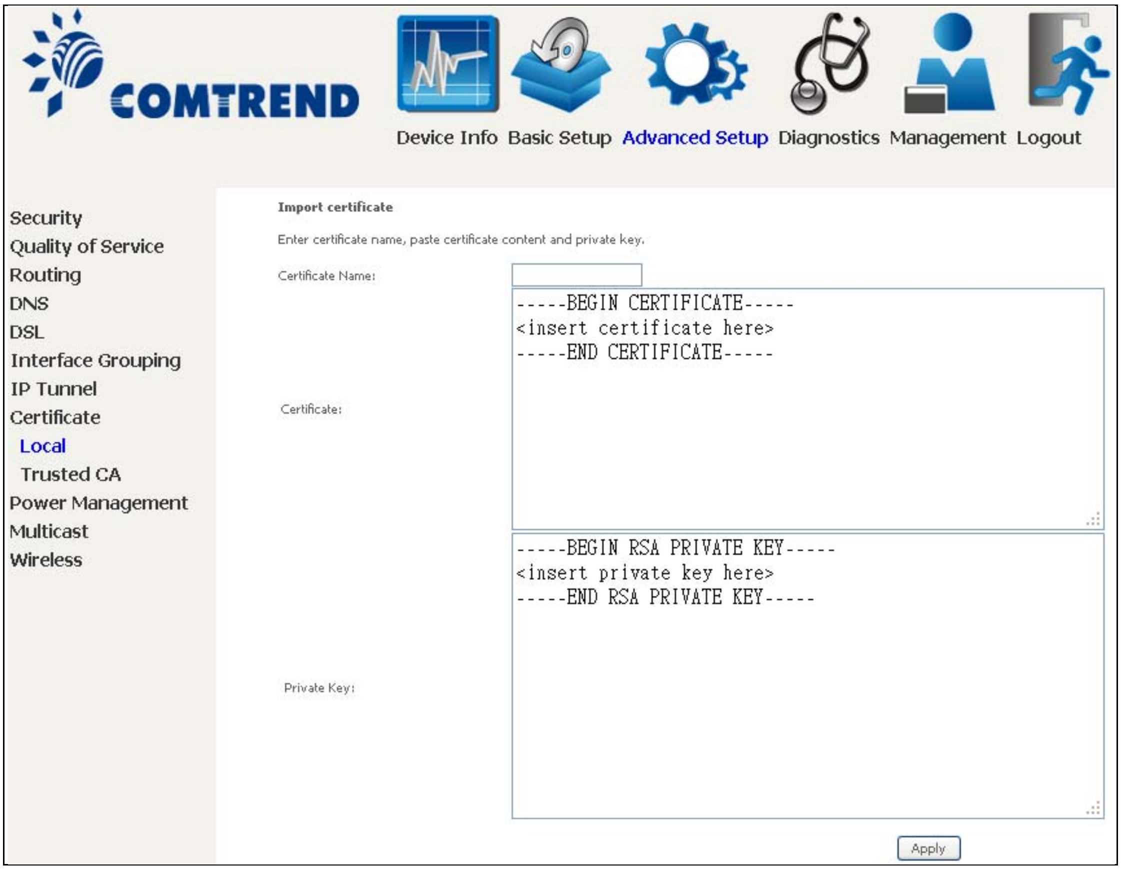
The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.

Field	Description
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.



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

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

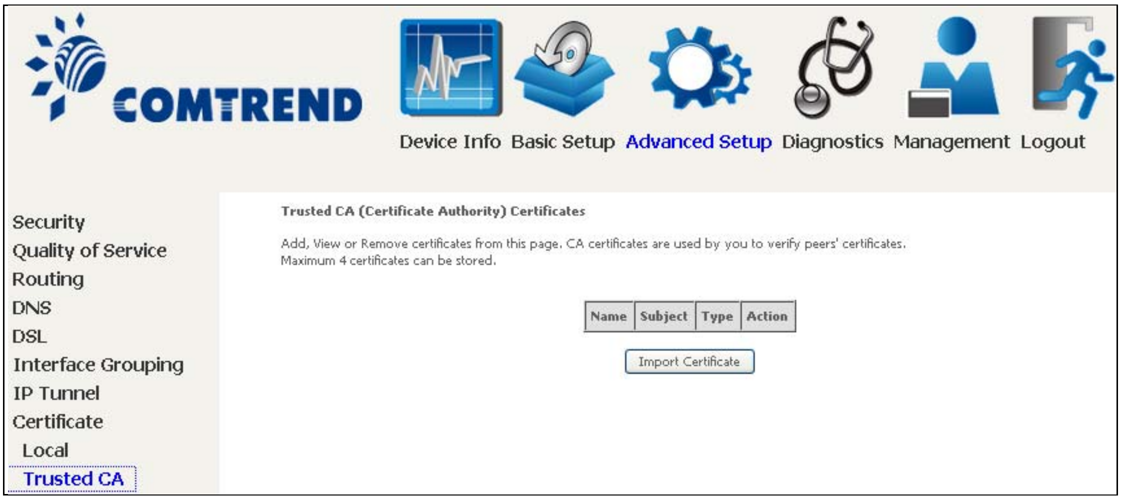
Private Key:

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

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

6.8.2 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.

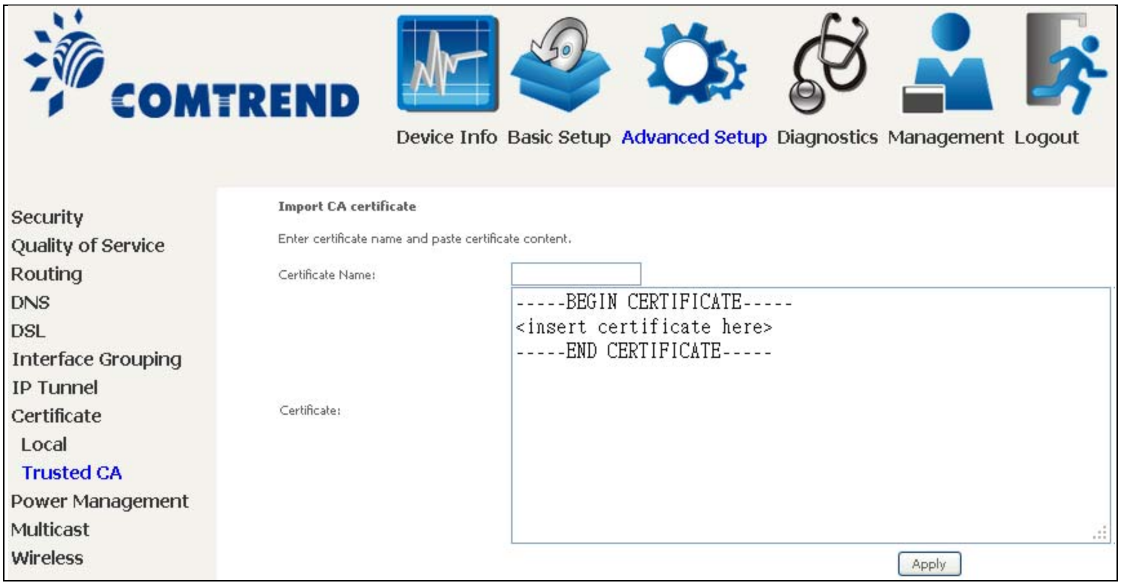


Trusted CA (Certificate Authority) Certificates

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

Name	Subject	Type	Action

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.



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

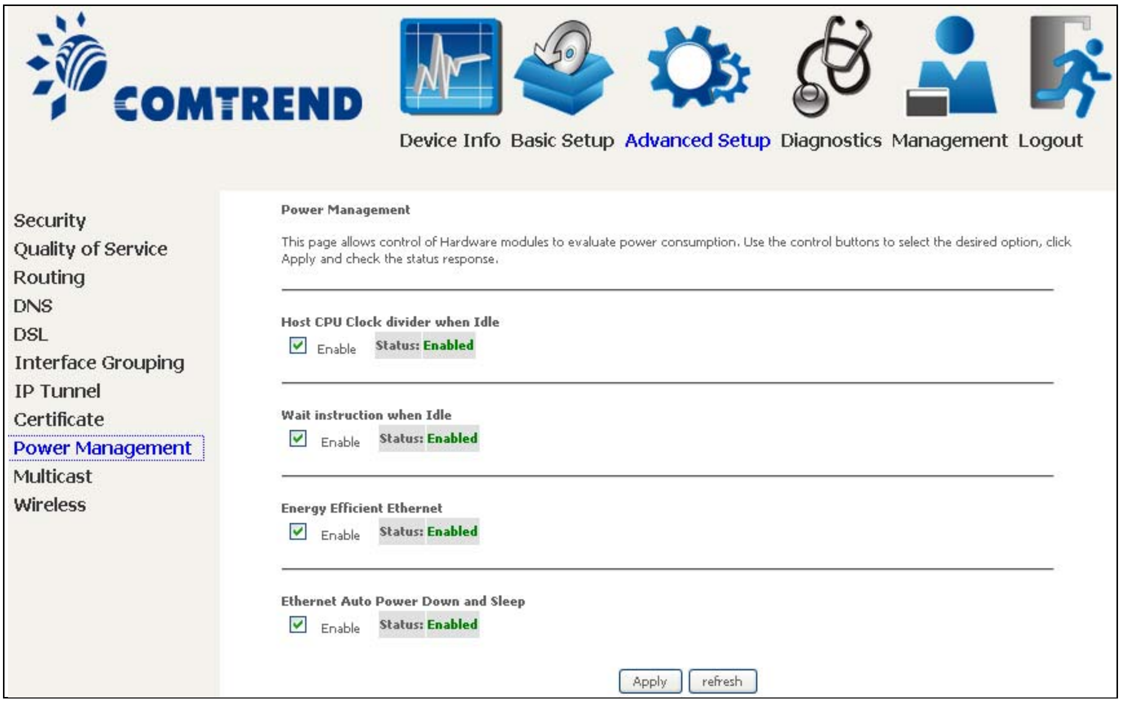
Certificate:

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

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

6.9 Power Management

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



Power Management

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

Host CPU Clock divider when Idle
☑ Enable Status: Enabled

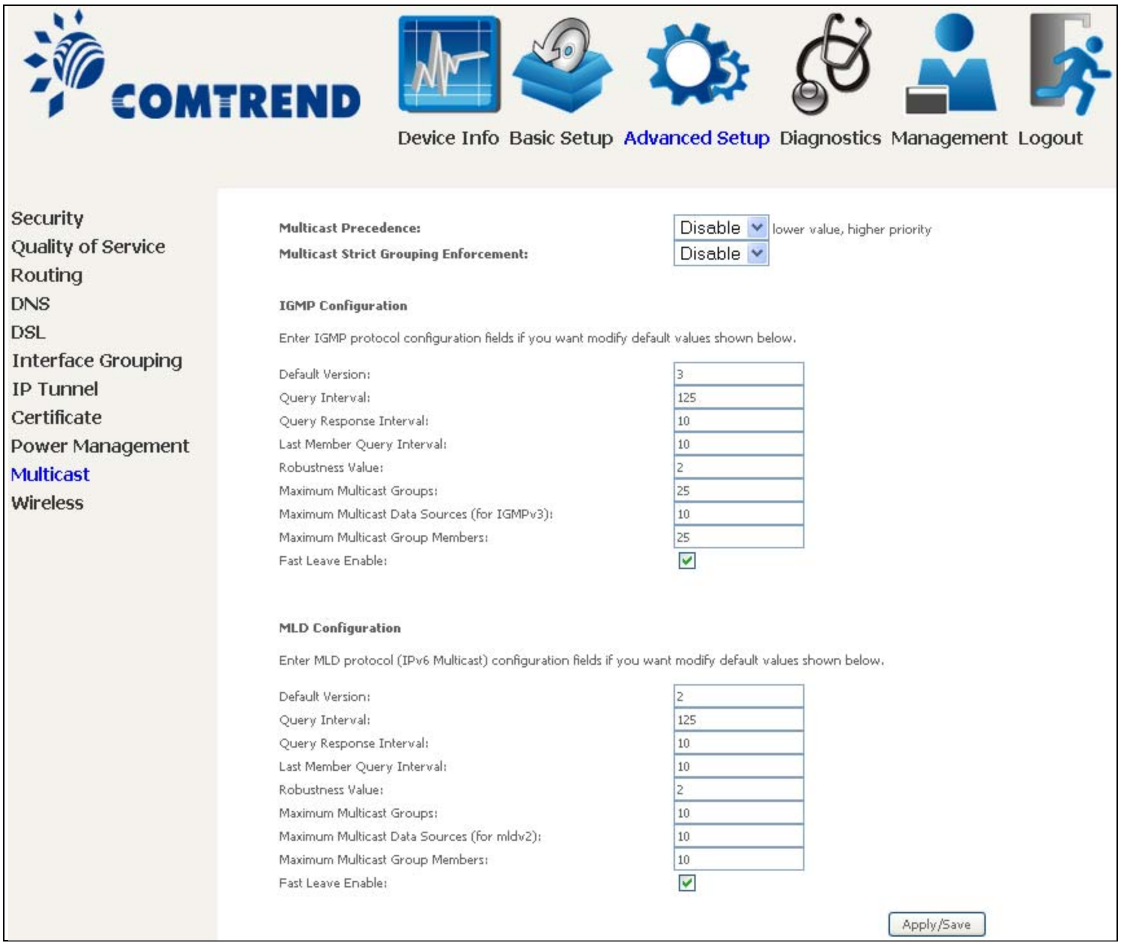
Wait instruction when Idle
☑ Enable Status: Enabled

Energy Efficient Ethernet
☑ Enable Status: Enabled

Ethernet Auto Power Down and Sleep
☑ Enable Status: Enabled

6.10 Multicast

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



Multicast Precedence: Disable lower value, higher priority
Multicast Strict Grouping Enforcement: Disable

IGMP Configuration

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

Default Version: 3
Query Interval: 125
Query Response Interval: 10
Last Member Query Interval: 10
Robustness Value: 2
Maximum Multicast Groups: 25
Maximum Multicast Data Sources (for IGMPv3): 10
Maximum Multicast Group Members: 25
Fast Leave Enable: ☑

MLD Configuration

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

Default Version: 2
Query Interval: 125
Query Response Interval: 10
Last Member Query Interval: 10
Robustness Value: 2
Maximum Multicast Groups: 10
Maximum Multicast Data Sources (for mldv2): 10
Maximum Multicast Group Members: 10
Fast Leave Enable: ☑

Multicast Precedence:

Select precedence of multicast packets.

Multicast Strict Grouping Enforcement:

Enable/Disable multicast strict grouping.

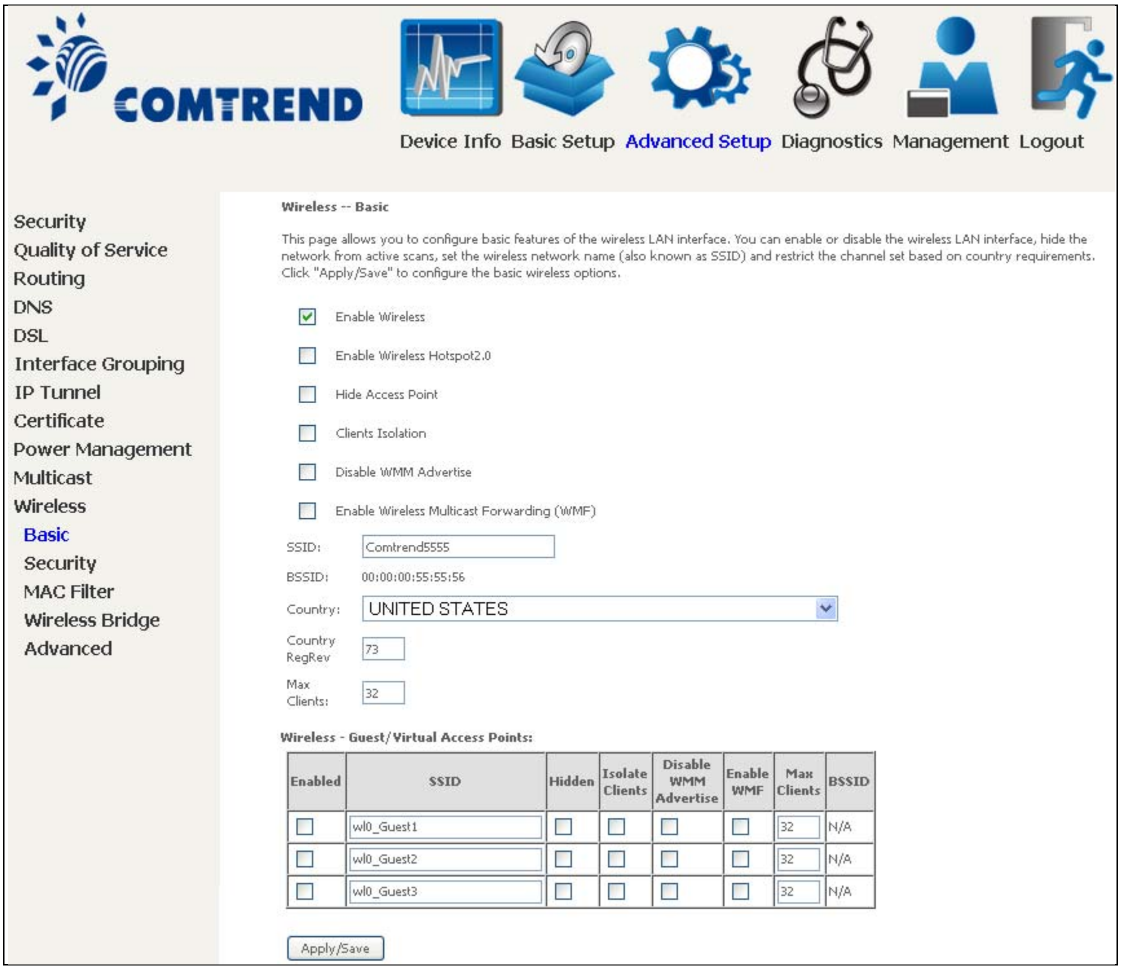
Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.

Field	Description
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.

6.11 Wireless

6.11.1 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

□ Enable Wireless Hotspot2.0

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID:	Comtrend5555
BSSID:	00:00:00:55:55:56
Country:	UNITED STATES
Country RegRev	73
Max Clients:	32

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	wl0_Guest1	□	□	□	□	32	N/A
□	wl0_Guest2	□	□	□	□	32	N/A
□	wl0_Guest3	□	□	□	□	32	N/A

Apply/Save

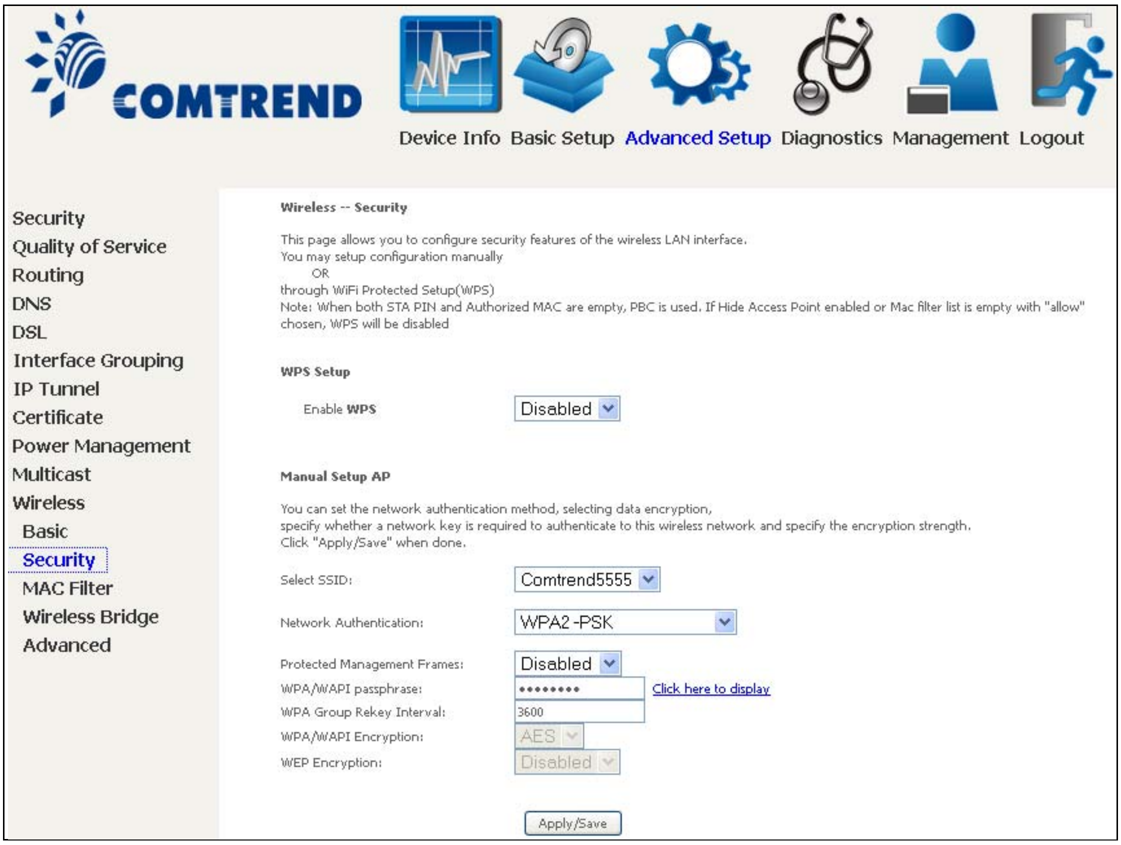
Click **Apply/Save** to apply the selected wireless options.

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.
Enable Wireless Hotspot2.0	Enable Wireless Hotspot 2.0 (Wi-Fi Certified Passpoint) on the wireless interface.
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.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Country RegRev	Wireless country code for transmit power limit.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	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.

6.11.2 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.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

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

Select SSID: Comtrend5555

Network Authentication: WPA2 -PSK

Protected Management Frames: Disabled

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

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Please see 6.11.3 for WPS setup instructions.

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

WIRELESS SECURITY

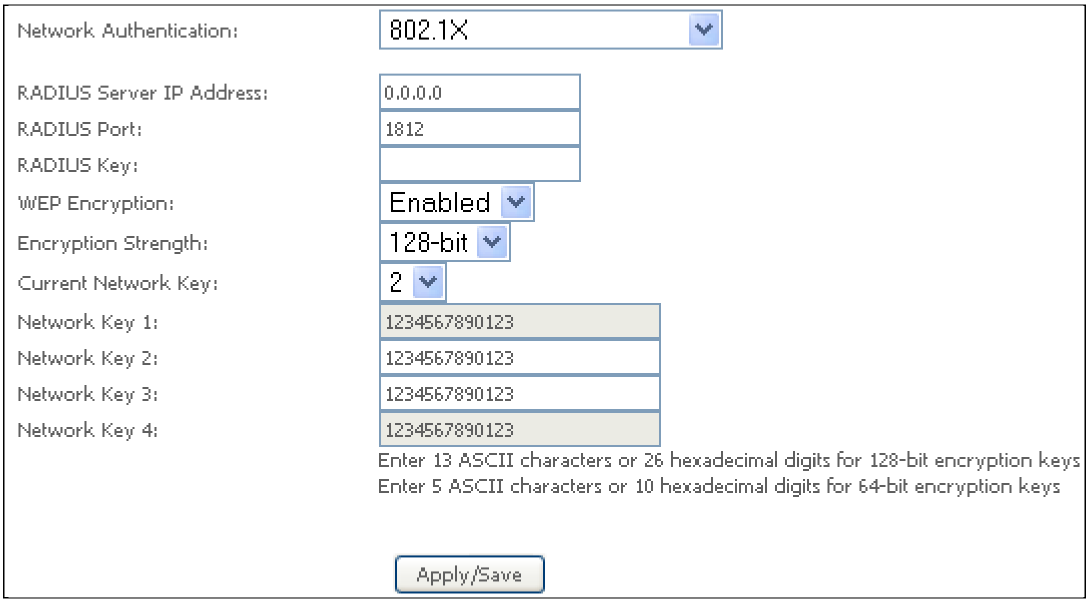
Setup requires that the user configure these settings using the Web User Interface (see the table below).

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

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below. Different authentication type pops up different settings requests.

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

Also, enable WEP Encryption and select Encryption Strength.

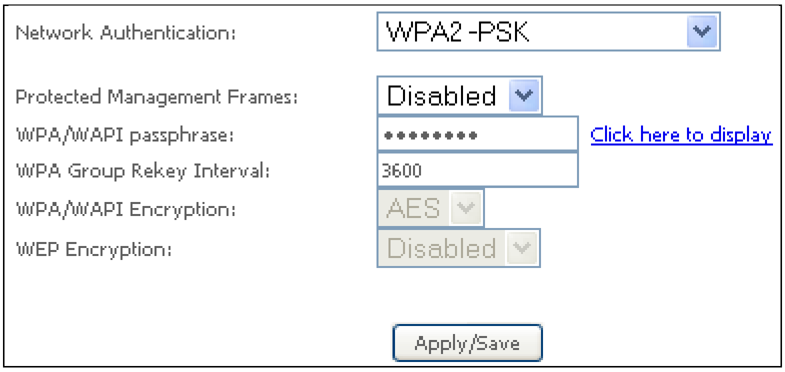


Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	2
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

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

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

Choosing **WPA2-PSK**, you must enter WPA Pre-Shared Key and Group Rekey Interval.



Network Authentication:	WPA2 -PSK
Protected Management Frames:	Disabled
WPA/WAPI passphrase:	•••••••• Click here to display
WPA Group Rekey Interval:	3600
WPA/WAPI Encryption:	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.

6.11.3 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The VR-3033 has a WPS button on the device.

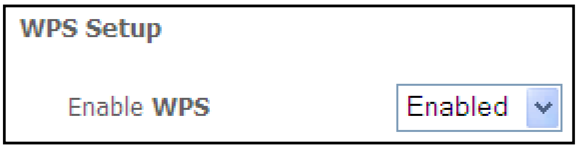
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".

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

To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

I. Setup

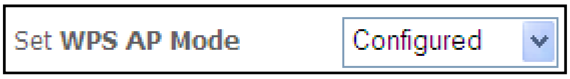
Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.



WPS Setup

Enable WPS: Enabled

Step 2: Set the WPS AP Mode. **Configured** is used when the VR-3033 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the VR-3033.

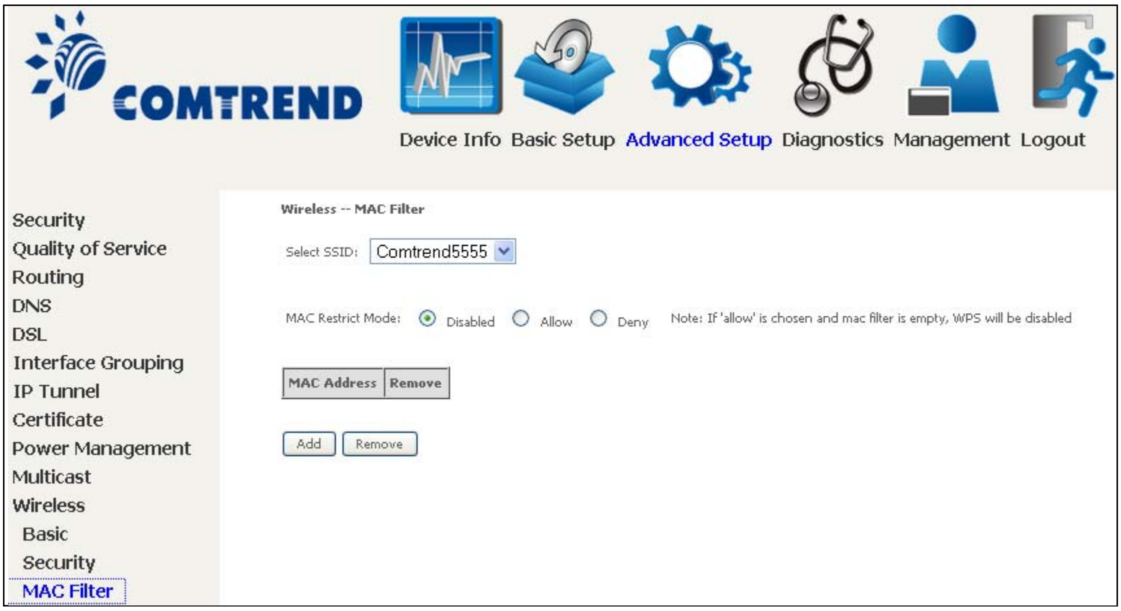


Set WPS AP Mode: Configured

NOTES: Your client may or may not have the ability to provide security settings to the VR-3033. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

6.11.4 MAC Filter

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



Wireless -- MAC Filter

Select SSID: Comtrend5555

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny Note: If 'allow' is chosen and mac filter is empty, WPS will be disabled

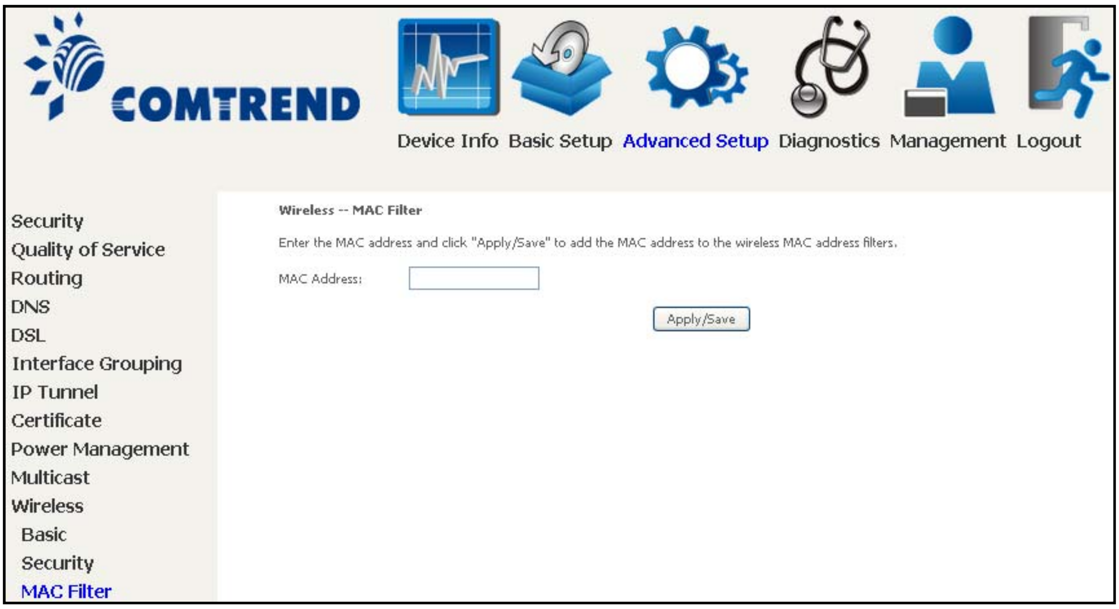
MAC Address	Remove

Add Remove

Option	Description
Select SSID	Select the wireless network name from the drop-down menu. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

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

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



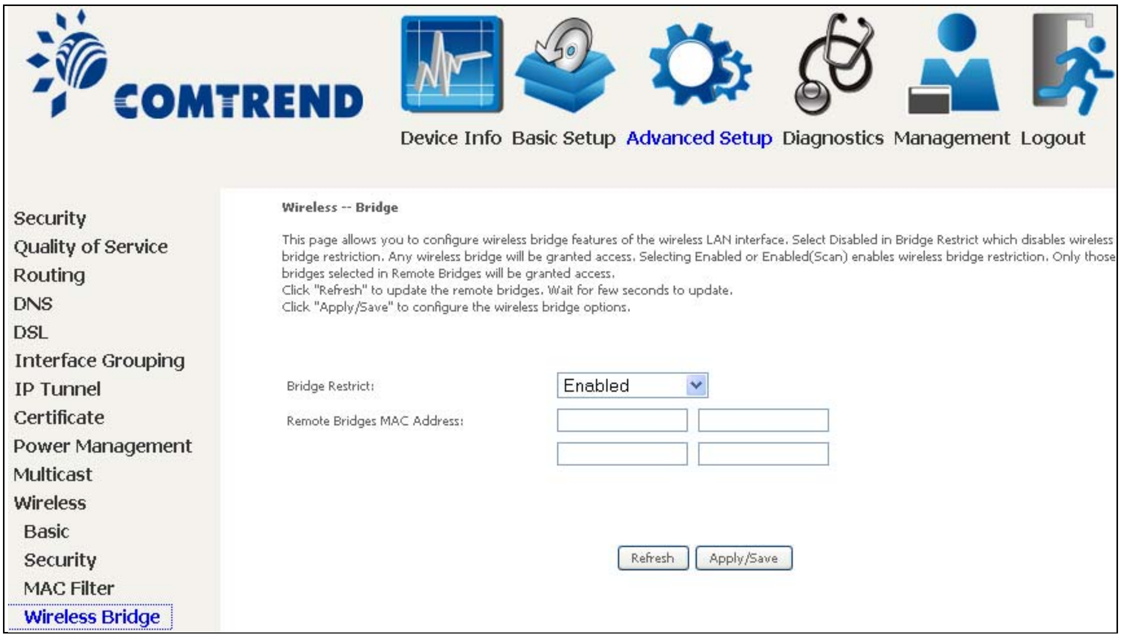
Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

6.11.5 Wireless Bridge

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



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

Bridge Restrict: Enabled

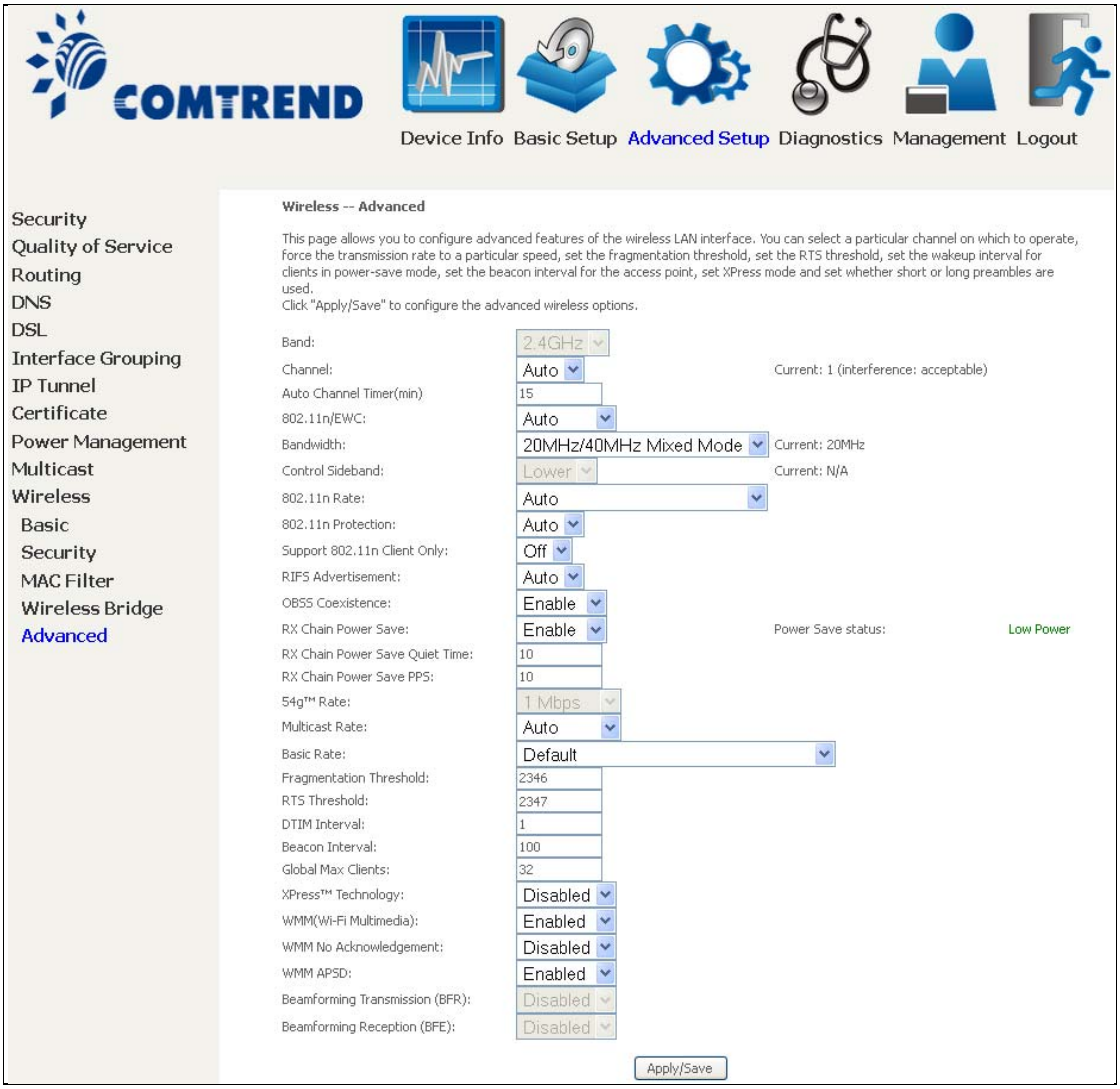
Remote Bridges MAC Address:

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

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

6.11.6 Advanced

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



Wireless -- Advanced

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

Band:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	15	
802.11n/EWC:	Auto	
Bandwidth:	20MHz/40MHz Mixed Mode	Current: 20MHz
Control Sideband:	Lower	Current: N/A
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Auto	
OBSS Coexistence:	Enable	
RX Chain Power Save:	Enable	Power Save status: Low Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	32	
XPress™ Technology:	Disabled	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	
Beamforming Transmission (BFR):	Disabled	
Beamforming Reception (BFE):	Disabled	

Field	**Description**
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz.
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)

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

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