

# VR-3030

## Multi-DSL Router

### User Manual



## Preface

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

## Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

### CAUTION:

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



### WARNING

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

## Copyright

Copyright©2019 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

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

## Protect Our Environment



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

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

# Table of Contents

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>5</b>
<b>CHAPTER 2 INSTALLATION.....</b>	<b>6</b>
2.1 HARDWARE SETUP.....	6
2.2 LED INDICATORS.....	8
<b>CHAPTER 3 WEB USER INTERFACE.....</b>	<b>9</b>
3.1 DEFAULT SETTINGS .....	9
3.2 IP CONFIGURATION.....	10
3.3 LOGIN PROCEDURE.....	12
<b>CHAPTER 4 DEVICE INFORMATION.....</b>	<b>14</b>
4.1 WAN .....	15
4.2 STATISTICS.....	16
4.2.1 LAN Statistics .....	16
4.2.2 WAN Service .....	17
4.2.3 XTM Statistics.....	18
4.2.4 xDSL Statistics.....	19
4.3 ROUTE .....	24
4.4 ARP.....	25
4.5 DHCP.....	25
4.6 NAT SESSION .....	27
4.7 IGMP PROXY .....	28
4.8 IPV6 .....	29
4.8.1 IPv6 Info.....	29
4.8.2 IPv6 Neighbor .....	30
4.8.3 IPv6 Route .....	31
4.9 NETWORK MAP .....	32
<b>CHAPTER 5 BASIC SETUP.....</b>	<b>33</b>
5.1 LAYER 2 INTERFACE .....	34
5.1.1 WAN Service Setup .....	35
5.2 NAT .....	36
5.2.1 Virtual Servers.....	36
5.2.2 Port Triggering.....	38
5.2.3 DMZ Host.....	40
5.2.4 IP Address Map .....	41
5.2.5 IPSEC ALG.....	42
5.2.6 SIP ALG.....	42
5.3 LAN.....	43
5.3.1 LAN IPv6 Autoconfig.....	46
5.3.2 Static IP Neighbor .....	49
5.3.3 UPnP .....	50
5.4 PARENTAL CONTROL.....	51
5.4.1 Time Restriction.....	51
5.4.2 URL Filter .....	52
<b>CHAPTER 6 ADVANCED SETUP.....</b>	<b>54</b>
6.1 AUTO-DETECTION SETUP .....	54
6.2 SECURITY .....	59
6.2.1 IP Filtering .....	59
6.2.2 MAC Filtering .....	62
6.3 QUALITY OF SERVICE (QoS).....	64
6.3.1 QoS Queue Setup.....	65
6.3.2 QoS Policer .....	67
6.3.3 QoS Classification.....	69
6.4 ROUTING .....	72



6.4.1 Default Gateway.....	72
6.4.2 Static Route.....	73
6.4.3 Policy Routing.....	74
6.4.4 RIP.....	75
6.5 DNS.....	76
6.5.1 DNS Server.....	76
6.5.2 Dynamic DNS.....	77
6.5.3 DNS Entries.....	78
6.5.4 DNS Proxy/Relay.....	79
6.6 DSL.....	80
6.7 IPTUNNEL.....	83
6.7.1 IPv6inIPv4.....	83
6.7.2 IPv4inIPv6.....	85
6.8 CERTIFICATE.....	86
6.8.1 Local.....	86
6.8.2 Trusted CA.....	88
6.9 POWER MANAGEMENT.....	89
6.10 MULTICAST.....	90
<b>CHAPTER 7 DIAGNOSTICS.....</b>	<b>92</b>
7.1 DIAGNOSTICS – INDIVIDUAL TESTS.....	92
7.2 FAULT MANAGEMENT.....	93
7.3 UPTIME STATUS.....	94
7.4 PING.....	95
7.5 TRACE ROUTE.....	96
7.6 SYSTEM UTILIZATION.....	97
<b>CHAPTER 8 MANAGEMENT.....</b>	<b>98</b>
8.1 SETTINGS.....	98
8.1.1 Backup Settings.....	98
8.1.2 Update Settings.....	99
8.1.3 Restore Default.....	100
8.2 SYSTEM LOG.....	101
8.3 SNMP AGENT.....	103
8.4 TR-069 CLIENT.....	104
8.5 INTERNET TIME.....	106
8.6 ACCESS CONTROL.....	107
8.6.1 Accounts.....	107
8.6.2 Service Access.....	109
8.6.3 IP Address.....	110
8.7 UPDATE SOFTWARE.....	111
8.8 REBOOT.....	112
<b>CHAPTER 9 LOGOUT.....</b>	<b>113</b>
<b>APPENDIX A - FIREWALL.....</b>	<b>114</b>
<b>APPENDIX B - PIN ASSIGNMENTS.....</b>	<b>117</b>
<b>APPENDIX C - SPECIFICATIONS.....</b>	<b>118</b>
<b>APPENDIX D - SSH CLIENT.....</b>	<b>120</b>
<b>APPENDIX E - CONNECTION SETUP.....</b>	<b>121</b>

## Chapter 1 Introduction

The VR-3030 is a Multi-DSL router that supports both ADSL2+ and VDSL2. The latter is a brand new standard and technology perfect for triple play (Video, Voice and Data) applications. The VR-3030 comes with one 10/100 Base-T Ethernet port.

The VR-3030 is a cost effective 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-3030 is cost effective for ISPs and carriers because deploying a single CPE DSL device with multiple profile support minimizes the number of required upgrades.

## Chapter 2 Installation

### 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.



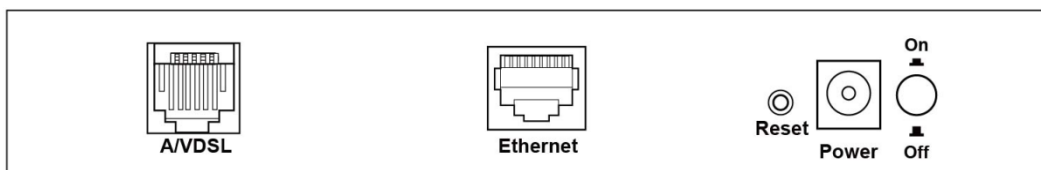
**DO NOT STACK**

#### **Non-stackable**

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

#### **BACK PANEL**

The figure below shows the back panel of the device.



#### **Power ON**

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

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

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

#### **Reset Button**

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

**NOTE:** If pressed down for more than 60 seconds, the VR-3030 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.

**Ethernet (LAN) Port**

Use a 10/100 BASE-T RJ-45 cable to connect to a network device. The ports is 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.

## 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.
ETHERNET	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
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**)

#### **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

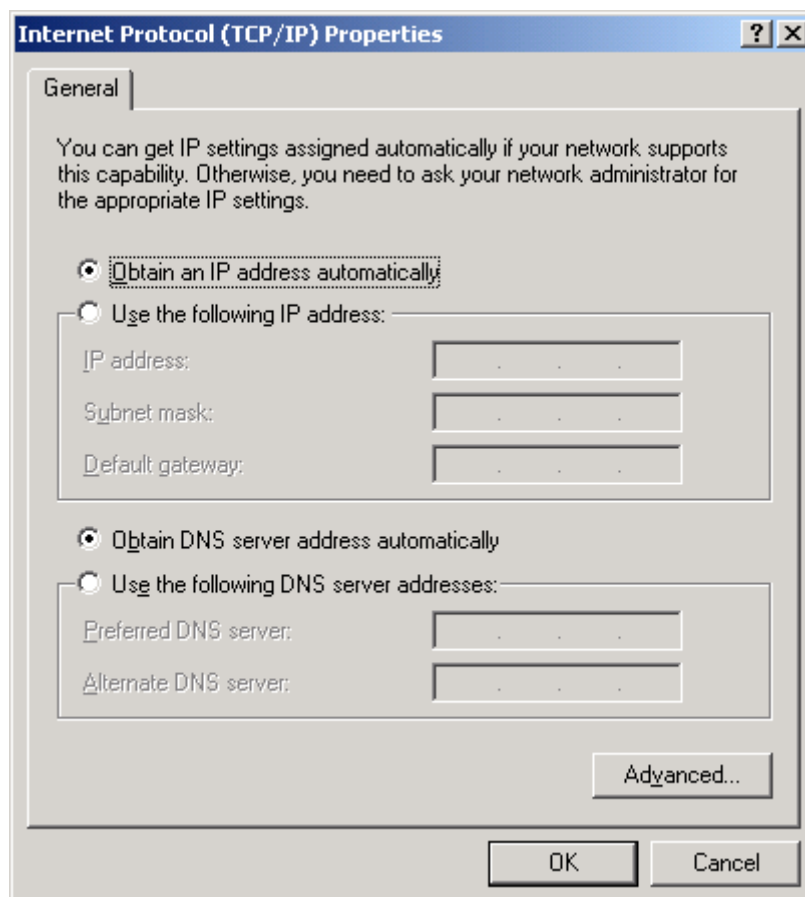
### DHCP MODE

When the VR-3030 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

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

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

- STEP 1:** From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the **Properties** button.
- STEP 2:** Select Internet Protocol (TCP/IP) **and click the** Properties button.
- STEP 3:** Select Obtain an IP address automatically as shown below.



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

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

## STATIC IP MODE

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

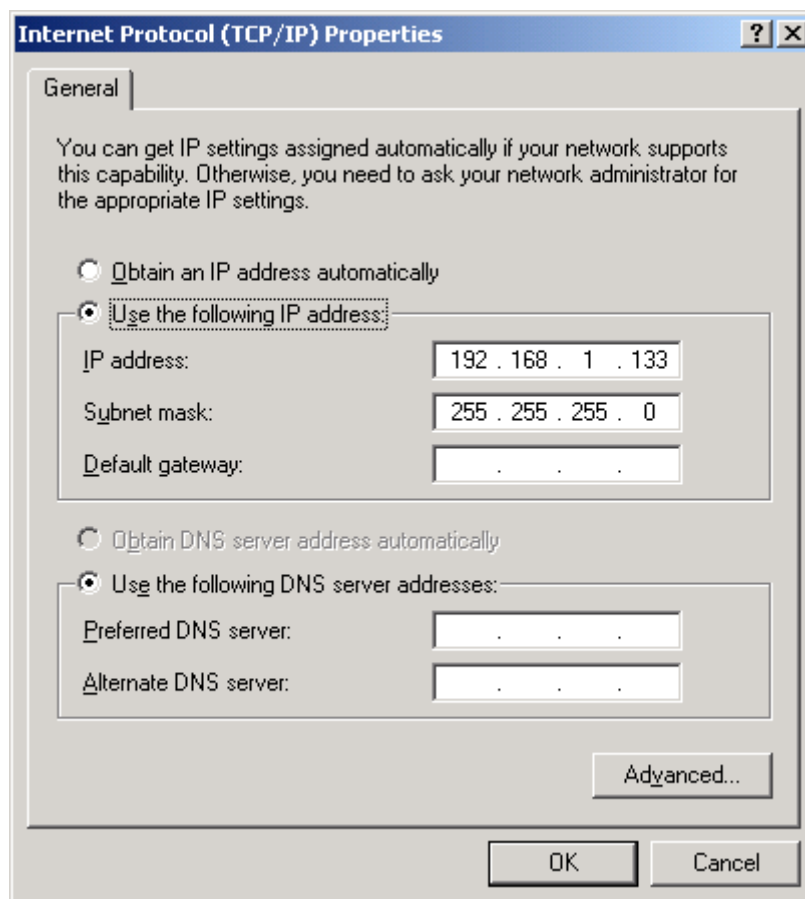
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



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



## 3.3 Login Procedure

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

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

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

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

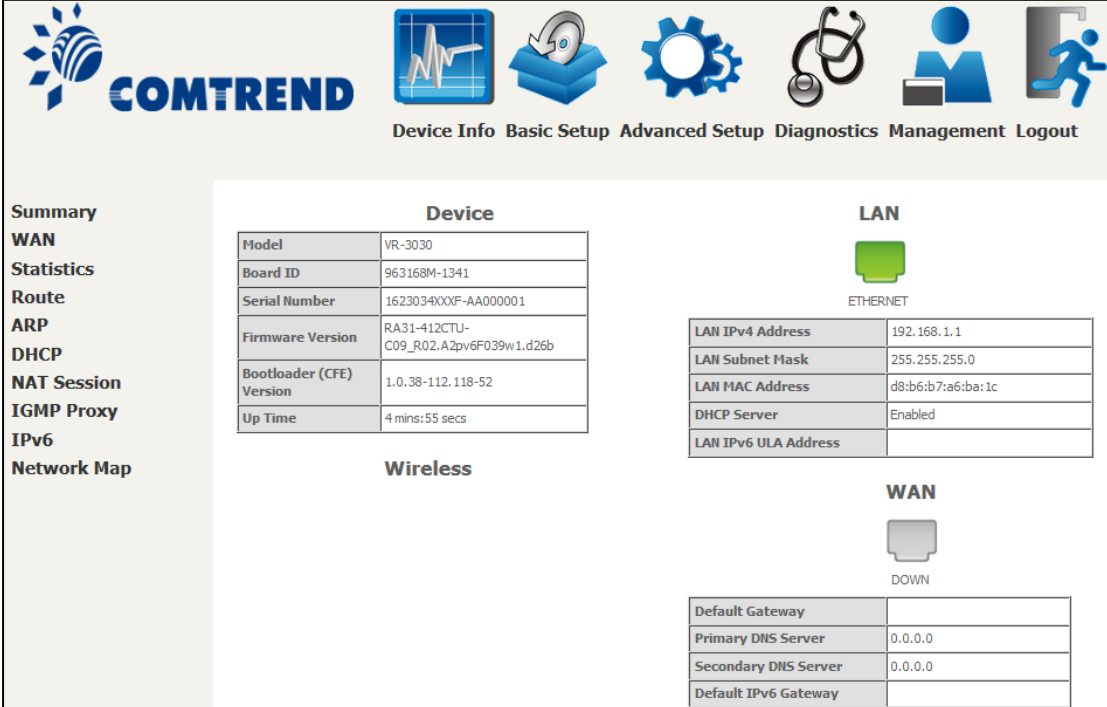
**STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in section [3.1 Default Settings](#).



Click **OK** to continue.

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

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



The screenshot shows the COMTREND web interface with the following navigation tabs: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area is divided into three sections:

- Device:** A table containing the following information:
 

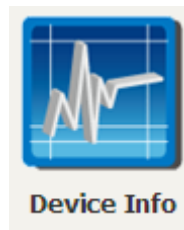
Model	VR-3030
Board ID	963168M-1341
Serial Number	162303400XF-AA00001
Firmware Version	RA31-412CTU-C09_R02.A2pv6F039w1.d26b
Bootloader (CFE) Version	1.0.38-112.118-52
Up Time	4 mins:55 secs
- LAN:** A section titled "ETHERNET" with a table of configuration details:
 

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:a6:ba:1c
DHCP Server	Enabled
LAN IPv6 ULA Address	
- WAN:** A section titled "DOWN" with a table of configuration details:
 

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

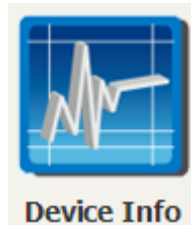
On the left side of the interface, there is a vertical menu with the following items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, and Network Map.

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.

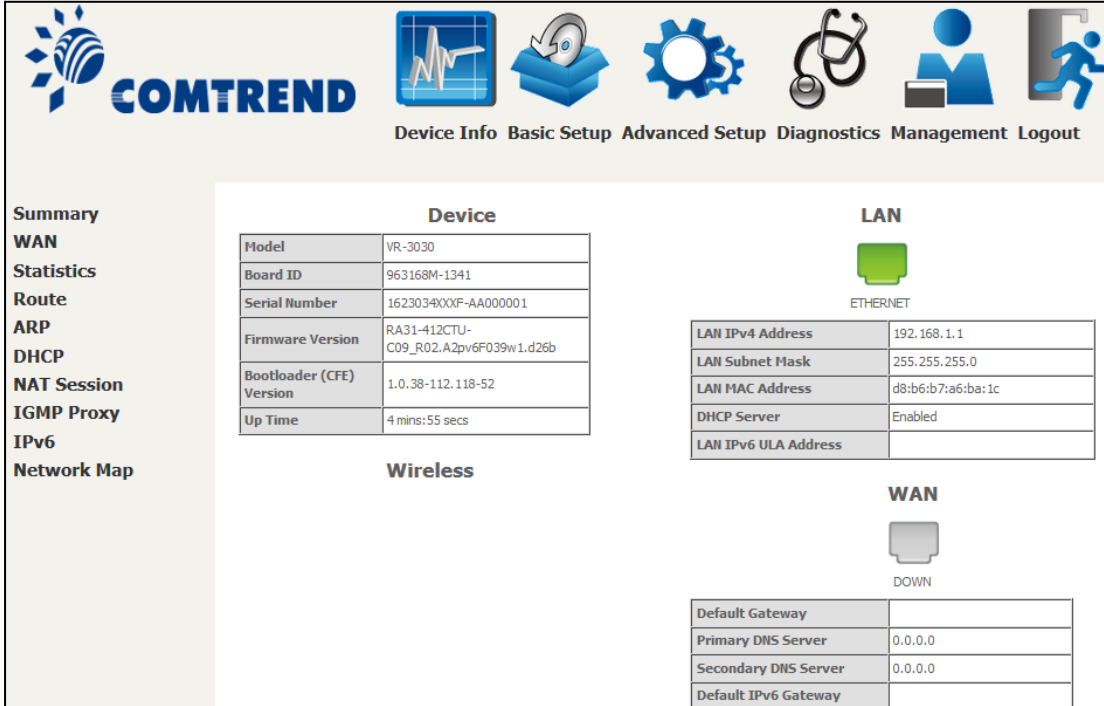


The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

**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.



The screenshot shows the Device Info Summary screen. At the top, there is a navigation bar with the COMTREND logo and icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area is divided into several sections:

- Summary:** A vertical list of menu items including WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, and Network Map.
- Device:** A table containing hardware and software information.
 

Model	VR-3030
Board ID	963168M-1341
Serial Number	162303400XF-AA000001
Firmware Version	RA31-412CTU-C09_R02.A2pv6F039w1.d26b
Bootloader (CFE) Version	1.0.38-112.118-52
Up Time	4 mins:55 secs
- Wireless:** A section for wireless network settings.
- LAN:** A section for LAN network settings, showing an Ethernet icon and a table of parameters.
 

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:a6:ba:1c
DHCP Server	Enabled
LAN IPv6 ULA Address	
- WAN:** A section for WAN network settings, showing a Down icon and a table of parameters.
 

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

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

## 4.1 WAN

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



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info (selected), Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with options: Summary, WAN (selected), Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, and Network Map. The main content area is titled 'WAN Info' and contains a table with the following columns: Interface, Description, Type, VlanMuxId, IPv6, Igmp, MLD, NAT, Firewall, Status, IPv4 Address, and IPv6 Address.

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

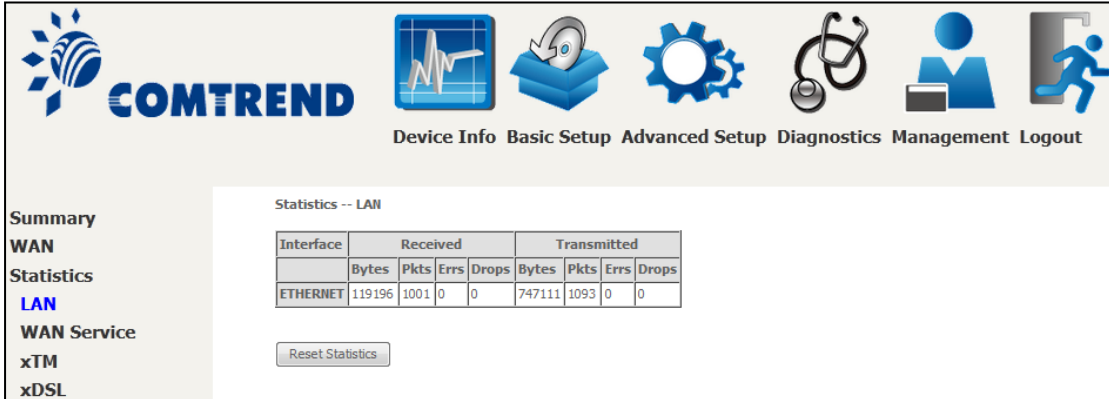
## 4.2 Statistics

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

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

### 4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



Summary  
WAN  
Statistics  
**LAN**  
WAN Service  
xTM  
xDSL

Statistics -- LAN


Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ETHERNET	119196	1001	0	0	747111	1093	0	0

Reset Statistics

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

## 4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.



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

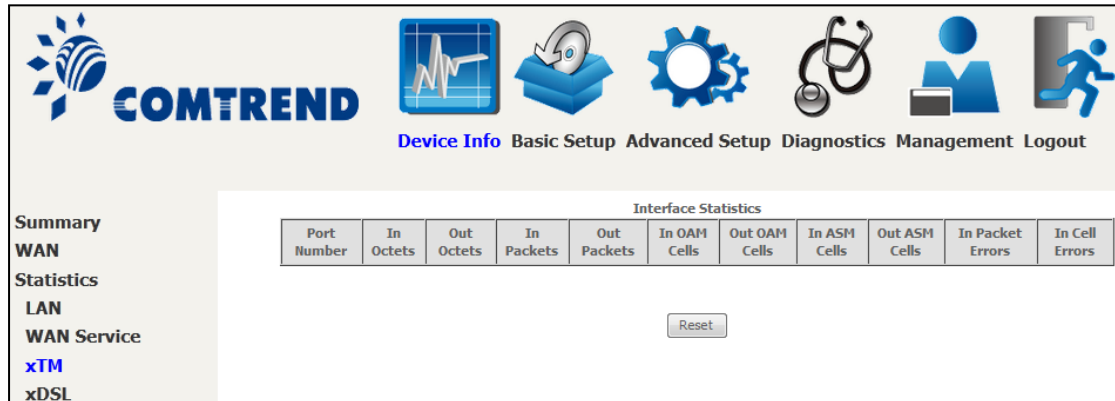
Statistics -- WAN

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

Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted	<ul style="list-style-type: none"> <li>- Bytes</li> <li>- Pkts</li> <li>- Errs</li> <li>- Drops</li> </ul>
	<ul style="list-style-type: none"> <li>Number of Bytes</li> <li>Number of Packets</li> <li>Number of packets with errors</li> <li>Number of dropped packets</li> </ul>

### 4.2.3 XTM Statistics

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




### ATM Interface Statistics







Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error

## 4.2.4 xDSL Statistics

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

### VDSL



[Device Info](#) [Basic Setup](#) [Advanced Setup](#) [Diagnostics](#) [Management](#) [Logout](#)

Summary

**WAN**

Statistics

LAN

WAN Service

xTM

**xDSL**

Route

ARP

DHCP

NAT Session

IGMP Proxy

IPv6

Network Map

Statistics -- xDSL


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):		159	70
Attenuation (0.1 dB):		56	0
Output Power (0.1 dBm):		145	86
Attainable Rate (Kbps):		148882	60897
		Path 0	
		Downstream	Upstream
Rate (Kbps):		99999	59999
B (# of bytes in Mux Data Frame):		79	239
M (# of Mux Data Frames in an RS codeword):		1	1
T (# of Mux Data Frames in an OH sub-frame):		59	64
R (# of redundancy bytes in the RS codeword):		16	0
S (# of data symbols over which the RS code word spans):		0.0255	0.1273
L (# of bits transmitted in each data symbol):		30168	15081
D (interleaver depth):		631	1
I (interleaver block size in bytes):		96	120
N (RS codeword size):		96	240
Delay (msec):		4	0
INP (DMT symbol):		1.00	0.00
OH Frames:		467768	258286
OH Frame Errors:		472	1
RS Words:		82639186	3736256
RS Correctable Errors:		3	0
RS Uncorrectable Errors:		0	0
HEC Errors:		7	0
OCD Errors:		0	0
LCD Errors:		0	0
Total Cells:		101728747	0
Data Cells:		196	0
Bit Errors:		0	0
Total ES:		12	1
Total SES:		11	0
Total UAS:		153	142







19

Leading the **Communication Trend**



**ADSL**



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary

**WAN**

Statistics

LAN

WAN Service

xTM

**xDSL**

Route

ARP

DHCP

NAT Session

IGMP Proxy

IPv6

Network Map

Statistics -- xDSL

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):	71	71
Attenuation (0.1 dB):	15	31
Output Power (0.1 dBm):	57	120
Attainable Rate (Kbps):	27008	1199
	Path 0	
	Downstream	Upstream
Rate (Kbps):	27387	1199
MSGc (# of bytes in overhead channel message):	51	11
B (# of bytes in Mux Data Frame):	243	74
M (# of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	4	2
R (# of check bytes in FEC Data Frame):	0	0
S (ratio of FEC over PMD Data Frame length):	0.2847	1.9867
L (# of bits in PMD Data Frame):	6854	302
D (interleaver depth):	1	1
Delay (msec):	0	0
INP (DMT symbol):	0.00	0.00
Super Frames:	0	0
Super Frame Errors:	0	0
RS Words:	0	159087
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	5182956	215701
Data Cells:	0	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	119	119

xDSL BER Test
Reset Statistics
Draw Graph

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

Field	Description
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+
Traffic Type	Channel type Interleave or Fast
Status	Lists the status of the DSL link
Link Power State	Link output power state
PhyR Status	The Status of the BCM physical layer re-transmission technology
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

20

Leading the **Communication Trend**

Field	Description
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain
Rate (Kbps)	Current sync rates downstream/upstream

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

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

**In ADSL2+ 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 FEC Data Frame
T	Mux Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

**In G.DMT mode, the following section is inserted.**

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors

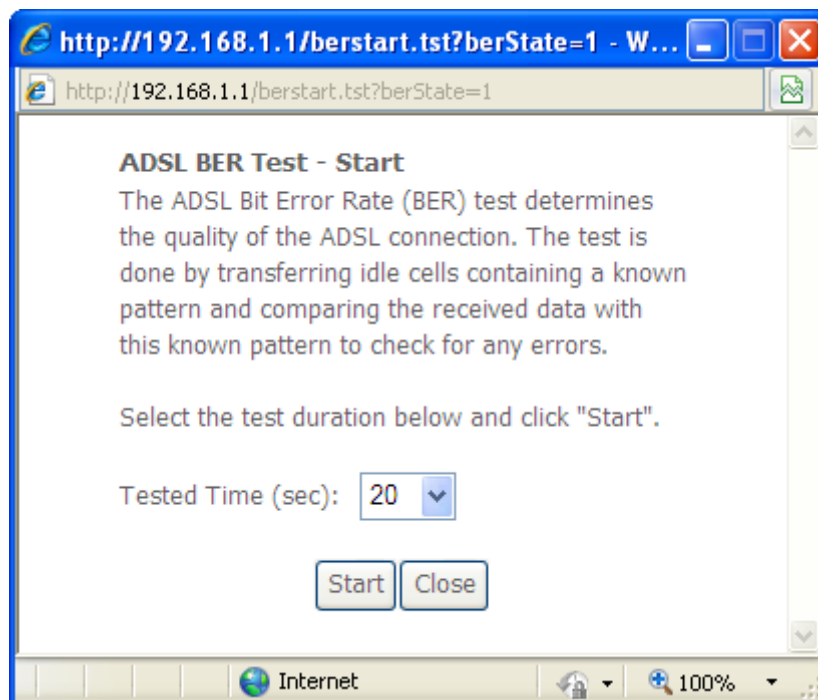
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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

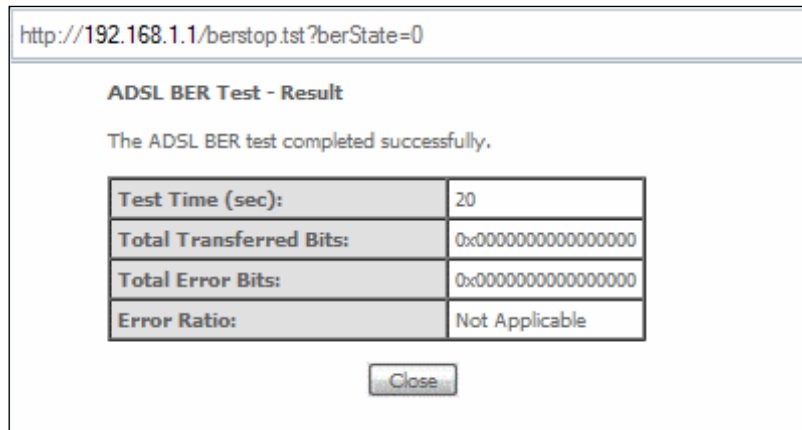
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

### xDSL BER TEST

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



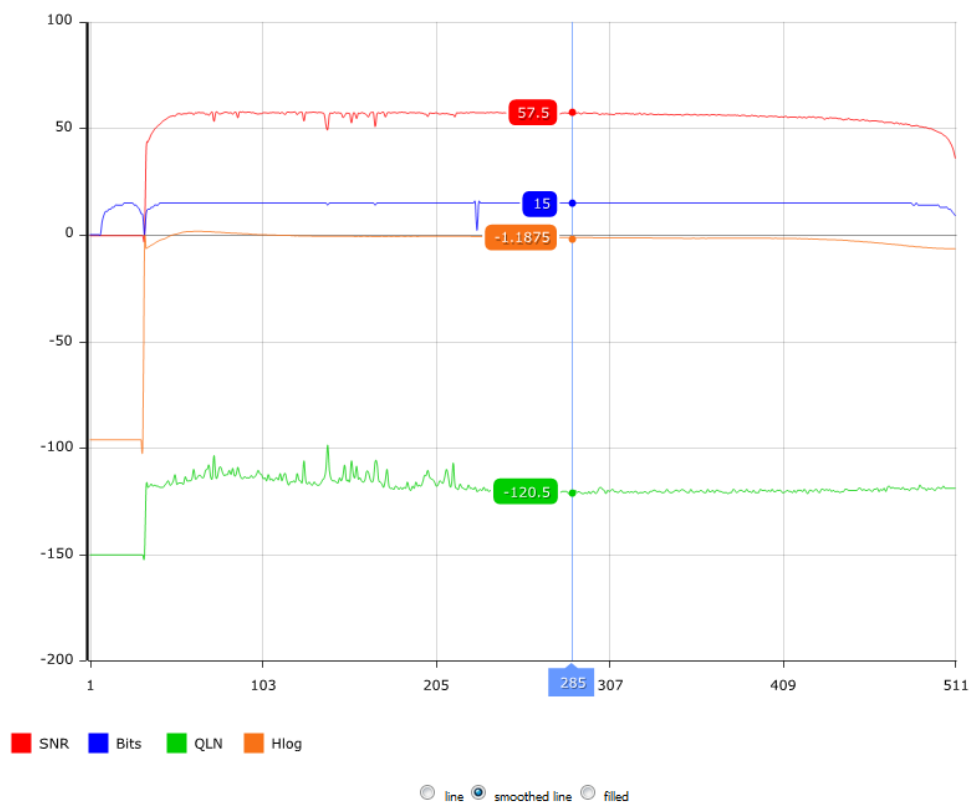
Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



### xDSL TONE GRAPH

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

**DSL Line Statistics**



## 4.3 Route

Choose **Route** to display the routes that the VR-3030 has found.



Summary  
WAN  
Statistics  
**Route**  
ARP  
DHCP  
NAT Session  
IGMP Proxy  
IPv6

Device Info -- Route

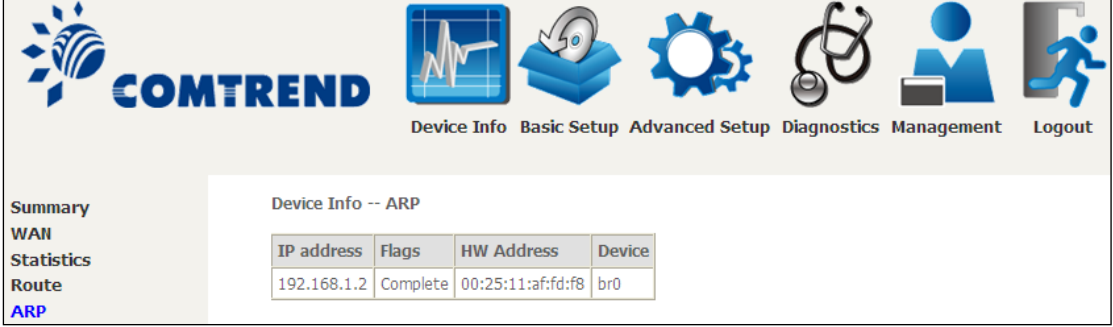
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

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.



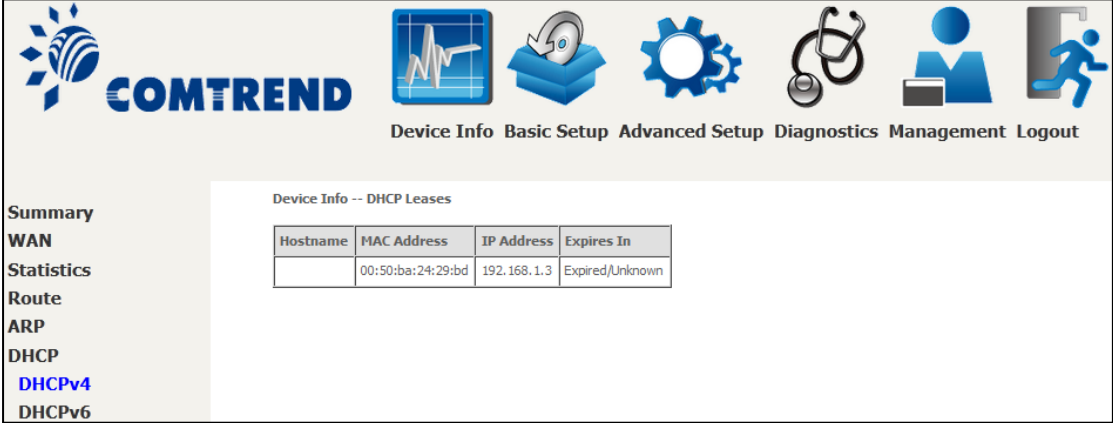
The screenshot shows the COMTREND web interface with a navigation menu at the top: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left sidebar, the menu items are Summary, WAN, Statistics, Route, and ARP (highlighted in blue). The main content area displays 'Device Info -- ARP' with the following table:

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

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

## 4.5 DHCP

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



The screenshot shows the COMTREND web interface with the same navigation menu. On the left sidebar, the menu items are Summary, WAN, Statistics, Route, ARP, DHCP, DHCPv4 (highlighted in blue), and DHCPv6. The main content area displays 'Device Info -- DHCP Leases' with the following table:

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

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



Device Info -- DHCPv6 Leases

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

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

## 4.6 NAT Session

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



**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

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


**NAT Session**

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

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout

Refresh Show All

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	57655	192.168.1.1	80	tcp	431999

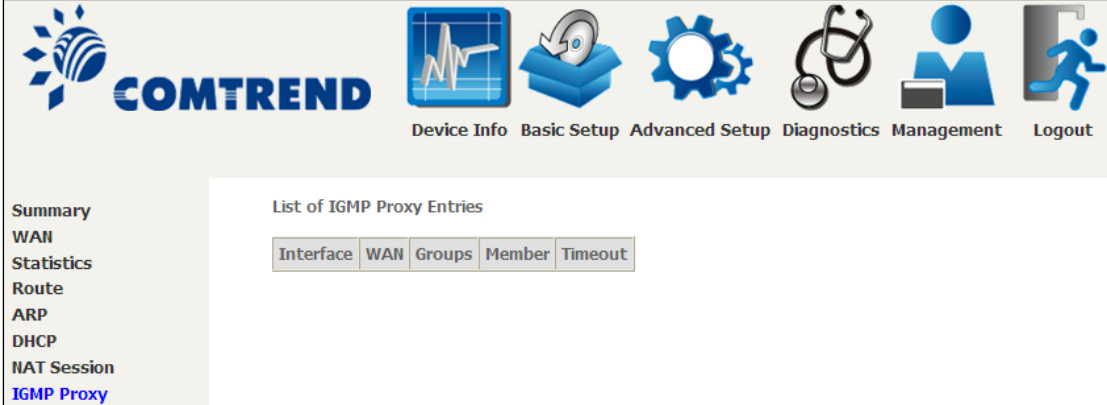
Refresh Show Less

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



## 4.7 IGMP Proxy

Click **IGMP Proxy** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.

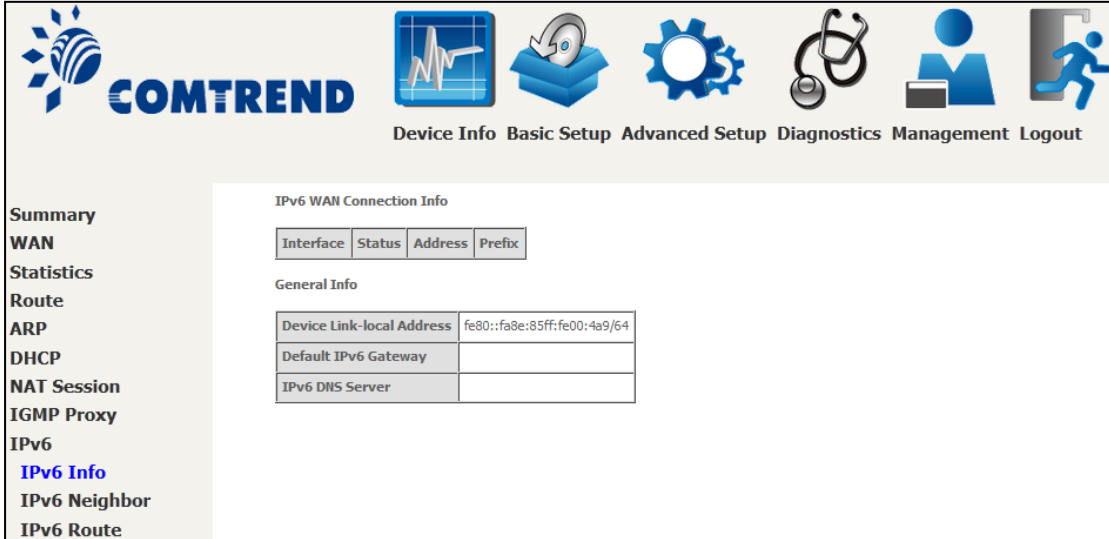


Field	Description
Interface	The Source interface from which the IGMP report was received
WAN	The WAN interface from which the multicast traffic is received
Groups	The destination IGMP group address
Member	The Source IP from which the IGMP report was received
Timeout	The time remaining before the IGMP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

## 4.8 IPv6

### 4.8.1 IPv6 Info

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



**COMTREND**

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary  
 WAN  
 Statistics  
 Route  
 ARP  
 DHCP  
 NAT Session  
 IGMP Proxy  
 IPv6  
**IPv6 Info**  
 IPv6 Neighbor  
 IPv6 Route

IPv6 WAN Connection Info

Interface	Status	Address	Prefix


General Info

Device Link-local Address	fe80::fa8e:85ff:fe00:4a9/64
Default IPv6 Gateway	
IPv6 DNS Server	

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

## 4.8.2 IPv6 Neighbor

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

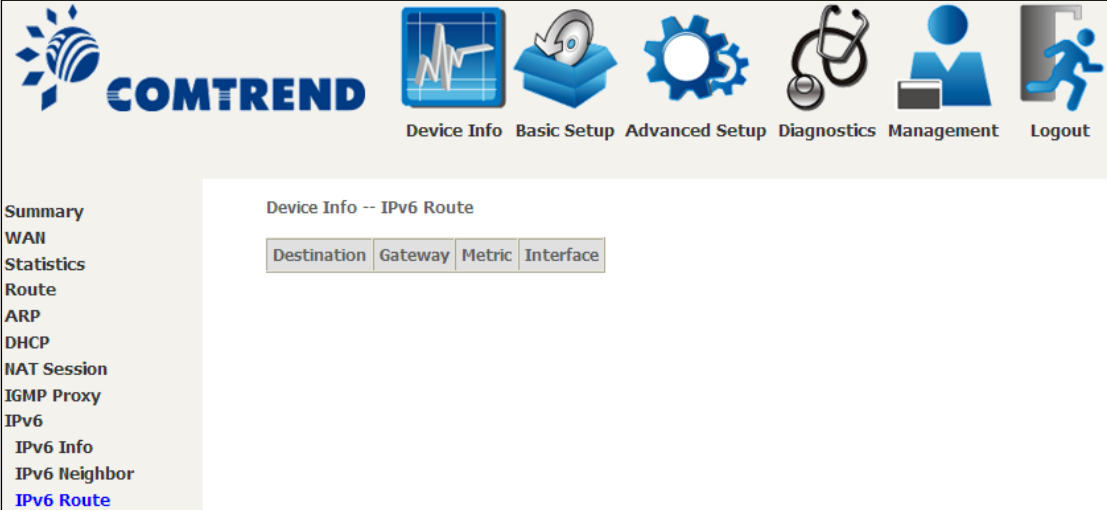


The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options like Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, IPv6 Info, **IPv6 Neighbor**, and IPv6 Route. The main content area displays the title "Device Info -- IPv6 Neighbor Discovery table" and a table with the following columns: IPv6 address, Flags, HW Address, and Device.

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

### 4.8.3 IPv6 Route

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

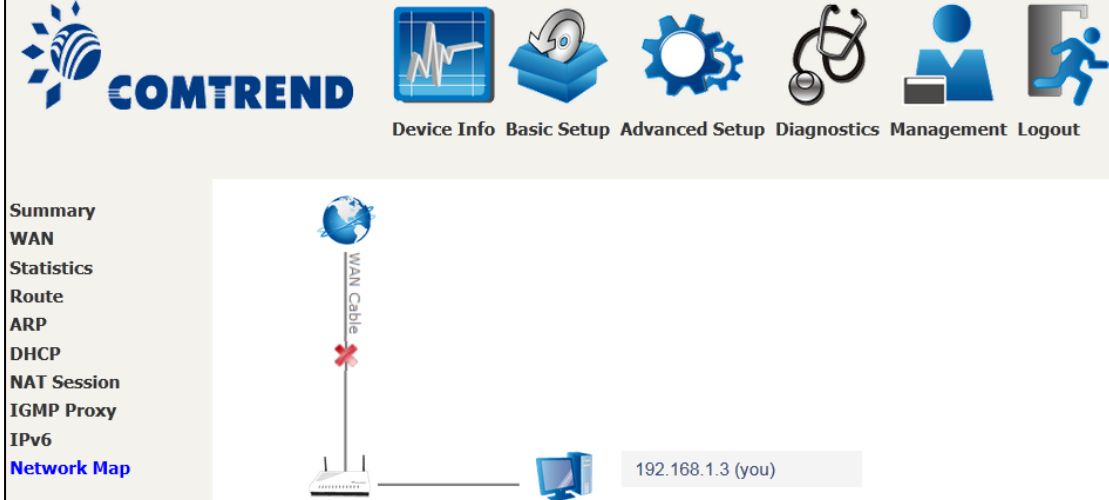


Field	Description
Destination	Destination IP Address
Gateway	Gateway address used for destination IP
Metric	Metric specified for gateway
Interface	Interface used for destination IP

## 4.9 Network Map

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

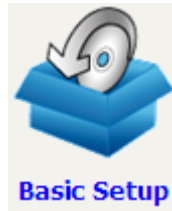
Note: This graph is unavailable for Internet Explorer users.



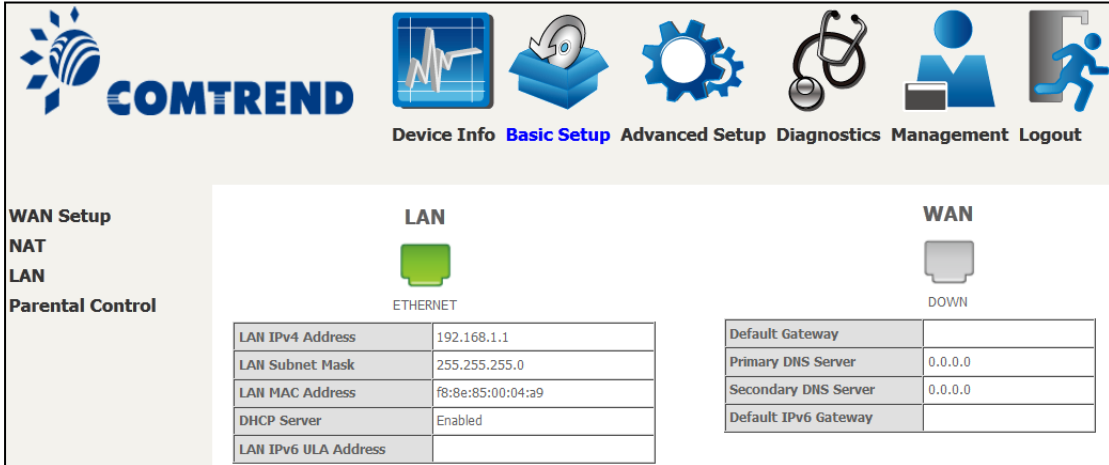
The screenshot displays the COMTREND web interface for the Network Map. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below this, a left-hand navigation menu lists various system status options: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, and Network Map (which is highlighted in blue). The main content area shows a network diagram. On the left, a router icon is connected to a computer icon on the right. The computer icon is labeled with the IP address '192.168.1.3 (you)'. A vertical line labeled 'WAN Cable' connects the router to the top of the page, with a red 'X' mark indicating a disconnected or error state.

## 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.



**COMTREND**

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

**WAN Setup**  
**NAT**  
**LAN**  
**Parental Control**

**LAN**  
 ETHERNET

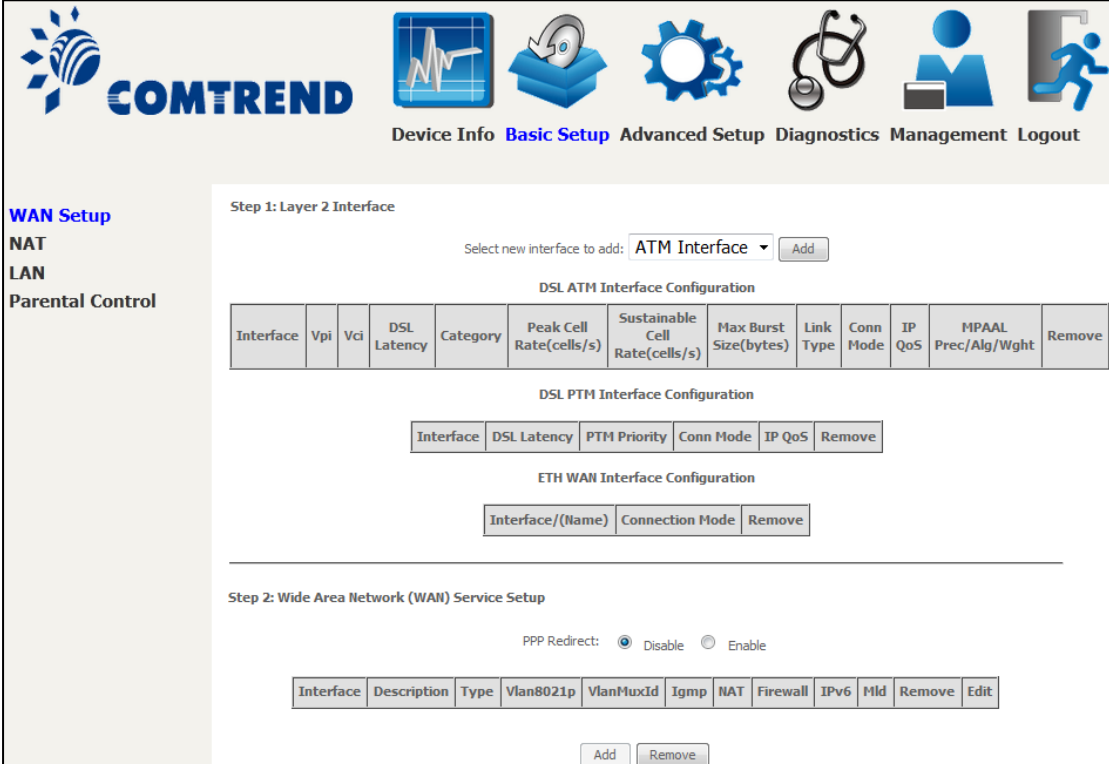
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:00:04:a9
DHCP Server	Enabled
LAN IPv6 ULA Address	

**WAN**  
 DOWN

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

## 5.1 Layer 2 Interface

Click WAN Setup on the on the left of your screen.  
Add or remove ATM, PTM and ETH WAN interface connections here.



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

**WAN Setup**  
NAT  
LAN  
Parental Control

Step 1: Layer 2 Interface

Select new interface to add: ATM Interface

DSL ATM Interface Configuration

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
DSL PTM Interface Configuration												
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove							
ETH WAN Interface Configuration												
Interface/(Name)	Connection Mode	Remove										

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect:  Disable  Enable

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

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

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

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

### 5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

**Step 2: Wide Area Network (WAN) Service Setup**

PPP Redirect:  Disable  Enable

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

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

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

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

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



## 5.2 NAT

To display this option, NAT must be enabled in at least one PVC.

### 5.2.1 Virtual Servers

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



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

**WAN Setup**  
**NAT**  
[Virtual Servers](#)  
 Port Triggering  
 DMZ Host  
 IP Address Map  
 IPSEC ALG  
 SIP ALG

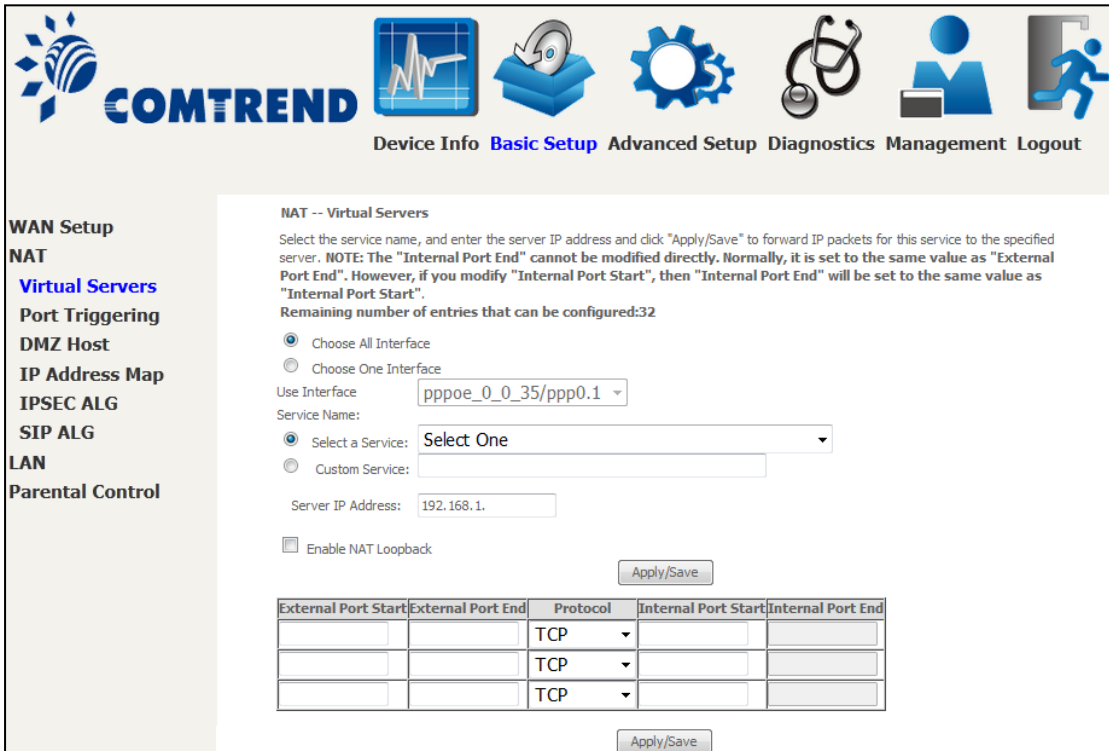
**NAT -- Virtual Servers Setup**

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

Add Remove

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

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



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

**WAN Setup**  
**NAT**  
[Virtual Servers](#)  
 Port Triggering  
 DMZ Host  
 IP Address Map  
 IPSEC ALG  
 SIP ALG  
**LAN**  
 Parental Control

**NAT -- Virtual Servers**

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

Remaining number of entries that can be configured:32

Choose All Interface  
 Choose One Interface

Use Interface:

Service Name:  
 Select a Service:   
 Custom Service:

Server IP Address:

Enable NAT Loopback

Apply/Save

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

Apply/Save

Consult the table below for field and header descriptions.

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

## 5.2.2 Port Triggering

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



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

**WAN Setup**  
**NAT**  
 Virtual Servers  
**Port Triggering**  
 DMZ Host  
 IP Address Map  
 IPSEC ALG  
 SIP ALG  
 LAN

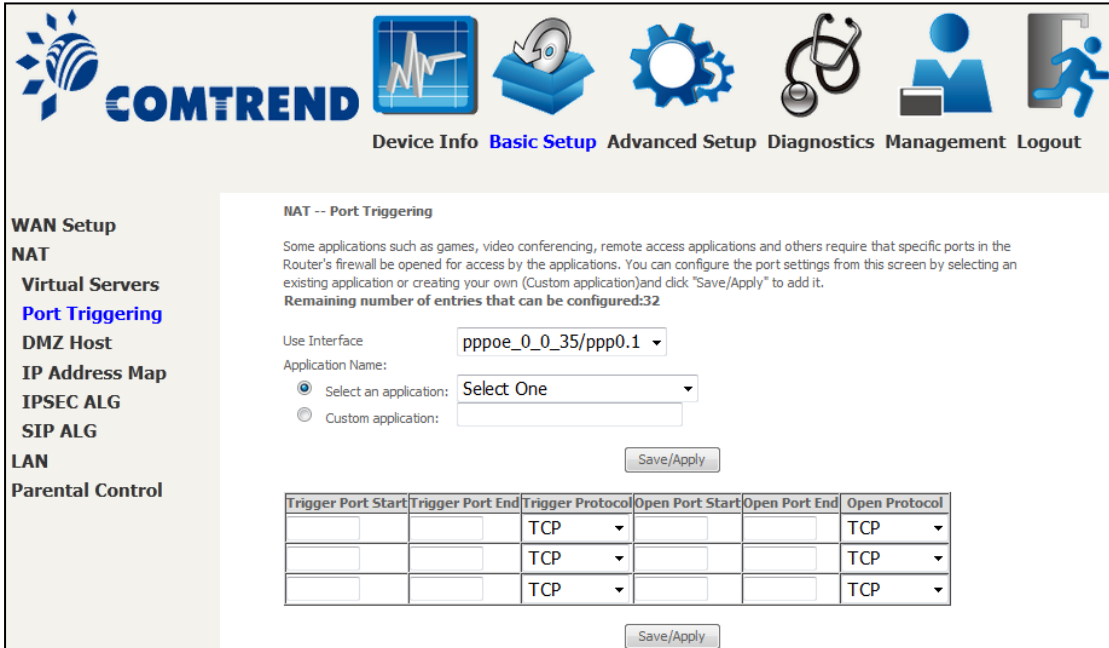
**NAT -- Port Triggering Setup**

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

Add Remove

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

To add a Trigger Port, click **Add**. The following will be displayed.



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

**WAN Setup**  
**NAT**  
 Virtual Servers  
**Port Triggering**  
 DMZ Host  
 IP Address Map  
 IPSEC ALG  
 SIP ALG  
 LAN  
 Parental Control

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.  
 Remaining number of entries that can be configured:32

Use Interface:

Application Name:  
 Select an application:   
 Custom application:

Save/Apply

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

Save/Apply

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

Consult the table below for field and header descriptions.

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

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

### 5.2.3 DMZ Host

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



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, the main content area is titled "NAT -- DMZ Host". It contains the following text: "The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer." Below this, there are two instructions: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." There is a text input field labeled "DMZ Host IP Address:" and a checkbox labeled "Enable NAT Loopback". A "Save/Apply" button is located at the bottom right of the form.

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

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

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

## 5.2.4 IP Address Map

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



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

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



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

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

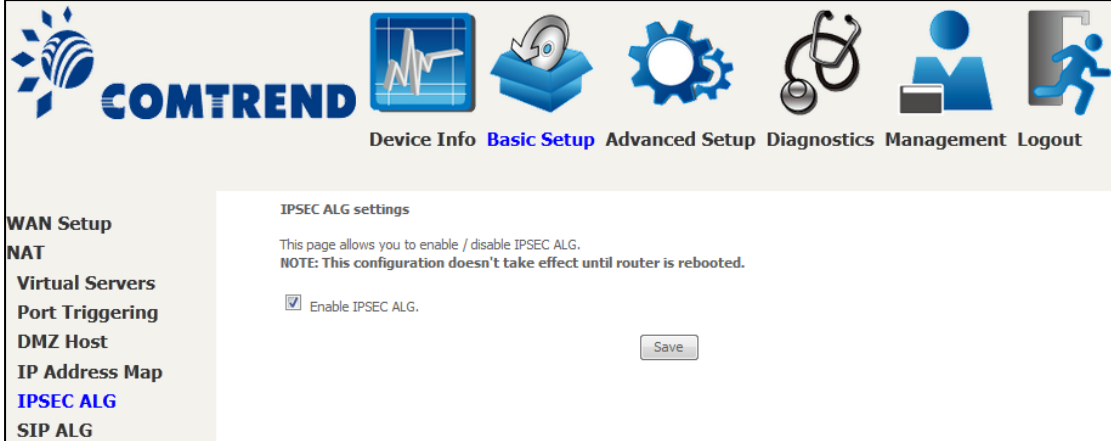
**Many to one:** mapping a range of local IP to a specific public IP

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

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

## 5.2.5 IPSEC ALG

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



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of menu items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG (highlighted), and SIP ALG. The main content area is titled "IPSEC ALG settings" and contains the following text: "This page allows you to enable / disable IPSEC ALG. NOTE: This configuration doesn't take effect until router is rebooted." Below this text, there is a checkbox labeled "Enable IPSEC ALG." which is checked. To the right of the checkbox is a "Save" button.

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

## 5.2.6 SIP ALG

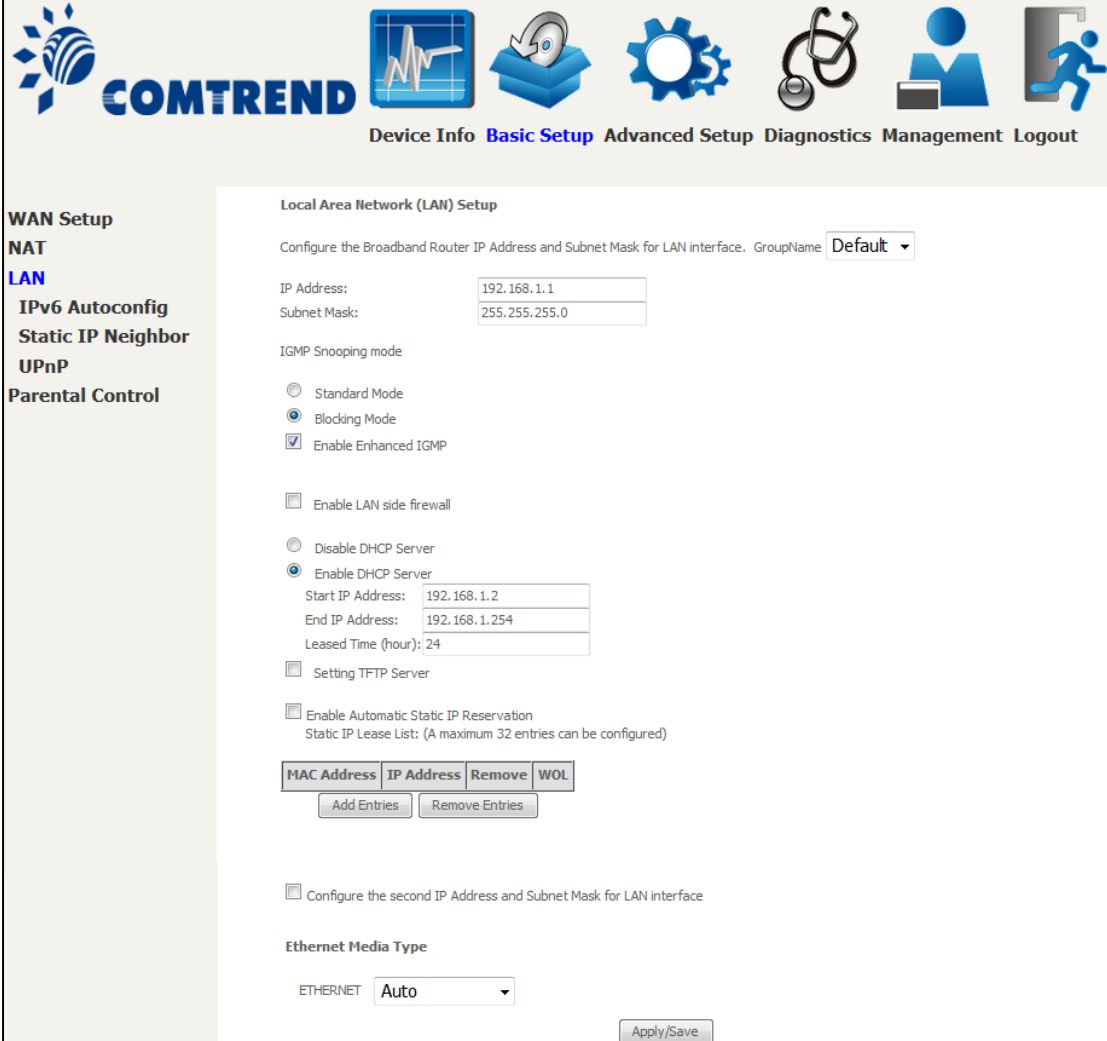
This page allows you to enable / disable SIP ALG.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of menu items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG, and SIP ALG (highlighted). The main content area is titled "SIP ALG settings" and contains the following text: "This page allows you to enable / disable SIP ALG. NOTE: This configuration doesn't take effect until router is rebooted." Below this text, there is a checkbox labeled "Enable SIP ALG." which is checked. To the right of the checkbox is a "Save" button.

## 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:

IP Address:

Subnet Mask:

IGMP Snooping mode

Standard Mode

Blocking Mode

Enable Enhanced IGMP

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Setting TFTP Server

Enable Automatic Static IP Reservation

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

MAC Address	IP Address	Remove	WOL

Configure the second IP Address and Subnet Mask for LAN interface

**Ethernet Media Type**

ETHERNET:

Consult the field descriptions below for more details.

**GroupName:** Select an Interface Group.

### 1<sup>st</sup> LAN INTERFACE

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

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

### **IGMP Snooping:**

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



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

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

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

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

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

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

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

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

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

**DHCP Static IP Lease**

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

MAC Address:

IP Address:

Enable Wake On Lan.

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

MAC Address	IP Address	Remove	WOL
12:34:56:78:90:12	192.168.1.33	<input checked="" type="checkbox"/>	Disable
<input type="button" value="Add Entries"/>		<input type="button" value="Remove Entries"/>	

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

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

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

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

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

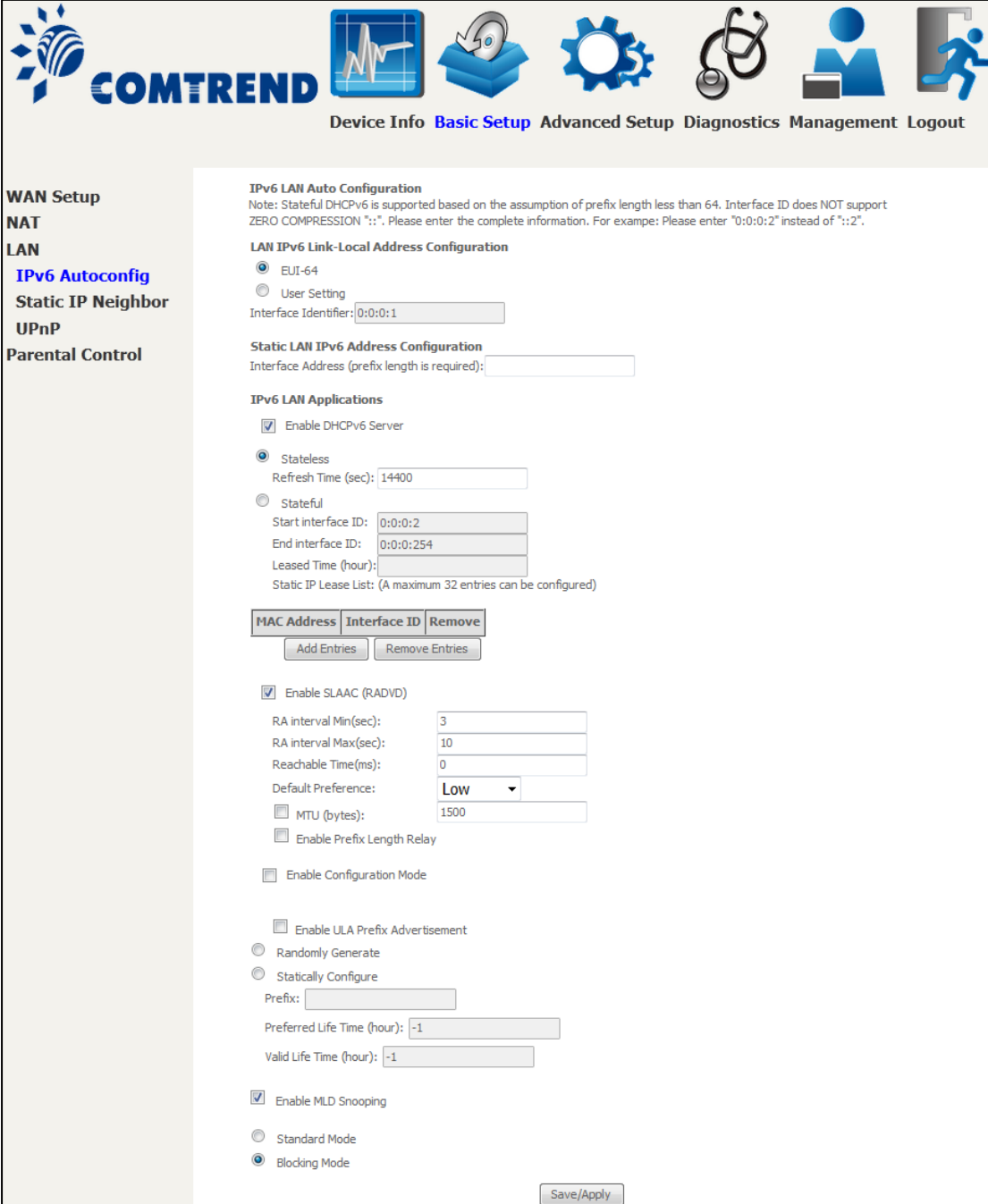
### **Ethernet Media Type:**

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

Auto	▼
Auto	
10Mbps-Half	
10Mbps-Full	
100Mbps-Half	
100Mbps-Full	

### 5.3.1 LAN IPv6 Autoconfig

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



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

**LAN IPv6 Link-Local Address Configuration**

- EUI-64
- User Setting

Interface Identifier:

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

**IPv6 LAN Applications**

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

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

- Enable SLAAC (RADVD)  
 RA interval Min(sec):   
 RA interval Max(sec):   
 Reachable Time(ms):   
 Default Preference:
- MTU (bytes):
- Enable Prefix Length Relay
- Enable Configuration Mode
- Enable ULA Prefix Advertisement
- Randomly Generate
- Statically Configure  
 Prefix:   
 Preferred Life Time (hour):   
 Valid Life Time (hour):
- Enable MLD Snooping
- Standard Mode
- Blocking Mode

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

Heading	Description
User Setting	Use the Interface Identifier field to define a link-local address

### Static LAN IPv6 Address Configuration

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

### IPv6 LAN Applications

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

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

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

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

**DHCP Static IP Lease**

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

MAC Address:

Interface ID:

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

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

Heading	Description
<b>Enable RADVD</b>	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable Configuration Mode	Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure	Specify the prefix to be used
Prefix	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports
Standard Mode Blocking Mode	<p>In standard mode, IPv6 multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if MLD snooping is enabled</p> <p>In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group</p>

### 5.3.2 Static IP Neighbor

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



Click the Add button to display the following.




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

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

### 5.3.3 UPnP

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



**COMTREND**

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

WAN Setup  
NAT  
LAN  
IPv6 Autoconfig  
Static IP Neighbor  
**UPnP**  
Parental Control

UPnP Configuration

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

Enable UPnP

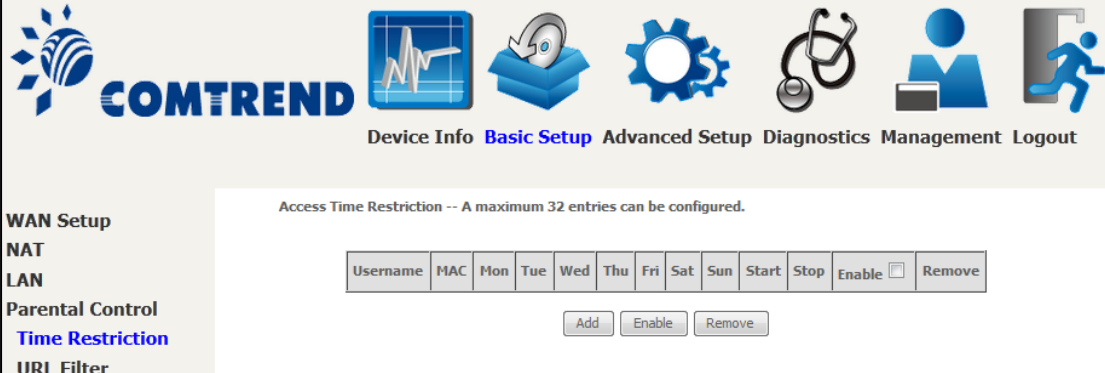
Apply/Save

## 5.4 Parental Control

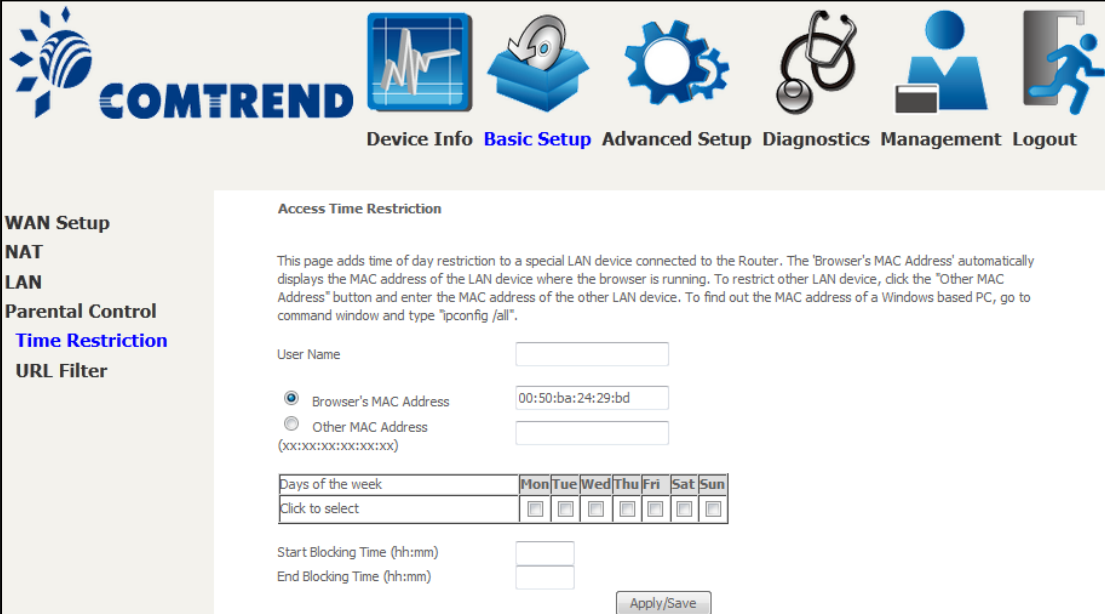
This selection provides WAN access control functionality.

### 5.4.1 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.



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



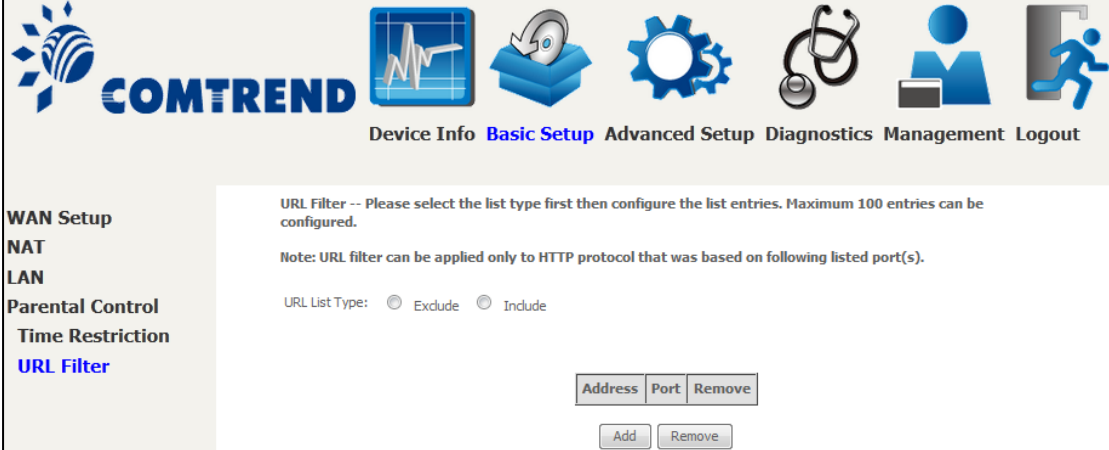
See below for field descriptions. Click **Apply/Save** to add a time restriction.

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



## 5.4.2 URL Filter

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

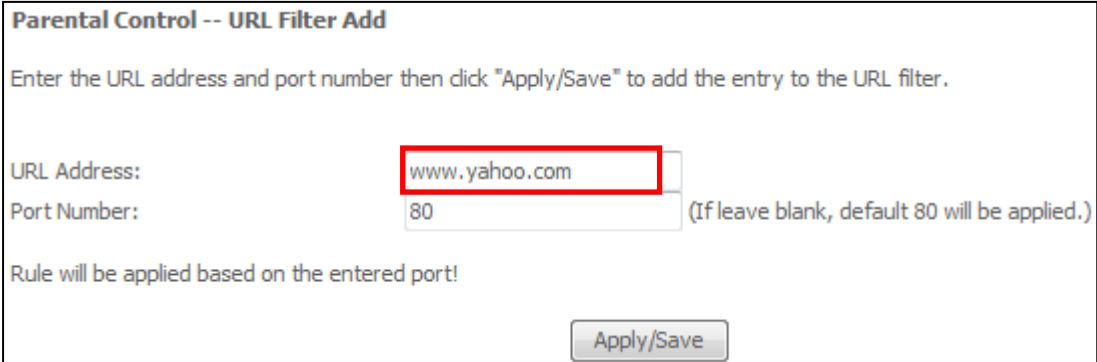


Select URL List Type: Exclude or Include.

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

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

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



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

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

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

URL List Type:  Exclude  Include

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

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

## Chapter 6 Advanced Setup

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










### 6.1 Auto-detection setup

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

A screenshot of the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with options: Auto-Detection (highlighted), Security, Quality of Service, Routing, DNS, DSL, IP Tunnel, Certificate, Power Management, and Multicast. The main content area is titled "Auto-detection setup" and contains the following text: "The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface when applicable. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function." Below the text, there is a checkbox labeled "Enable auto-detect" which is currently unchecked. At the bottom right of the main content area, there are two buttons: "Apply/Save" and "Restart".

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



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection

Security

Quality of Service

Routing

DNS

DSL

IP Tunnel

Certificate

Power Management

Multicast

### Auto-detection setup

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

Enable auto-detect

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

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

PPP Username:

PPP Password:

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

Select Service ATM ▾

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

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

PPP Username:

PPP Password:

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

55  
Leading the **Communication Trend**

Select Service

ATM ▾

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

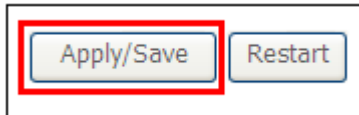
**WAN services list for ATM mode:** A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement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

Select Service

PTM/ETHWAN ▾

VLAN ID[0-4094]	Service
-1	Disable ▾
-1	PPPoE IPoE Disable
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Default Bridge ▾

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



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

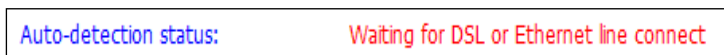
**Options for each WAN service:** These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

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

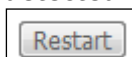
VLAN ID[0-4094]	Service	Option
-1	PPPoE	<input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

### Auto Detection status and Restart

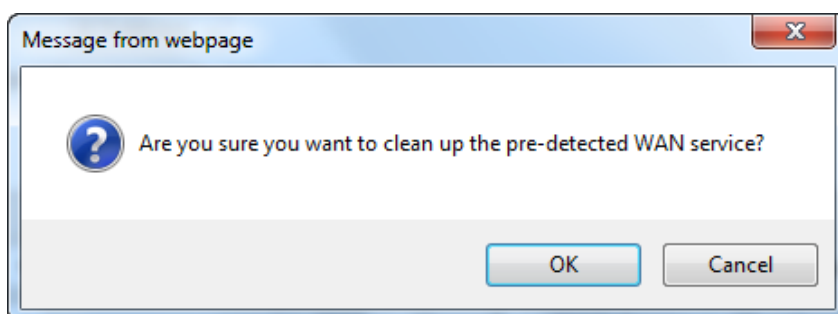
The Auto-detection status is used to display the real time status of the Auto-detection feature.



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



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



### Auto Detection notice

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

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

## 6.2 Security

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

### 6.2.1 IP Filtering

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

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

#### OUTGOING IP FILTER

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



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

Auto-Detection  
Security  
IP Filtering  
**Outgoing**  
Incoming  
MAC Filtering

**Outgoing IP Filtering Setup**

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

Choose Add or Remove to configure outgoing IP filters.

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

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

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





Consult the table below for field descriptions.

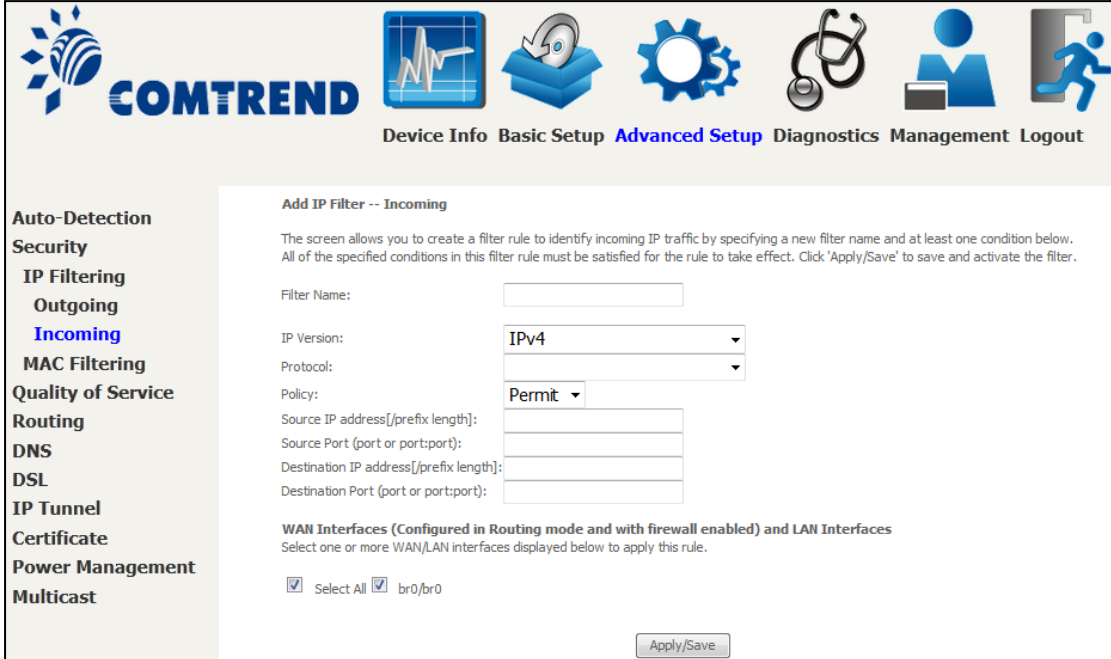
Field	Description
Filter Name	The filter rule label
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination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



To add a filter (to allow incoming IP traffic), click the **Add** button. On the following screen, enter your filter criteria and then click **Apply/Save**.



Consult the table below for field descriptions.

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.

## 6.2.2 MAC Filtering

**NOTE:** This option is only available in bridge mode. Other modes use [IP Filtering](#) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the VR-3030 can be set according to the following procedure.

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



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

**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	<b>FORWARD</b>	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/>	<input type="button" value="Remove"/>				

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


**COMTREND**







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

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

**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

Save/Apply

Consult the table below for detailed field descriptions.

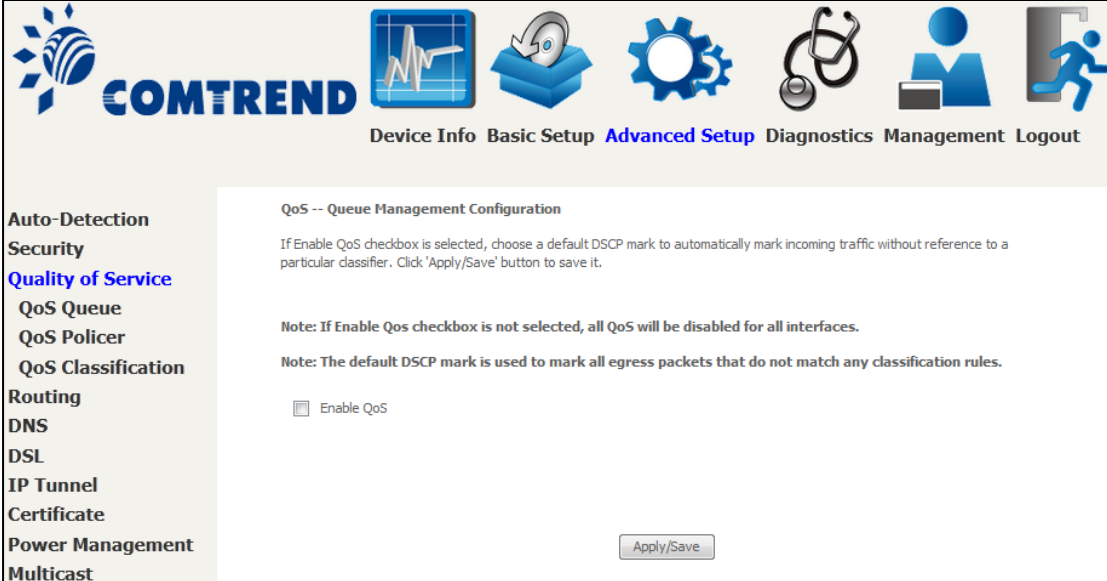
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

## 6.3 Quality of Service (QoS)

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

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

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



### **QoS and DSCP Mark are defined as follows:**

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

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

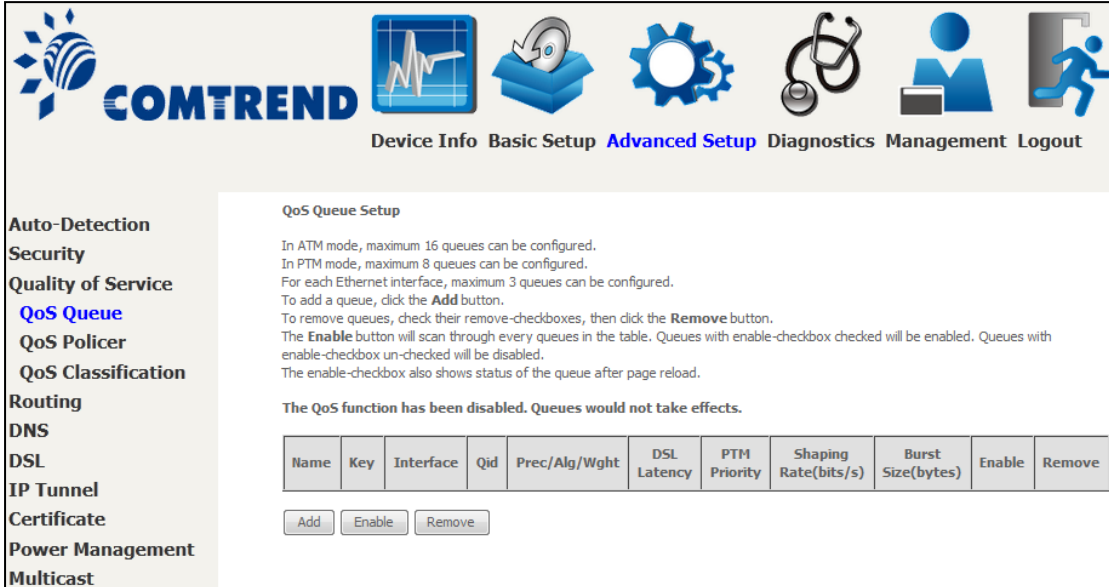
### 6.3.1 QoS Queue Setup

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 3 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.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bits/s)	Burst Size(bytes)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>										

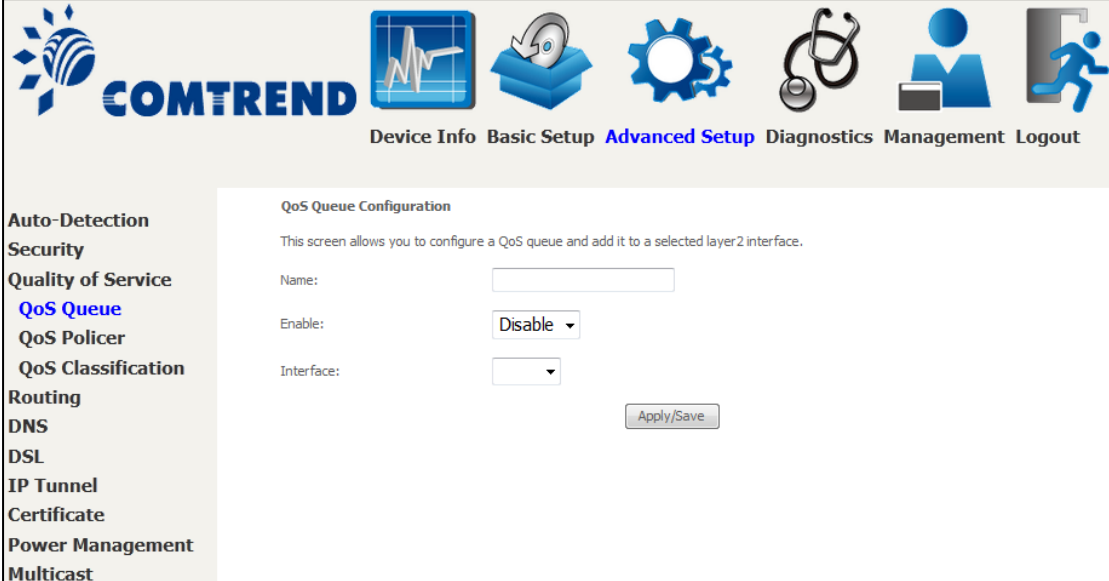
To add a queue, click the **Add** button.

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

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

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

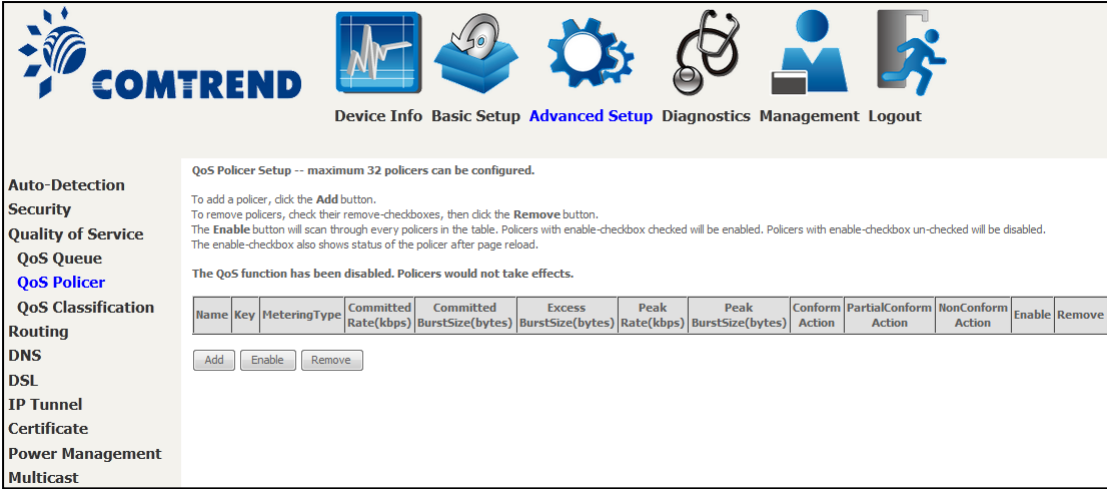
**Interface:** Assign the entry to a specific network interface (QoS enabled).

### 6.3.2 QoS Policer

To remove policers, check their remove-checkboxes, then click the **Remove** button.

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

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



QoS Policer Setup -- maximum 32 policers can be configured.

To add a policer, click the **Add** button.

To remove policers, check their remove-checkboxes, then click the **Remove** button.

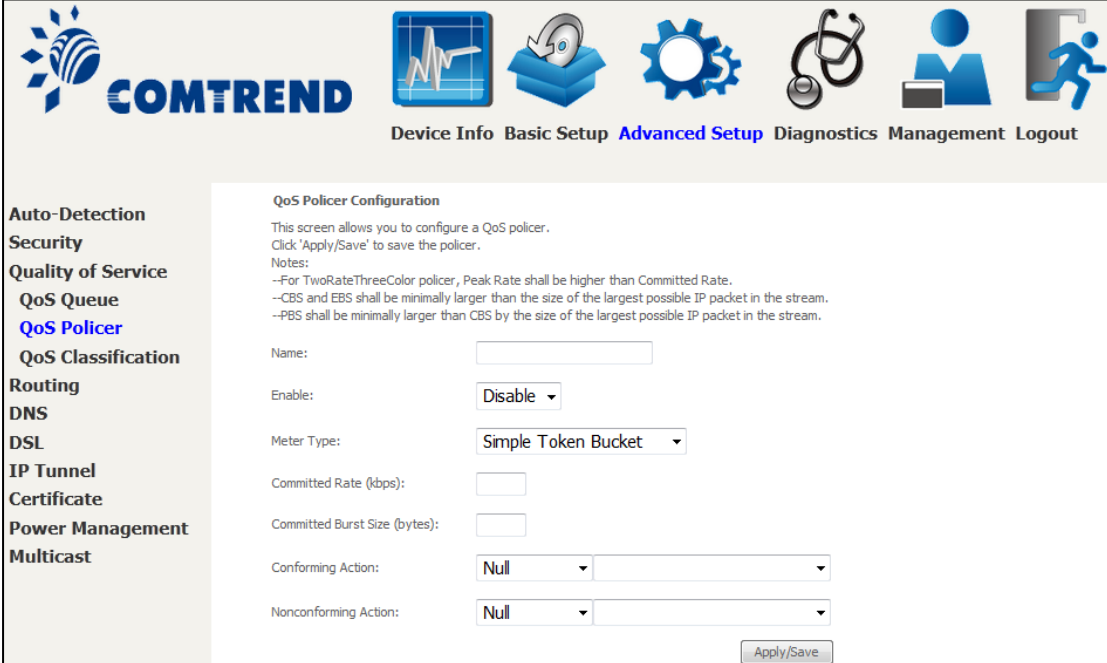
The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

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

The QoS function has been disabled. Policers would not take effects.

Name	Key	MeteringType	Committed Rate(kbps)	Committed BurstSize(bytes)	Excess BurstSize(bytes)	Peak Rate(kbps)	Peak BurstSize(bytes)	Conform Action	PartialConform Action	NonConform Action	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>												

To add a policer, click the **Add** button.



QoS Policer Configuration

This screen allows you to configure a QoS policer.

Click 'Apply/Save' to save the policer.

Notes:

- For TwoRateThreeColor policer, Peak Rate shall be higher than Committed Rate.
- CBS and EBS shall be minimally larger than the size of the largest possible IP packet in the stream.
- PBS shall be minimally larger than CBS by the size of the largest possible IP packet in the stream.

Name:

Enable:

Meter Type:

Committed Rate (kbps):

Committed Burst Size (bytes):

Conforming Action:

Nonconforming Action:

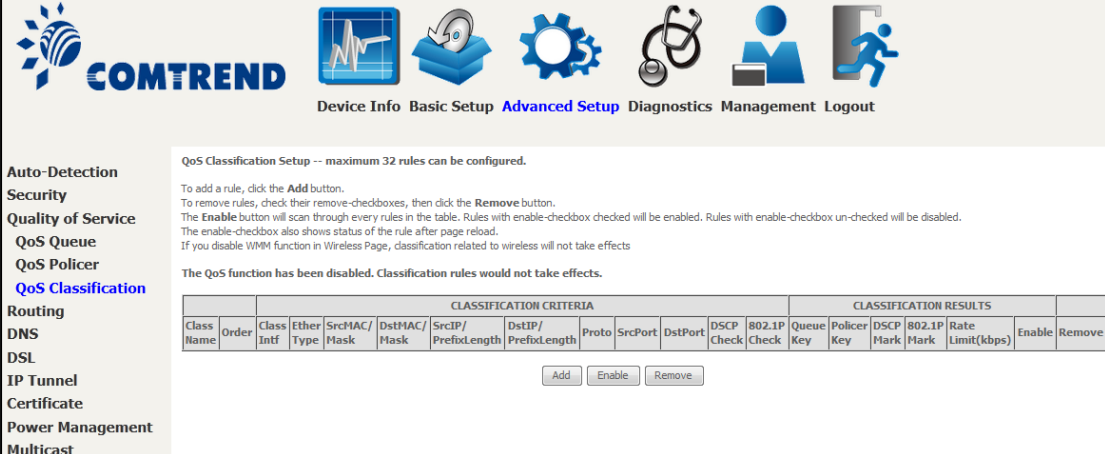
Click **Apply/Save** to save the policer.



<b>Field</b>	<b>Description</b>
Name	Name of this policer rule
Enable	Enable/Disable this policer rule
Meter Type	Meter type used for this policer rule
Committed Rate (kbps)	Defines the rate allowed for committed packets
Committed Burst Size (bytes)	Maximum amount of packets that can be processed by this policer
Conforming Action	Defines action to be taken if packets match this policer
Nonconforming Action	Defines actions to be taken if packets do not match this policer

### 6.3.3 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.

The QoS function has been disabled. Classification rules would 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	Policer Key	DSCP Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																			

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

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

**Add Network Traffic Class Rule**

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

Traffic Class Name:

Rule Order:

Rule Status:

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

Class Interface:

**Add Network Traffic Class Rule**

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

Traffic Class Name:

Rule Order:

Rule Status:

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

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

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

Specify Class 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.

Specify Class Policer:

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.

<b>Field</b>	<b>Description</b>
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
<b>Classification Criteria</b>	
Class Interface	Select an interface (i.e. Local, eth0-4, 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.
<b>Classification Results</b>	
Specify Class Queue	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.
Specify Class Policer	Packets classified into a policer will be marked based on the conforming action of the policer
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. <ul style="list-style-type: none"> <li>- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.</li> <li>- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.</li> <li>- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.</li> <li>- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.</li> </ul>
Set Rate Limit	The data transmission rate limit in kbps.


## 6.4 Routing

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

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

### 6.4.1 Default Gateway

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



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

**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**

Apply/Save

## 6.4.2 Static Route

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



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




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

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

### 6.4.3 Policy Routing

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



COMTREND

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

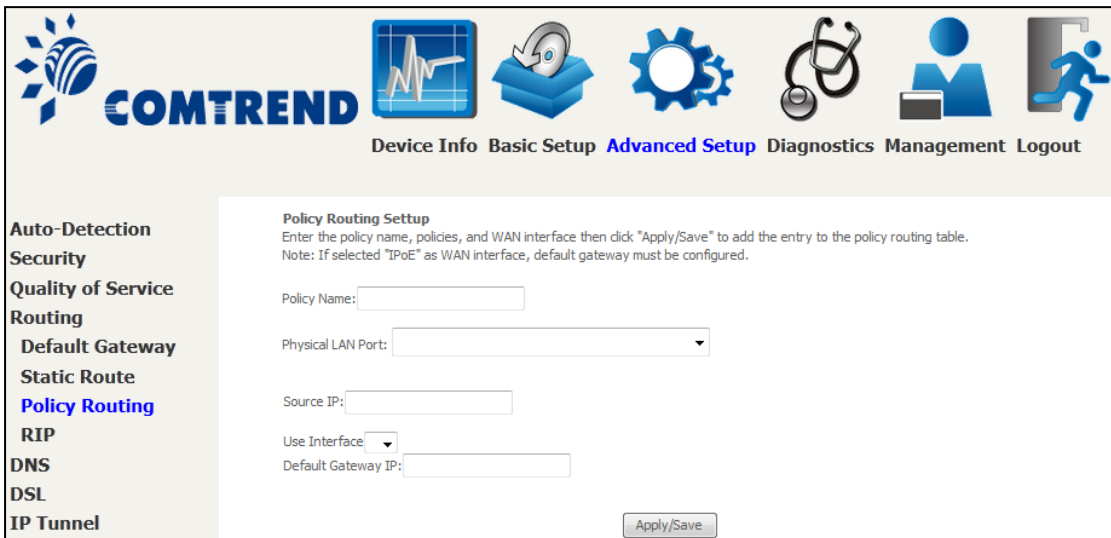
Auto-Detection  
Security  
Quality of Service  
Routing  
Default Gateway  
Static Route  
**Policy Routing**

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

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Add Remove

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



COMTREND

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

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

**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:

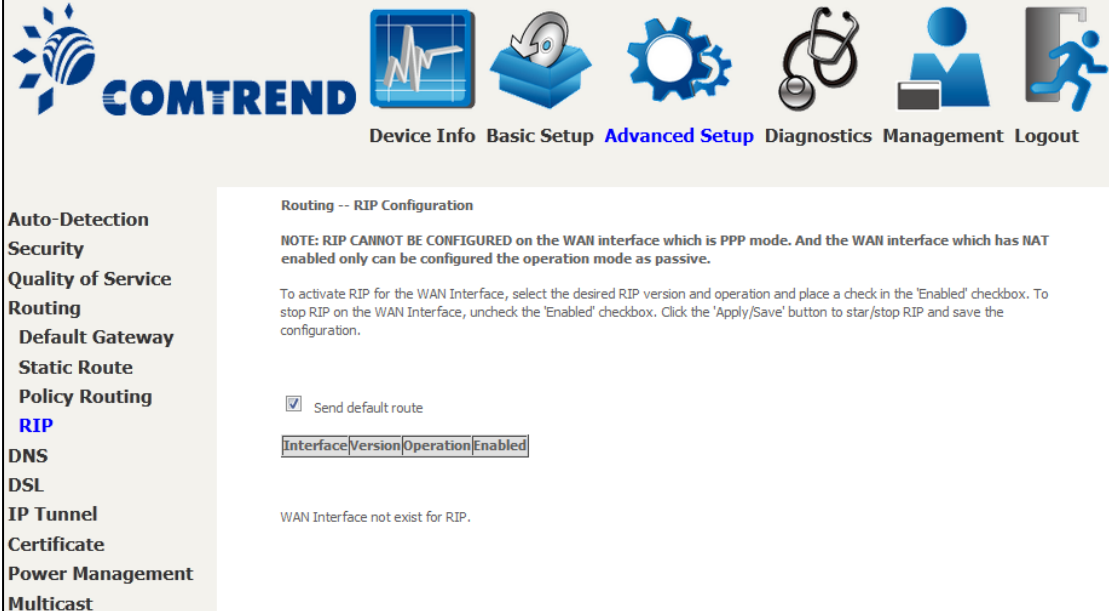
Default Gateway IP:

Apply/Save

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

## 6.4.4 RIP

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



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

**Auto-Detection**  
**Security**  
**Quality of Service**  
**Routing**  
 Default Gateway  
 Static Route  
 Policy Routing  
**RIP**  
 DNS  
 DSL  
 IP Tunnel  
 Certificate  
 Power Management  
 Multicast

Routing -- RIP Configuration

**NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.**

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

WAN Interface not exist for RIP.



## 6.5 DNS

### 6.5.1 DNS Server

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

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.



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

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

**DNS Server Configuration**

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

[->]  
[-<]

Use the following Static DNS IP address:

Primary DNS server:   
Secondary DNS server:

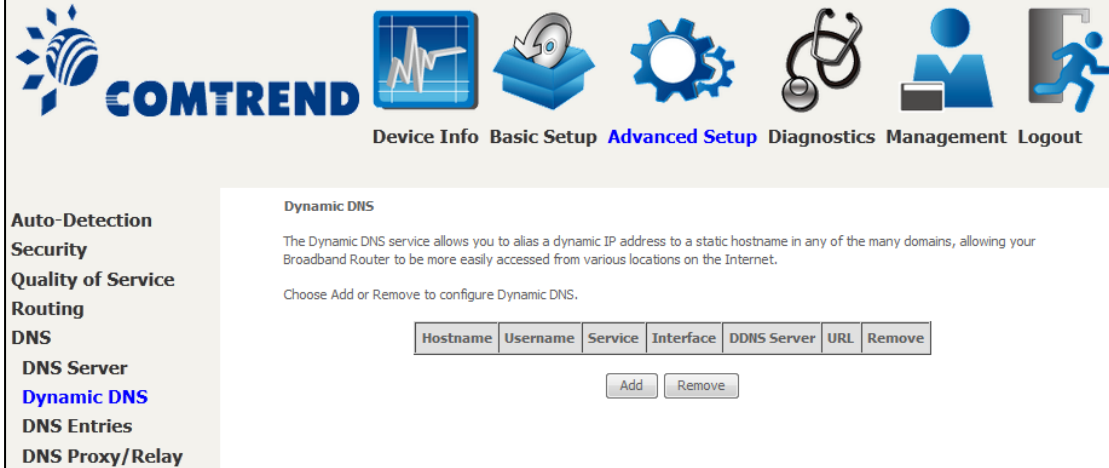
Apply/Save

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

**NOTE:** You must reboot the router to make the new configuration effective.

## 6.5.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the VR-3030 to be more easily accessed from various locations on the Internet.



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

**Dynamic DNS**


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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	DDNS Server	URL	Remove

Add Remove

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



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

**Add Dynamic DNS**

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

D-DNS provider: DynDNS.org

Hostname:

Interface:

DynDNS Settings

Username:

Password:

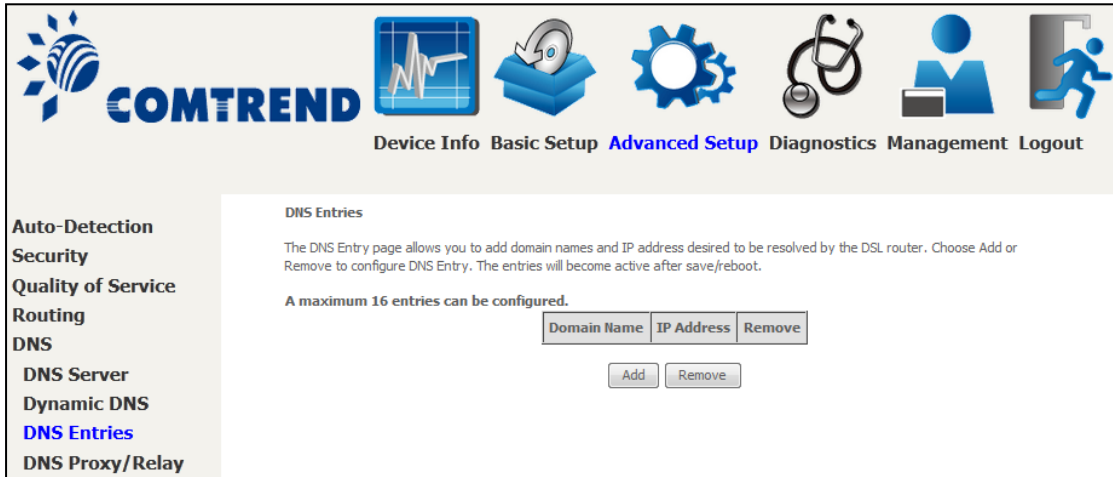
Apply/Save

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

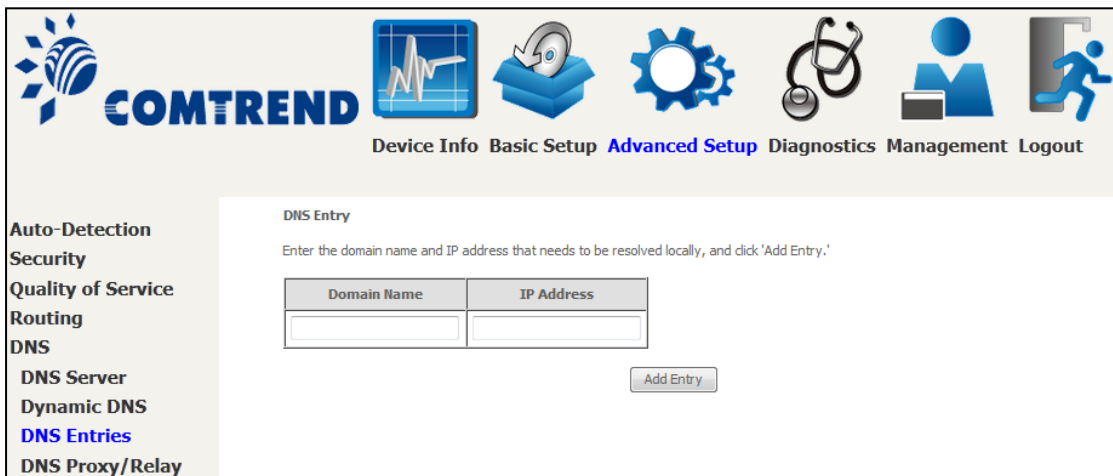
Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

### 6.5.3 DNS Entries

The DNS Entry page allows you to add domain 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.



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

## 6.5.4 DNS Proxy/Relay

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



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

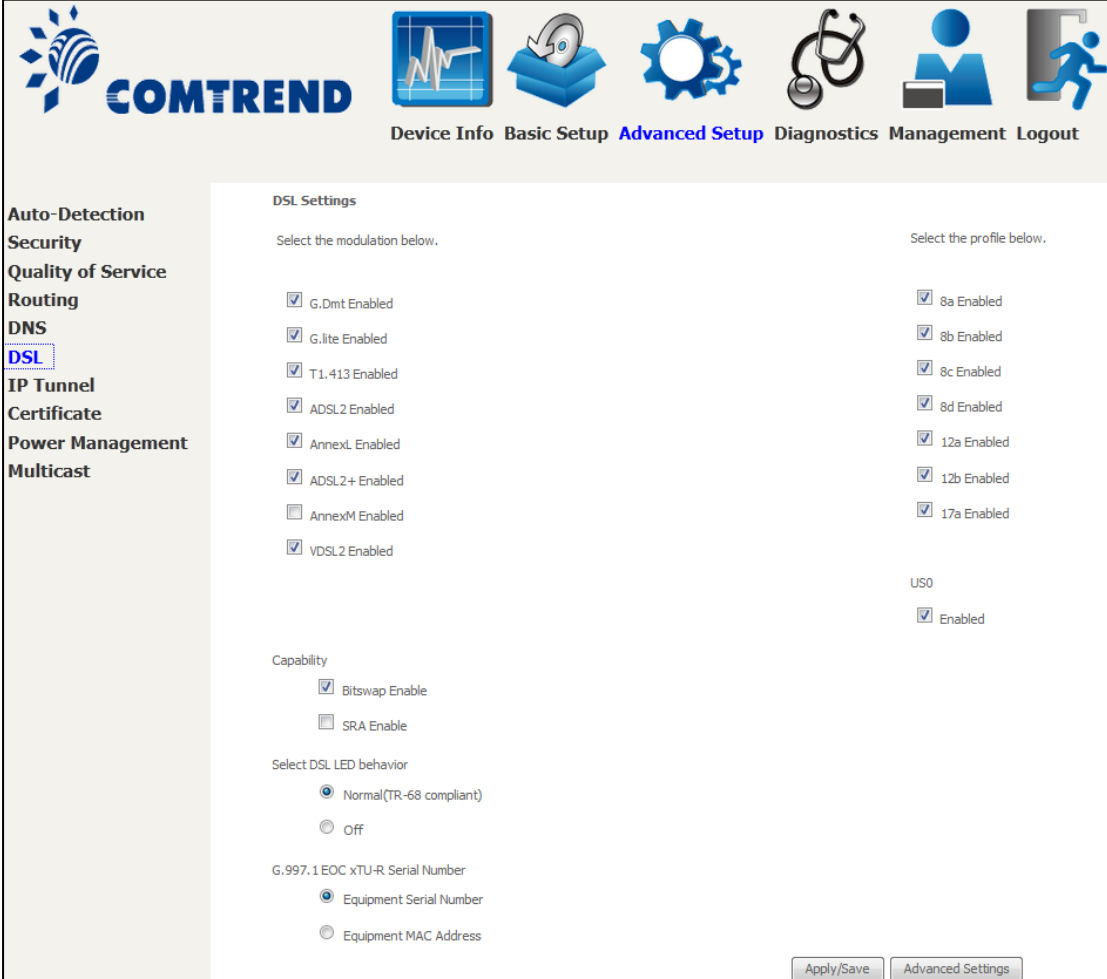
- Enable DNS Proxy
- Host name of the Broadband Router:
- Domain name of the LAN network:

Below these settings is the "DNS Relay Configuration" section, which includes the text "This controls the DHCP Server to assign public DNS." and a checked checkbox for "Enable DNS Relay". At the bottom right of the configuration area is an "Apply/Save" button.

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

## 6.6 DSL

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



**COMTREND**

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

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

**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

Select DSL LED behavior

- Normal (TR-68 compliant)
- Off

G.997.1 EOC xTU-R Serial Number

- Equipment Serial Number
- Equipment MAC Address

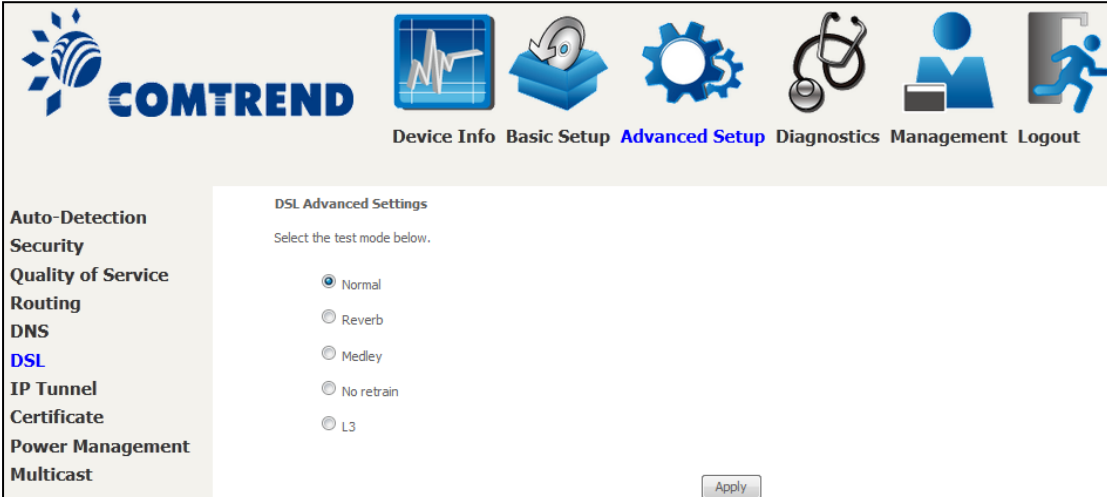
Apply/Save Advanced Settings

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

### Advanced DSL Settings

Click **Advanced Settings** to reveal additional options.



On this screen you select the required test mode, then click the **Apply** button.

Field	Description
Normal	DSL line signal is detected and sent normally
Reverb	DSL line signal is sent continuously in reverb mode
Medley	DSL line signal is sent continuously in medley mode

<b>Field</b>	<b>Description</b>
No Retrain	DSL line signal will always be on even when DSL line is unplugged
L3	DSL line is set in L3 power mode


## 6.7 IP Tunnel

### 6.7.1 IPv6inIPv4

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



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



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



<b>Options</b>	<b>Description</b>
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.



The screenshot shows the COMTREND web interface. The top navigation bar includes: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left, a sidebar lists: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, IP Tunnel, IPv6inIPv4, and **IPv4inIPv6**. The main content area is titled 'IP Tunneling -- 4in6 Tunnel Configuration' and contains a table with columns: Name, WAN, LAN, Dynamic, AFTR, and Remove. Below the table are 'Add' and 'Remove' buttons.

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



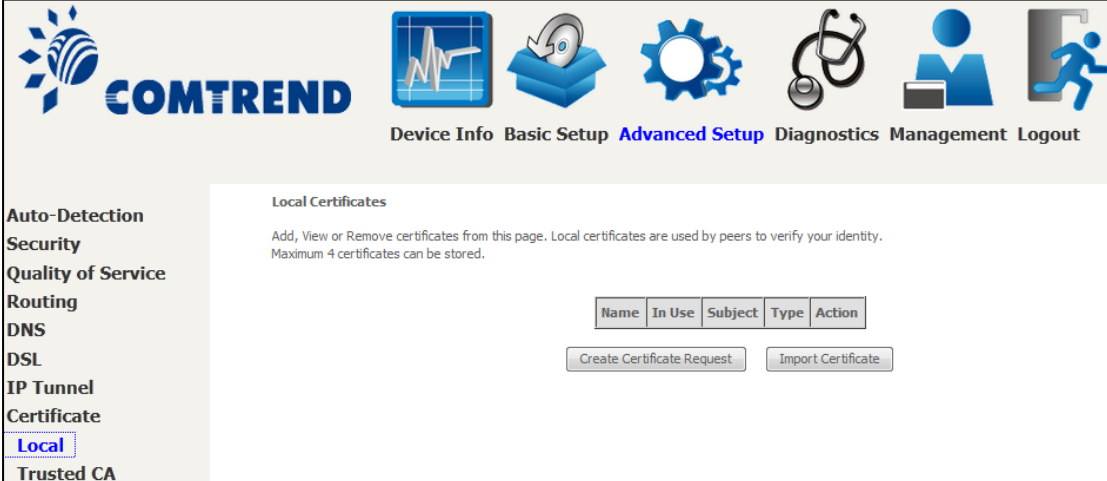
The screenshot shows the COMTREND web interface with the configuration page expanded. The top navigation bar and sidebar are the same as in the previous screenshot. The main content area is titled 'IP Tunneling -- 4in6 Tunnel Configuration' and includes the text: 'Currently, only DS-Lite configuration is supported.' Below this, there are configuration fields: 'Tunnel Name' (text input), 'Mechanism' (dropdown menu with 'DS-Lite' selected), 'Associated WAN Interface' (dropdown menu), 'Associated LAN Interface' (dropdown menu with 'LAN/br0' selected), and radio buttons for 'Manual' (selected) and 'Automatic'. There is also an 'AFTR:' label with a text input field and an 'Apply/Save' button.

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.

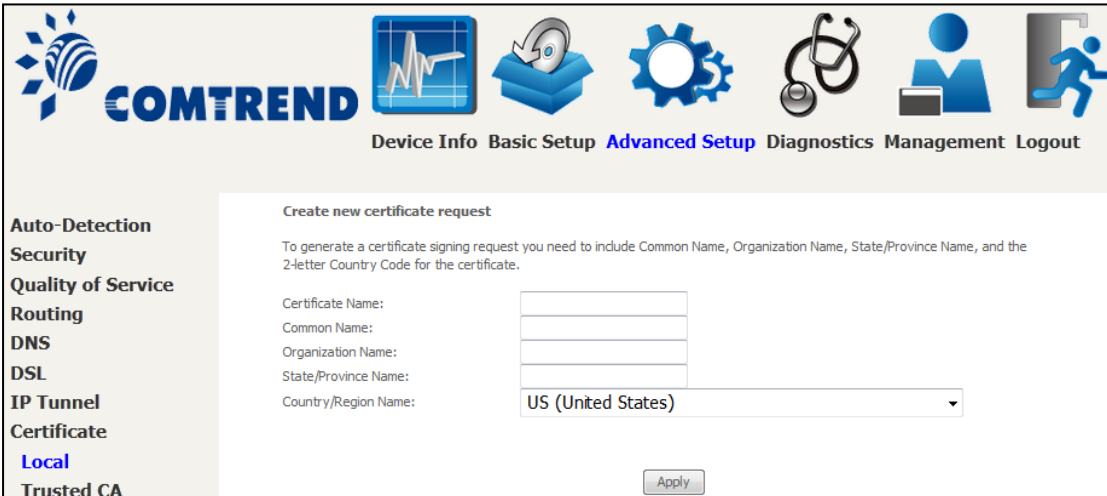
### 6.8.1 Local



### CREATE CERTIFICATE REQUEST

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

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

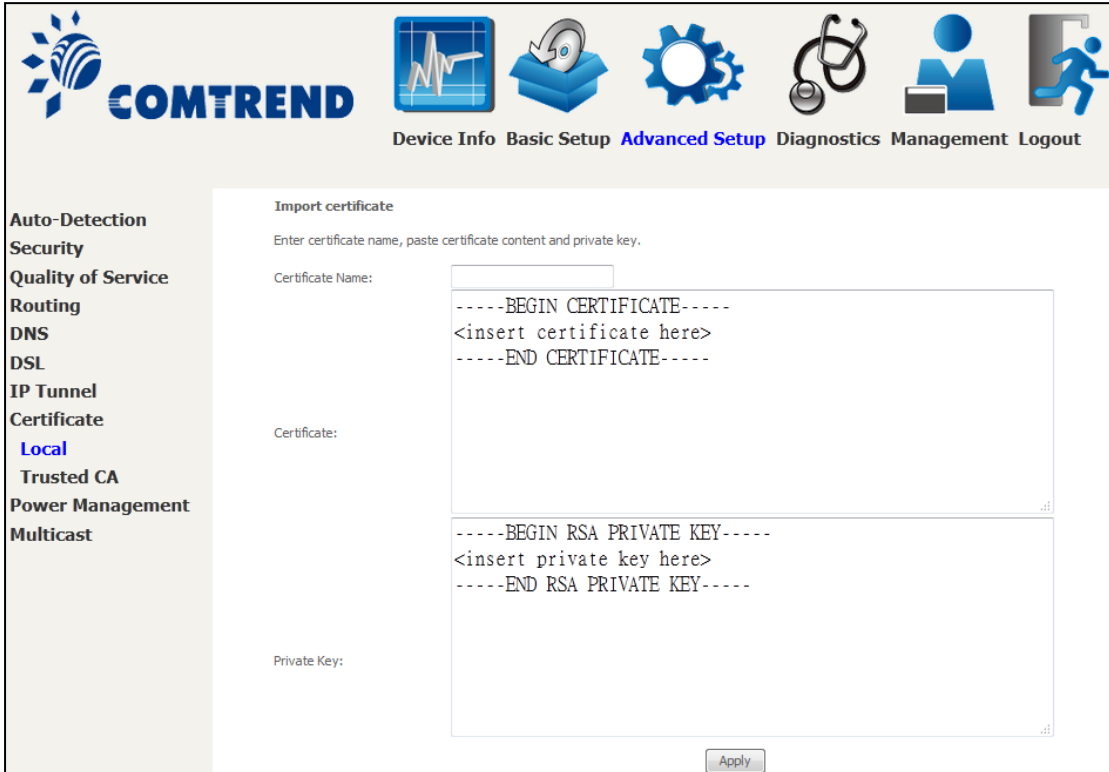


The following table is provided for your reference.

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

## IMPORT CERTIFICATE

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



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

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

Certificate Name:

Certificate: 

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

Private Key: 

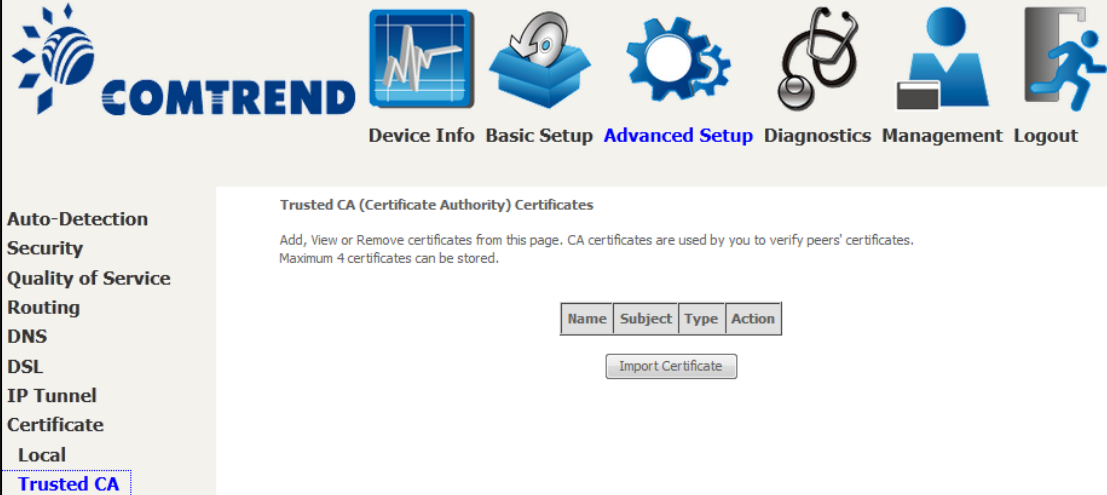
```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Apply

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.

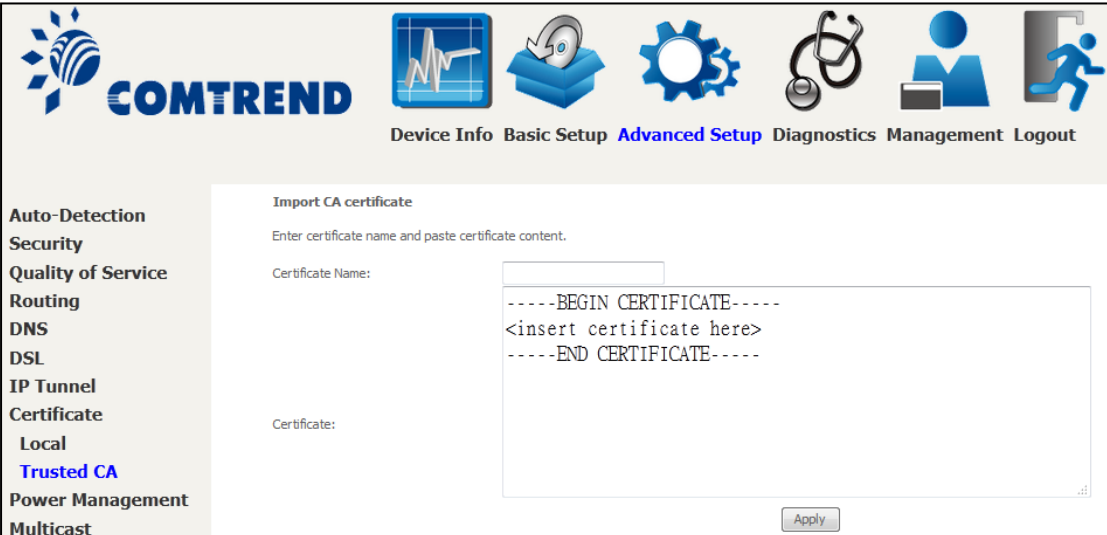


**Trusted CA (Certificate Authority) Certificates**

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
<input type="button" value="Import Certificate"/>			

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



**Import CA certificate**

Enter certificate name and paste certificate content.

Certificate Name:

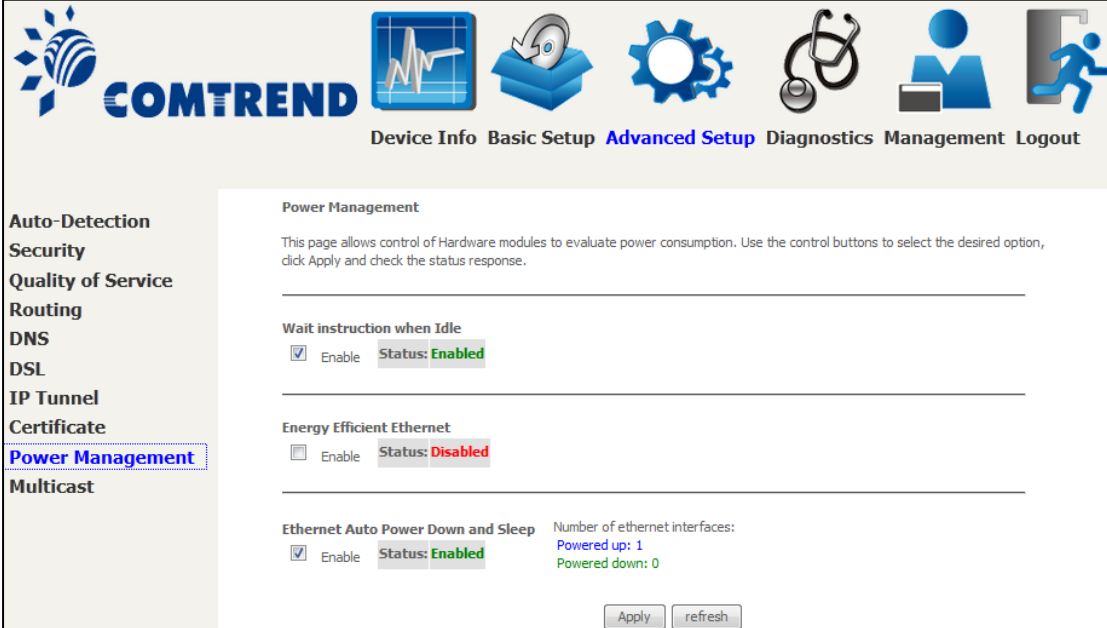
Certificate: 

```
-----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.



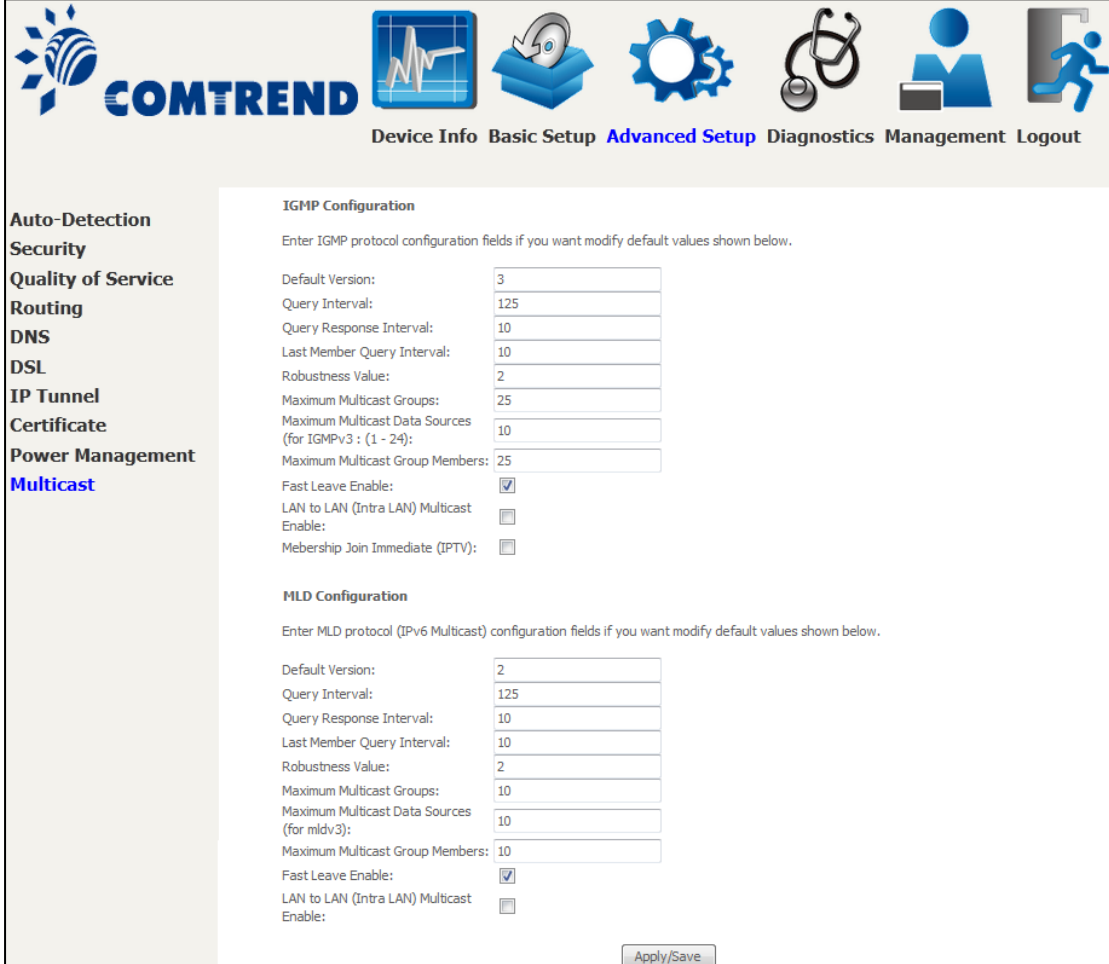
The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons and labels for: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Quality of Service, Routing, DNS, DSL, IP Tunnel, Certificate, **Power Management** (highlighted with a blue border), and Multicast. The main content area is titled "Power Management" and contains the following text: "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." Below this text are three configuration sections, each separated by a horizontal line:

- Wait instruction when Idle**:  Enable Status: **Enabled**
- Energy Efficient Ethernet**:  Enable Status: **Disabled**
- Ethernet Auto Power Down and Sleep**:  Enable Status: **Enabled**

To the right of the "Ethernet Auto Power Down and Sleep" section, there is a status display: "Number of ethernet interfaces: Powered up: 1 Powered down: 0". At the bottom right of the configuration area, there are two buttons: "Apply" and "refresh".

## 6.10 Multicast

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



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

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

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

Default Version:   
 Query Interval:   
 Query Response Interval:   
 Last Member Query Interval:   
 Robustness Value:   
 Maximum Multicast Groups:   
 Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):   
 Maximum Multicast Group Members:   
 Fast Leave Enable:   
 LAN to LAN (Intra LAN) Multicast Enable:   
 Mebership Join Immediate (IPTV):

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

Default Version:   
 Query Interval:   
 Query Response Interval:   
 Last Member Query Interval:   
 Robustness Value:   
 Maximum Multicast Groups:   
 Maximum Multicast Data Sources (for mldv3):   
 Maximum Multicast Group Members:   
 Fast Leave Enable:   
 LAN to LAN (Intra LAN) Multicast Enable:

Apply/Save

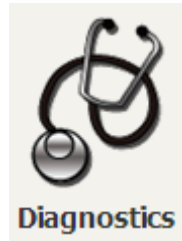
Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.

<b>Field</b>	<b>Description</b>
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.
LAN to LAN (Intra LAN) Multicast Enable	This will activate IGMP snooping for cases where multicast data source and player are all located on the LAN side.
Membership to join Immediate (IPTV)	Enable IGMP immediate join feature for multicast membership group.

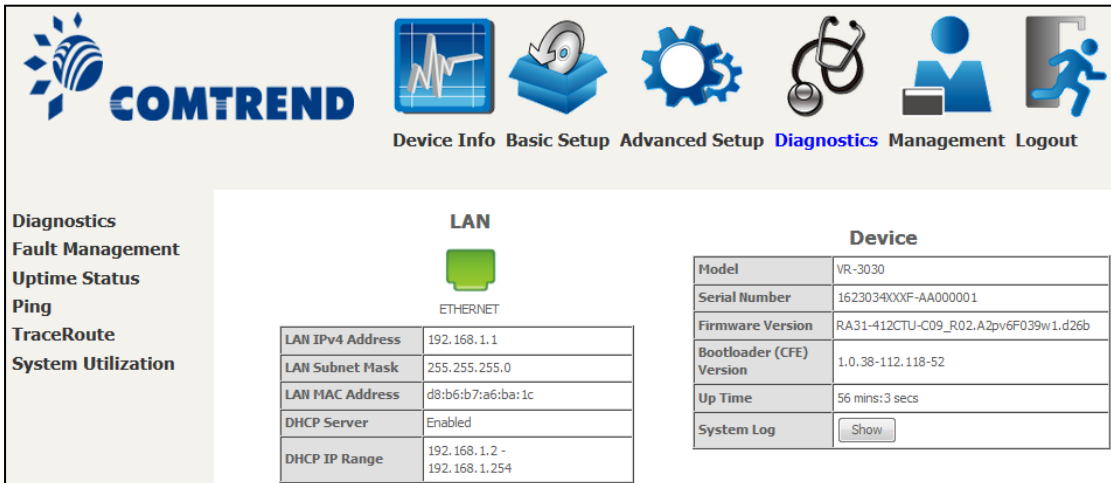


## Chapter 7 Diagnostics

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



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



The screenshot shows the COMTREND Diagnostics dashboard. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics (highlighted), Management, and Logout. The main content area is divided into three sections:

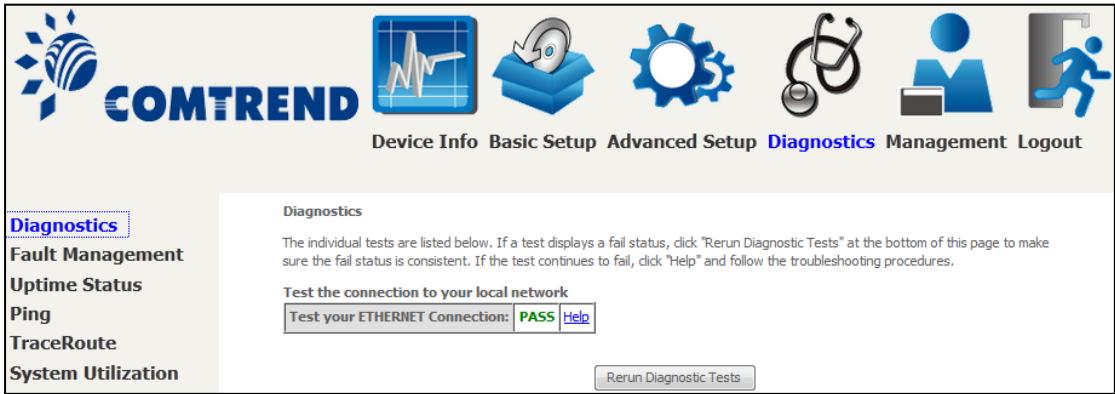
- Left Sidebar:** Contains links for Diagnostics, Fault Management, Uptime Status, Ping, TraceRoute, and System Utilization.
- LAN Section:** Shows a green status icon and the text "ETHERNET". Below it is a table with the following data:
 

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:a6:ba:1c
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 - 192.168.1.254
- Device Section:** Shows a table with the following data:
 

Model	VR-3030
Serial Number	162303400XF-AA000001
Firmware Version	RA31-412CTU-C09_R02.A2pv6F039w1.d26b
Bootloader (CFE) Version	1.0.38-112.118-52
Up Time	56 mins:3 secs
System Log	<input type="button" value="Show"/>

### 7.1 Diagnostics – Individual Tests

On the left side of your screen, click Diagnostics.



The screenshot shows the COMTREND Diagnostics Individual Tests screen. The navigation bar is the same as in the previous screenshot, with "Diagnostics" highlighted. The left sidebar is also the same, with "Diagnostics" highlighted. The main content area contains the following text:

**Diagnostics**

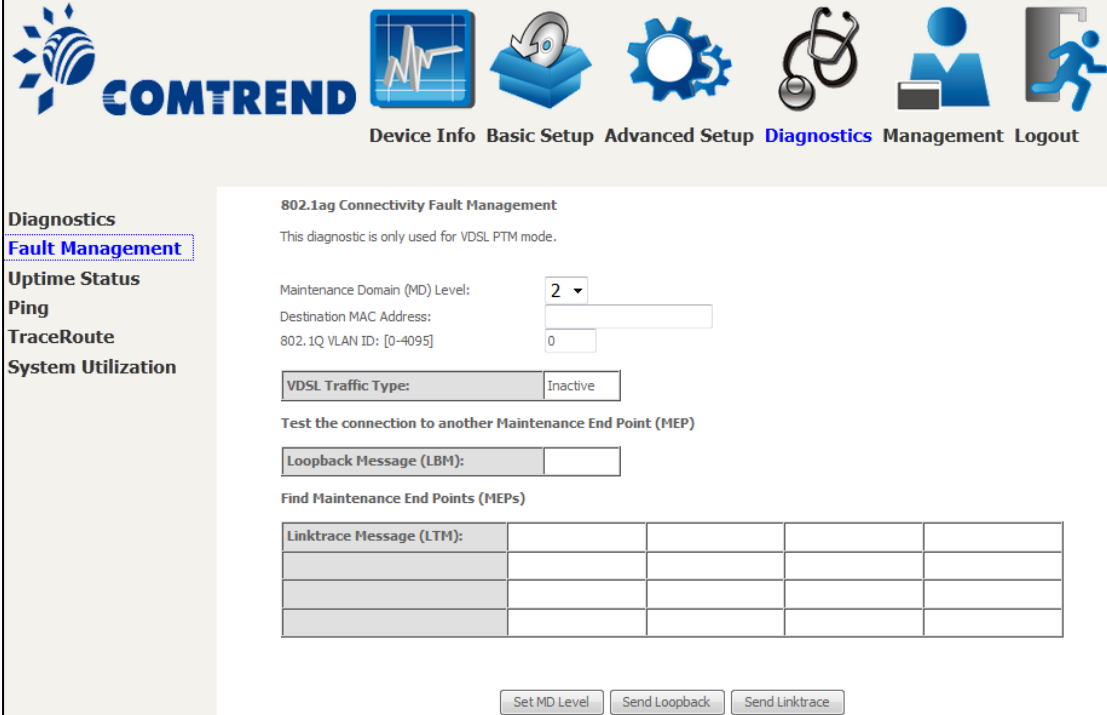
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

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

## 7.2 Fault Management

Fault management is the component of network management concerned with detecting, isolating and resolving problems. Properly implemented, fault management can keep a network running at an optimum level, provide a measure of fault tolerance and minimize downtime.



Item	Description
Maintenance Domain (MD) Level	Management space on the network, the larger the domain, the higher the level value
Destination MAC Address	Destination MAC address for sending the loopback message
802.1Q VLAN ID: [0-4095]	802.1Q VLAN used in VDSL PTM mode

### Set MD Level

Save the Maintenance domain level.

### Send Loopback

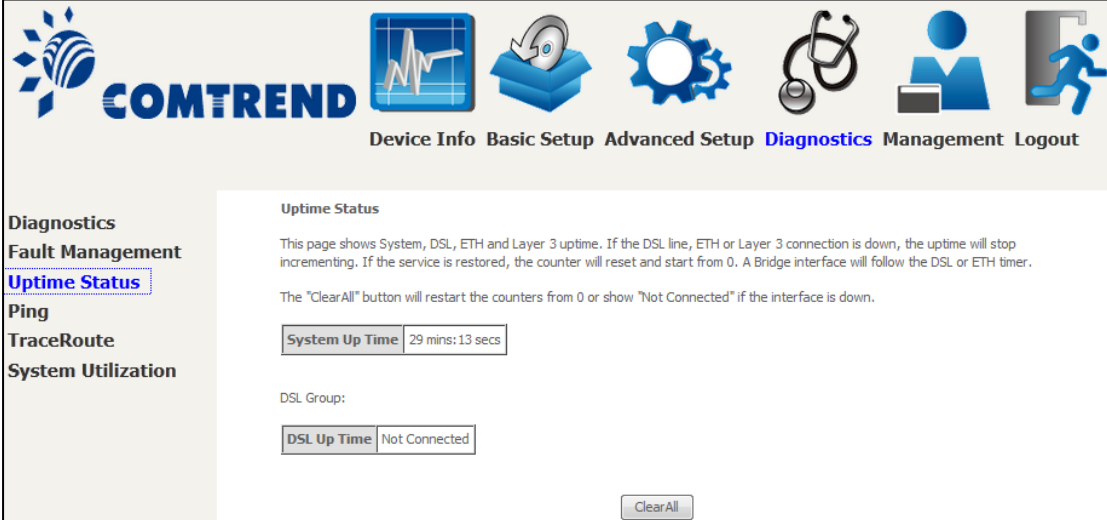
Send loopback message to destination MAC address.

### Send Linktrace

Send traceroute message to destination MAC address.

## 7.3 Uptime Status

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



**COMTREND**

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

**Diagnostics**  
**Fault Management**  
**Uptime Status**  
 Ping  
 TraceRoute  
 System Utilization

**Uptime Status**

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

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

**System Up Time** 29 mins: 13 secs

DSL Group:

**DSL Up Time** Not Connected

ClearAll

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

## 7.4 Ping

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



The screenshot displays the COMTREND web interface. At the top, there is a navigation menu with icons and labels for: Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted), Management, and Logout. On the left side, a sidebar menu lists: Diagnostics, Fault Management, Uptime Status, **Ping** (highlighted), TraceRoute, and System Utilization. The main content area is titled "Ping" and contains the following text and form:

Ping

Send ICMP ECHO\_REQUEST packets to network hosts.

Ping IP Address / Hostname:

PING 192.168.1.1 (192.168.1.1): 56 data bytes  
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.455 ms  
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.344 ms  
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.339 ms  
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.343 ms

--- 192.168.1.1 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max = 0.339/0.370/0.455 ms

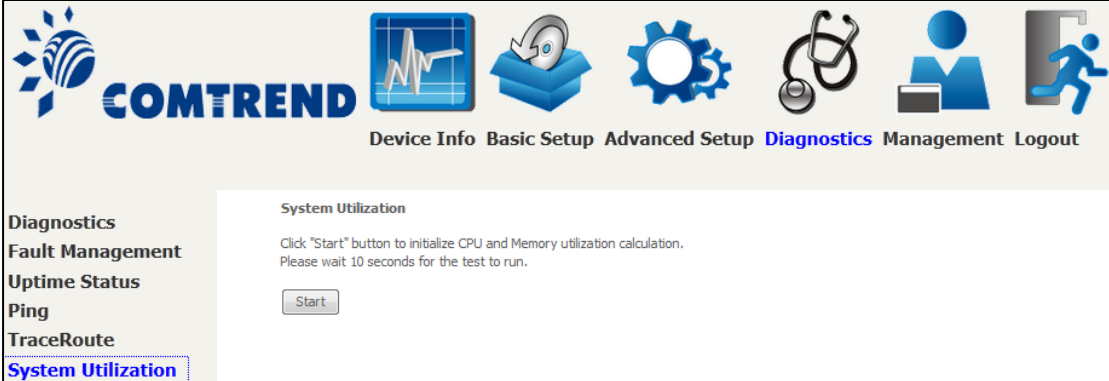
## 7.5 Trace Route

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



The screenshot displays the COMTREND web interface. At the top, there is a navigation menu with icons and labels: Device Info, Basic Setup, Advanced Setup, **Diagnostics** (highlighted), Management, and Logout. On the left side, a sidebar menu lists: Diagnostics, Fault Management, Uptime Status, Ping, **TraceRoute** (highlighted), and System Utilization. The main content area is titled "TraceRoute" and contains the following text: "Trace the route ip packets follow going to 'host'." Below this is a form with the label "TraceRoute IP Address / Hostname:" followed by an empty text input field and a "TraceRoute" button. At the bottom of the main area, there is a sample output: "traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets" followed by "1 192.168.1.1 (192.168.1.1) 0.392 ms".

## 7.6 System Utilization



**COMTREND**

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

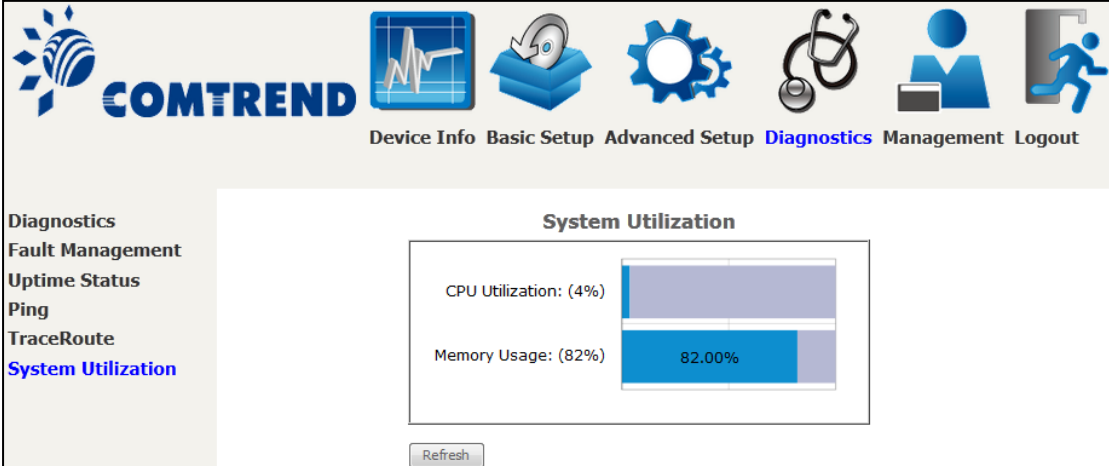
**Diagnostics**  
 Fault Management  
 Uptime Status  
 Ping  
 TraceRoute  
 System Utilization

**System Utilization**

Click "Start" button to initialize CPU and Memory utilization calculation.  
 Please wait 10 seconds for the test to run.

Start

Click "Start" button to initialize CPU and Memory utilization calculation.  
 Please wait 10 seconds for the test to run.



**COMTREND**

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

**Diagnostics**  
 Fault Management  
 Uptime Status  
 Ping  
 TraceRoute  
 System Utilization

**System Utilization**

CPU Utilization: (4%)	<div style="width: 4%; background-color: #4f81bd; height: 15px;"></div>
Memory Usage: (82%)	<div style="width: 82%; background-color: #4f81bd; height: 15px; display: flex; align-items: center; justify-content: center;"><span>82.00%</span></div>

Refresh

## Chapter 8 Management

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



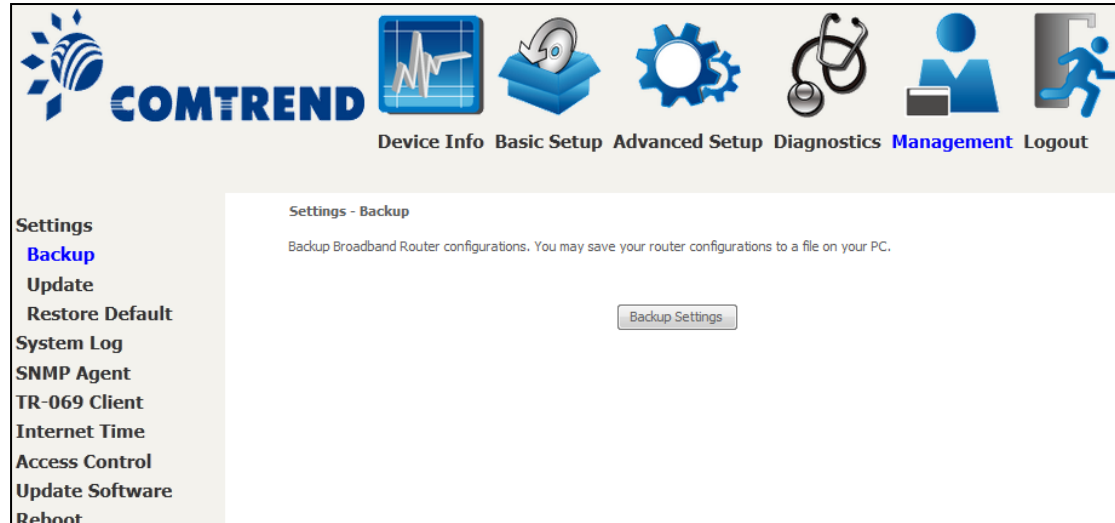
The Management menu has the following maintenance functions and processes:

### 8.1 Settings

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

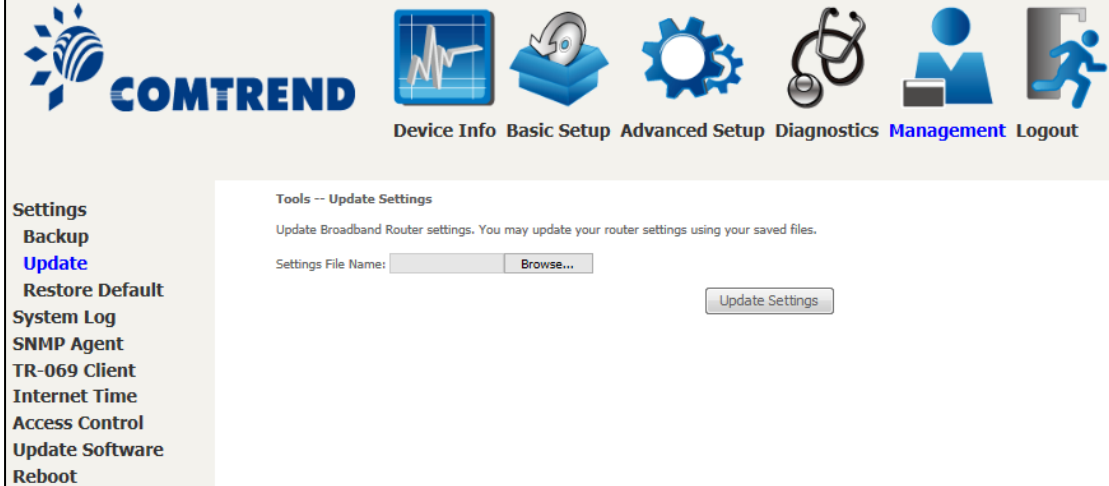
#### 8.1.1 Backup Settings

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



## 8.1.2 Update Settings

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

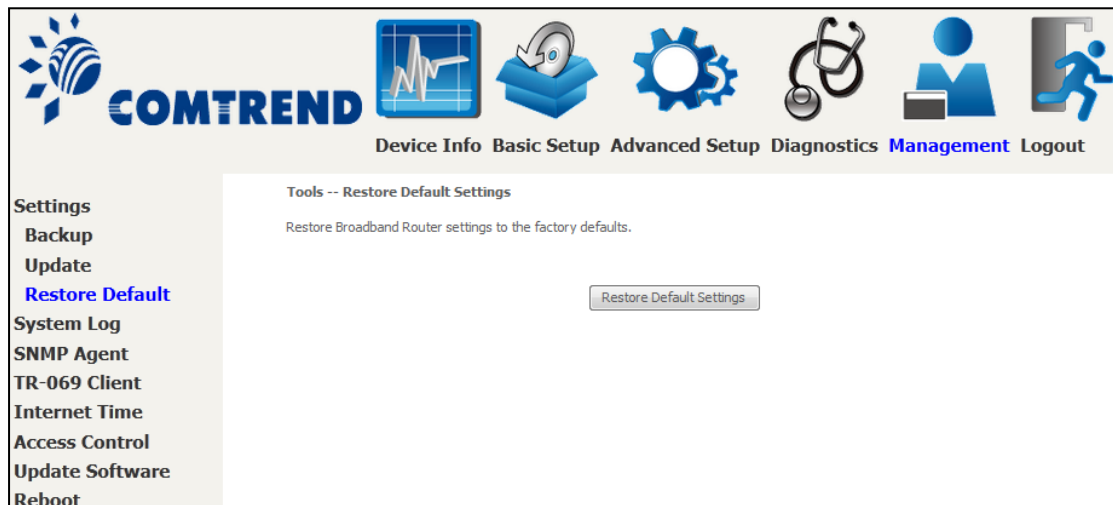


The screenshot displays the COMTREND web management interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (highlighted in blue), and Logout. Below the navigation bar, a left sidebar lists various settings options: Settings, Backup, Update (highlighted in blue), Restore Default, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Update Software, and Reboot. The main content area is titled 'Tools -- Update Settings' and contains the following text: 'Update Broadband Router settings. You may update your router settings using your saved files.' Below this text, there is a 'Settings File Name:' label followed by a text input field and a 'Browse...' button. To the right of the input field is an 'Update Settings' button.

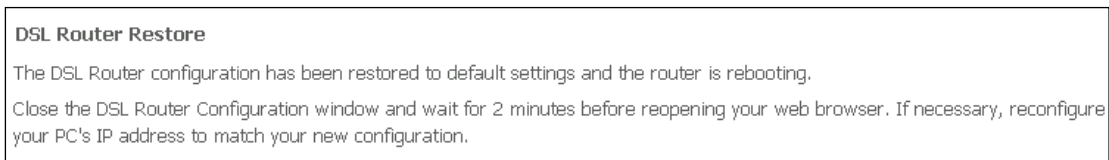


### 8.1.3 Restore Default

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



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



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

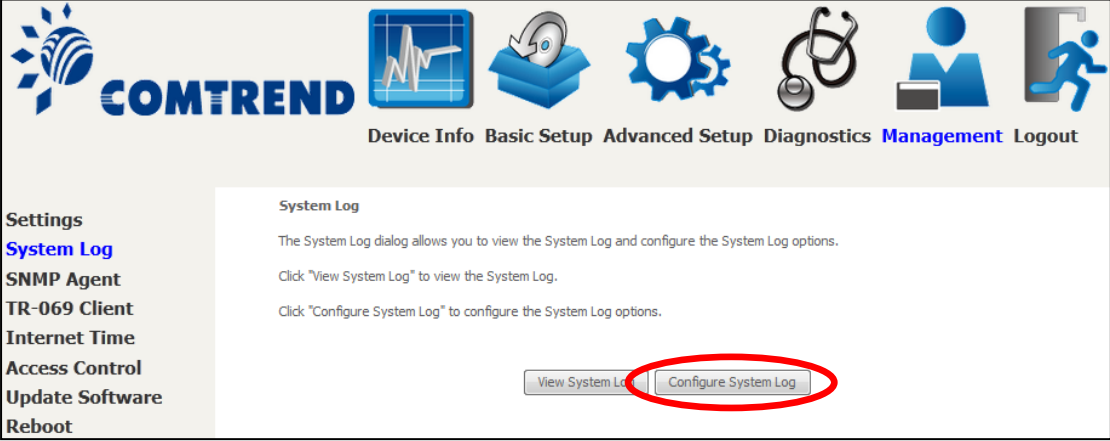
**NOTE:** This entry has the same effect as the **Reset** button. The VR-3030 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the boot loader will erase the configuration data saved in flash memory.

## 8.2 System Log

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

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

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



The screenshot shows the COMTREND Management interface. The navigation bar includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, **Management**, and Logout. The left sidebar lists: Settings, **System Log**, SNMP Agent, TR-069 Client, Internet Time, Access Control, Update Software, and Reboot. The main content area is titled "System Log" and contains the following text:

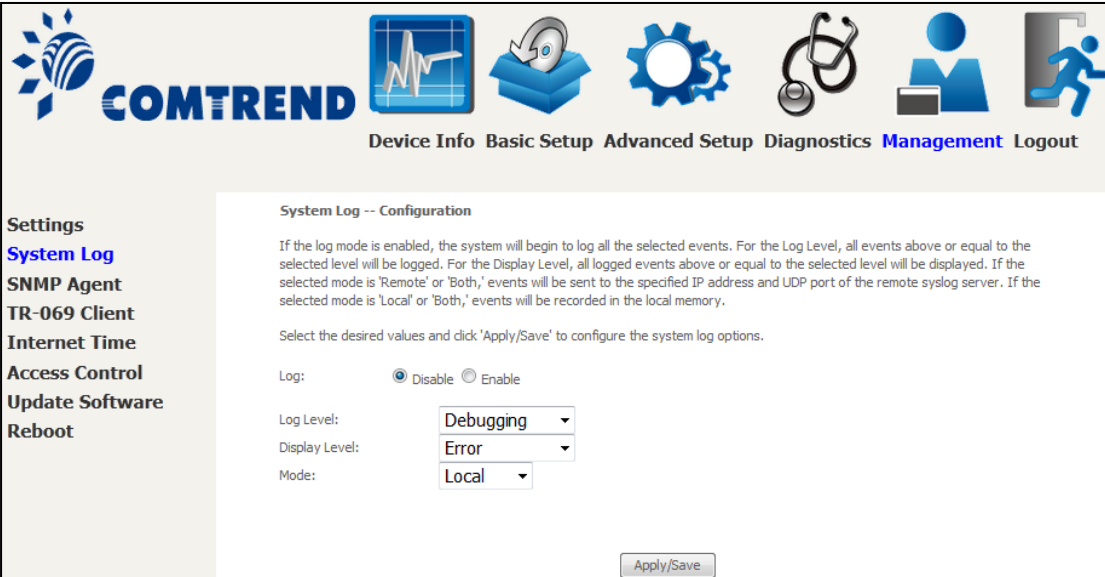
The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

At the bottom of the main content area, there are two buttons: "View System Log" and "Configure System Log". The "Configure System Log" button is circled in red.

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



The screenshot shows the COMTREND Management interface. The navigation bar includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, **Management**, and Logout. The left sidebar lists: Settings, **System Log**, SNMP Agent, TR-069 Client, Internet Time, Access Control, Update Software, and Reboot. The main content area is titled "System Log -- Configuration" and contains the following text:

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

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

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

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

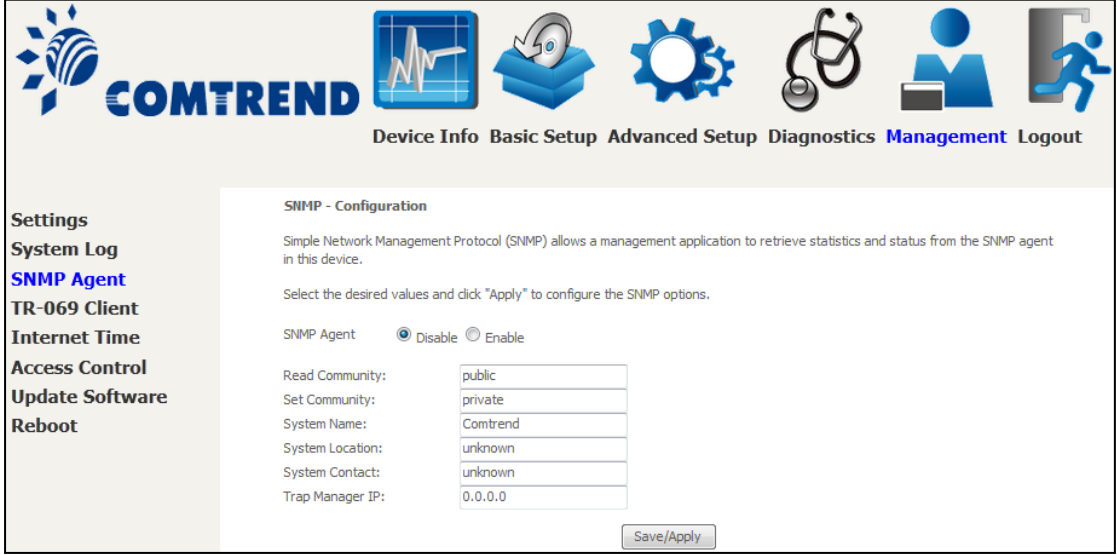
Option	Description
Log Level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the VR-3030 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> <li>• Emergency = system is unusable</li> <li>• Alert = action must be taken immediately</li> <li>• Critical = critical conditions</li> <li>• Error = Error conditions</li> <li>• Warning = normal but significant condition</li> <li>• Notice= normal but insignificant condition</li> <li>• Informational= provides information for reference</li> <li>• Debugging = debug-level messages</li> </ul> <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	<p>Allows the user to select the logged events and displays on the <b>View System Log</b> window for events of this level and above to the highest Emergency level.</p>
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

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

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

## 8.3 SNMP Agent


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



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management (highlighted), and Logout. Below the navigation bar, the left sidebar contains a list of settings: Settings, System Log, **SNMP Agent**, TR-069 Client, Internet Time, Access Control, Update Software, and Reboot. The main content area is titled "SNMP - Configuration" and contains the following text: "Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the desired values and click 'Apply' to configure the SNMP options." Below this text, there are two radio buttons for "SNMP Agent": "Disable" (selected) and "Enable". Underneath, there are six input fields for configuration: "Read Community" (public), "Set Community" (private), "System Name" (Comtrend), "System Location" (unknown), "System Contact" (unknown), and "Trap Manager IP" (0.0.0.0). A "Save/Apply" button is located at the bottom right of the configuration area.

## 8.4 TR-069 Client

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



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

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

**TR-069 client - Configuration**

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

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

Enable TR-069

OUI-serial  MAC  Serialnumber  
 Inform  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

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

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

The table below is provided for ease of reference.

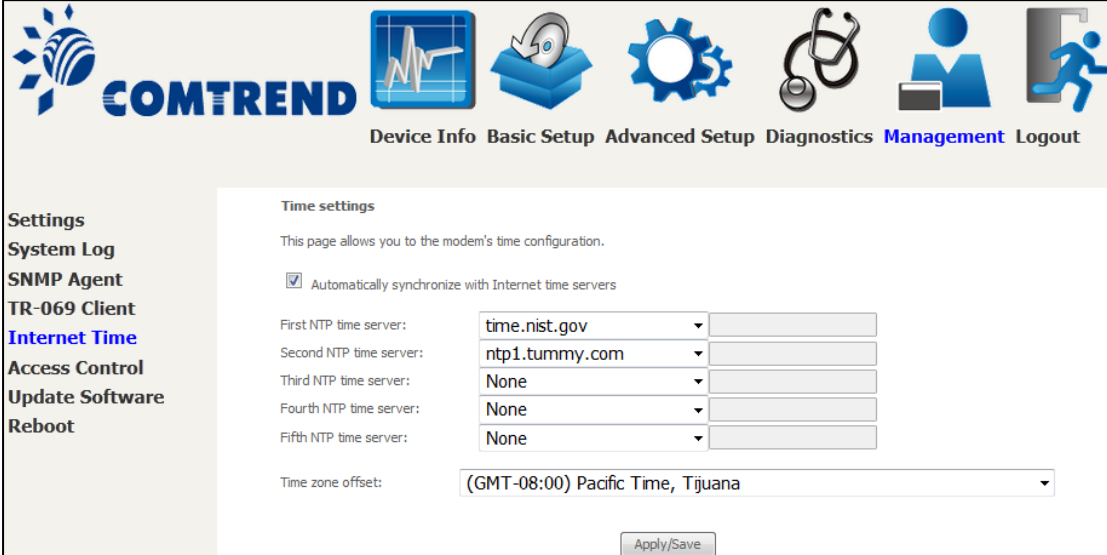
Option	Description
Enable TR-069	Tick the checkbox <input checked="" type="checkbox"/> to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate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

Option	Description
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
<b>Connection Request</b>	
Authentication	Tick the checkbox <input checked="" type="checkbox"/> to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to router.

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

## 8.5 Internet Time

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



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

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

**Time settings**

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

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

**NOTE:** Internet Time must be activated to use [Parental Control](#). In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

## 8.6 Access Control


### 8.6.1 Accounts







This screen is used to configure the user account access passwords for the device. Access to the VR-3030 is controlled through the following user accounts:

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

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





**Settings**

**System Log**

**SNMP Agent**

**TR-069 Client**

**Internet Time**

**Access Control**

**Accounts**

**Service Access**

**IP Address**

**Update Software**

**Reboot**

### Access Control -- Accounts/Passwords

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

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

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

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

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

Select an account: 
  
 Create an account:

Old Password:

New Password:

Confirm Password:

---

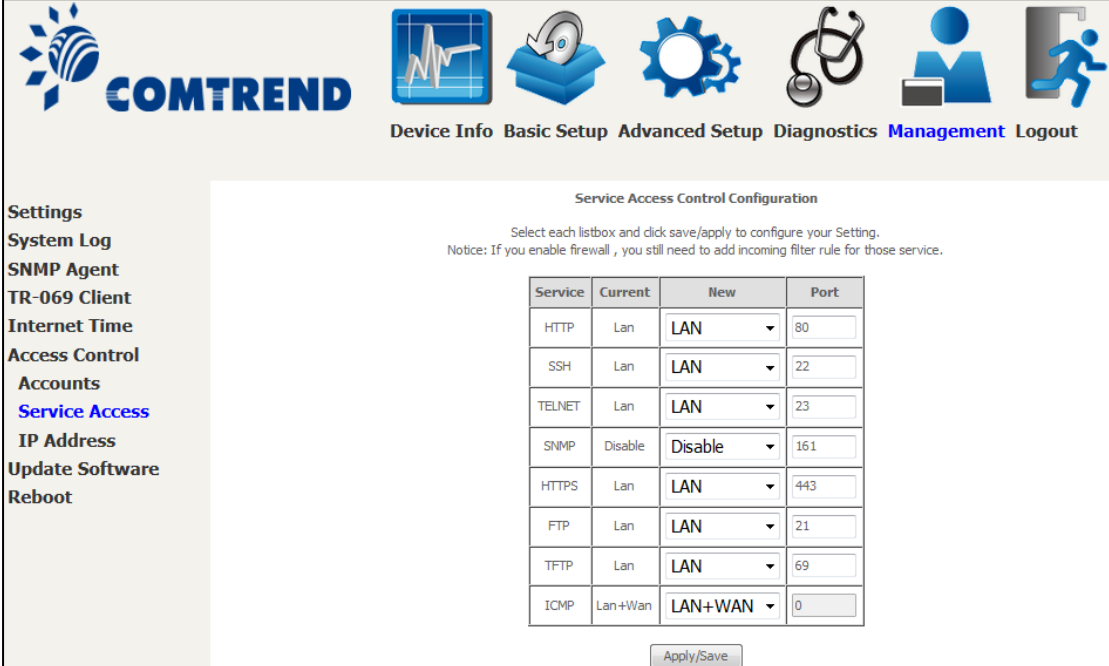
Use the fields below to enable/disable accounts as well as adjust their specific privileges.

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

Note: Passwords may be as long as 16 characters but must not contain a space. Click **Save/Apply** to continue.

## 8.6.2 Service Access

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



**COMTREND**

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

**Settings**  
 System Log  
 SNMP Agent  
 TR-069 Client  
 Internet Time  
 Access Control  
 Accounts  
**Service Access**  
 IP Address  
 Update Software  
 Reboot

**Service Access Control Configuration**

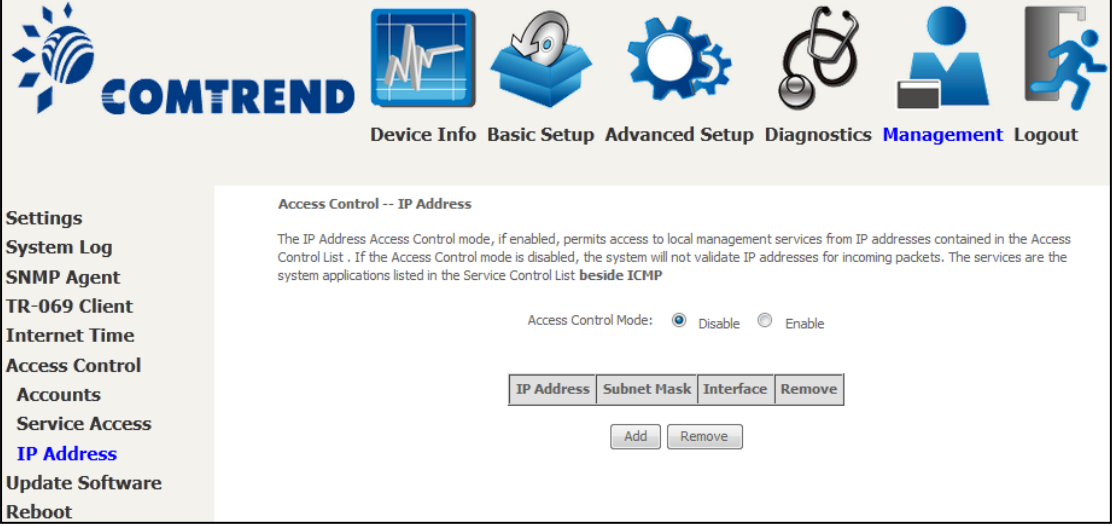
Select each listbox and click save/apply to configure your Setting.  
 Notice: If you enable firewall, you still need to add incoming filter rule for those service.

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

Apply/Save

### 8.6.3 IP Address

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



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

**Settings**  
 System Log  
 SNMP Agent  
 TR-069 Client  
 Internet Time  
 Access Control  
 Accounts  
 Service Access  
**IP Address**  
 Update Software  
 Reboot

**Access Control -- IP Address**

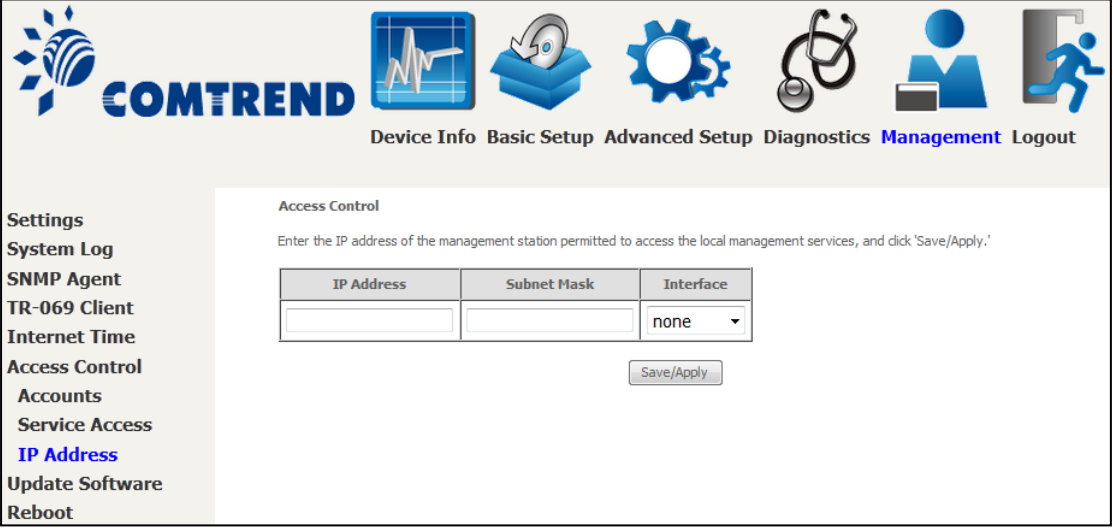
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List . If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed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

Access Control Mode:  Disable  Enable

IP Address	Subnet Mask	Interface	Remove

Add Remove

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



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

**Settings**  
 System Log  
 SNMP Agent  
 TR-069 Client  
 Internet Time  
 Access Control  
 Accounts  
 Service Access  
**IP Address**  
 Update Software  
 Reboot

**Access Control**

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

IP Address	Subnet Mask	Interface
		none

Save/Apply

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

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

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

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

## 8.7 Update Software

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



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

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

### Configuration options:

**No change** – upgrade software directly.

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

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

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

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

**NOTE1:** The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Chapter 4](#) Device Information screen with the firmware version installed, to confirm the installation was successful.

**NOTE2:** The Power LED indicates the status of firmware update progress. Please **DO NOT** power off the device when Power LED is flashing or the device will be damaged.

## 8.8 Reboot

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



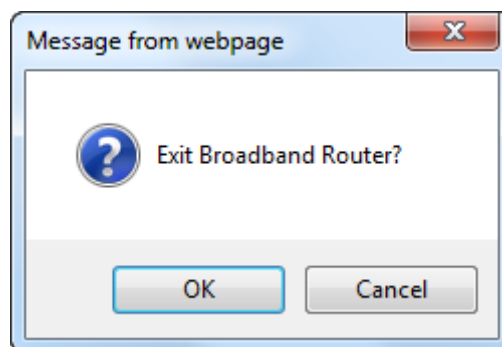
**NOTE:** You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

## Chapter 9 Logout

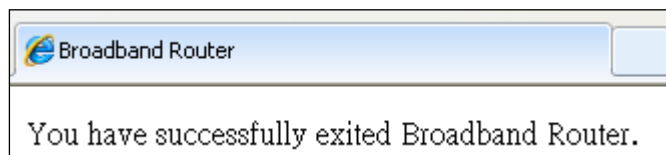
To log out from the device simply click the following icon located at the top of your screen.



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



Upon successful exit, the following message will be displayed.



## Appendix A - Firewall

### STATEFUL PACKET INSPECTION

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

### DENIAL OF SERVICE ATTACK

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

### TCP/IP/PORT/INTERFACE FILTER

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

### OUTGOING IP FILTER

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

**Example 1:**

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

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

**Example 2:**

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

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

## INCOMING IP FILTER

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

**Example 1:**

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

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

**Example 2:**

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

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

## MAC LAYER FILTER

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

**Example 1:**

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

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



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

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

### **DAYTIME PARENTAL CONTROL**

This feature restricts access of a selected LAN device to an outside Network through the VR-3030, as per chosen days of the week and the chosen times.

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

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

## Appendix B - Pin Assignments

### ETHERNET Ports (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

## Appendix C - Specifications

### Hardware Interface

RJ-11 X 1 for ADSL2+/VDSL2, RJ-45 X 1 for LAN (10/100 Base-T), Reset Button X 1, Power Switch X 1,

### WAN Interface

ADSL2+ .....Downstream : 24 Mbps      Upstream : 1.3 Mbps  
ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM

VDSL2 .....Downstream : 100 Mbps      Upstream : 60 Mbps  
ITU-T G.993.2 (supporting profile 8a, 8b, 8c, 8d, 12a, 12b, 17a)

### LAN Interface

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

### ATM Attributes

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

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

### PTM Attributes

ATM Adaptation Layer: Ethernet packet format,  
Support 8 flows,  
Support preemption and dual latency,  
Support PTM shaping

### Management

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

### Bridge Functions

Transparent bridging and learning .....IEEE 802.1d  
VLAN support .....Yes  
Spanning Tree Algorithm .....Yes  
IGMP Proxy .....Yes

### Routing Functions

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

**Security Functions**

Authentication protocols : PAP, CHAP  
TCP/IP/Port filtering rules, Port Triggering/Forwarding, Packet and MAC  
address filtering, Access Control, DoS Protection, SSH

**QoS** ..... L3 policy-based QoS, IP QoS, ToS

**Application Passthrough**

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-  
box

**Power Supply** .....Input: 100 - 240 Vac  
Output: 12 Vdc / 1.0 A

**Environment Condition**

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

**Dimensions** ..... 171 mm (W) x 37 mm (H) x 121 mm (D)

**Kit Weight**

(1\*VR-3030, 1\*RJ11 cable, 1\*RJ45 cable, 1\*power adapter) = 0.6 kg

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

## Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

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

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

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

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

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

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

## Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

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

The following sections describe each stage in turn.

### E1 ~ Layer 2 Interfaces

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

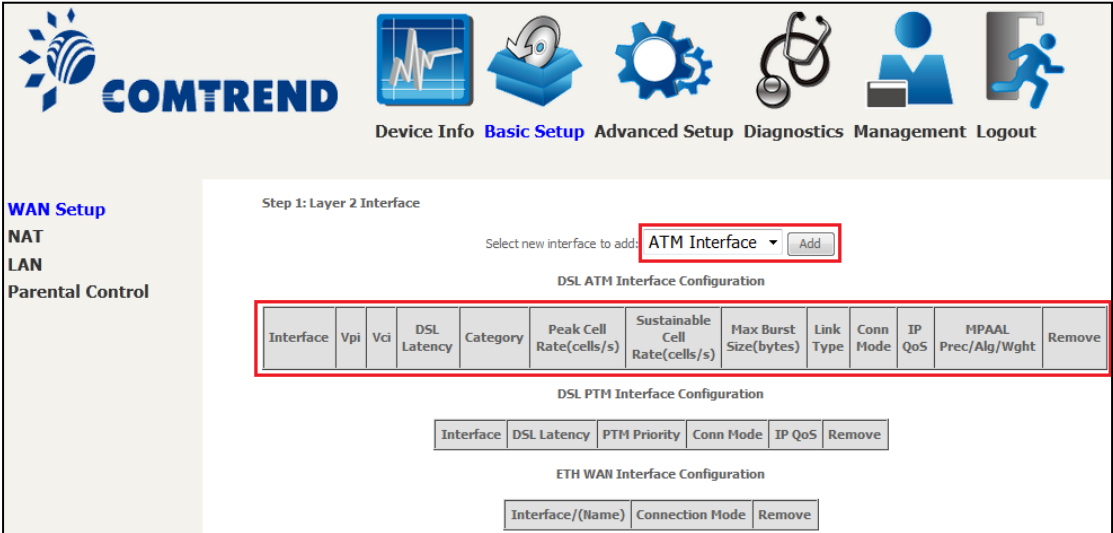
#### E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

**NOTE:** The VR-3030 supports up to 16 ATM interfaces.



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



**WAN Setup**

NAT  
LAN  
Parental Control

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	MPAAL Prec/Alg/Wght	Remove

DSL PTM Interface Configuration

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove

ETH WAN Interface Configuration

Interface/(Name)	Connection Mode	Remove

This table is provided here for ease of reference.

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

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

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

### ATM PVC Configuration

This screen allows you to configure a ATM PVC.

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

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

EoA  
 PPPoA  
 IPoA

Encapsulation Mode:  ▾

Service Category:  ▾

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

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

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

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

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

Here are the available encapsulations for each xDSL Link Type:

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



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

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

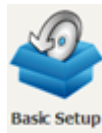
DSL ATM Interface Configuration												
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	8/WRR/1	Remove

To add a WAN connection go to [E2 ~ WAN Connections](#) WAN Connections.

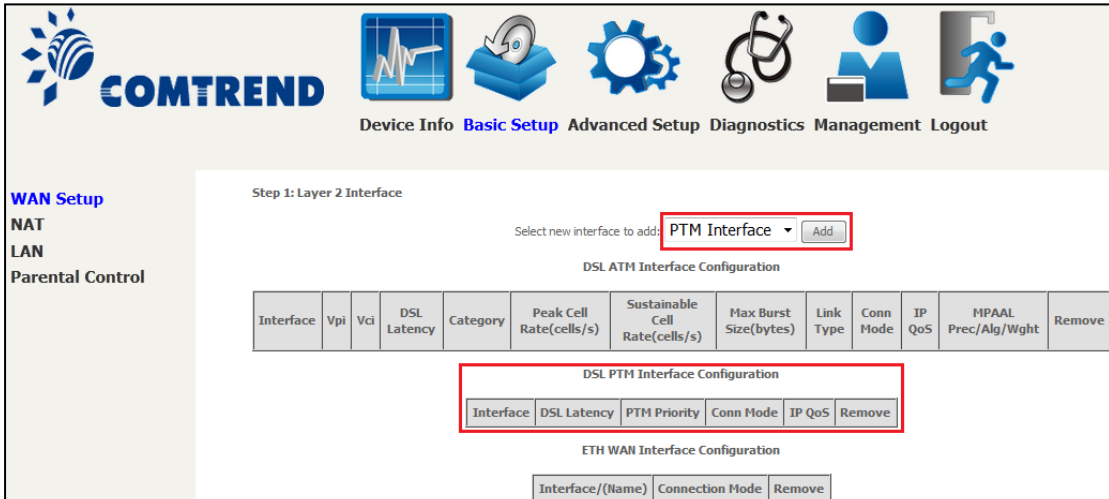
## E1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

**NOTE:** The VR-3030 supports up to four PTM interfaces.



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



The screenshot shows the WAN Setup configuration page. At the top, there is a navigation bar with icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. The main content area is titled "Step 1: Layer 2 Interface" and includes a dropdown menu to "Select new interface to add:" with "PTM Interface" selected and an "Add" button. Below this, there are three configuration tables:

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

DSL PTM Interface Configuration					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove

ETH WAN Interface Configuration		
Interface/(Name)	Connection Mode	Remove

This table is provided below for ease of reference.

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

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

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

**PTM Configuration**

This screen allows you to configure a PTM flow.

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

Default Queue Weight:  [1-63]

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

Default Queue Shaping Rate:  [Kbits/s] (blank indicates no shaping)

Default Queue Shaping Burst Size:  [bytes] (shall be >=1600)

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

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

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

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

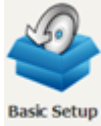
DSL PTM Interface Configuration					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="button" value="Remove"/>

To add a WAN connection go to [E2 ~ WAN Connections](#).

## E2 ~ WAN Connections

The VR-3030 supports one WAN connection for each interface, up to a maximum of 16 connections.

To setup a WAN connection follow these instructions.



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

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect:  Disable  Enable

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

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

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

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

atm0/(0\_0\_35) ▾

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

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

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

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

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

- (1) [E2.1 PPP over ETHERNET \(PPPoE\) – IPv4](#)
- (2) [E2.2 IP over ETHERNET \(IPoE\) – IPv4](#)
- (3) [E2.3 Bridging – IPv4](#)
- (4) [E2.4 PPP over ATM \(PPPoA\) – IPv4](#)
- (5) [E2.5 IP over ATM \(IPoA\) – IPv4](#)
- (6) [E2.6 PPP over ETHERNET \(PPPoE\) – IPv6](#)
- (7) [E2.7 IP over ETHERNET \(IPoE\) – IPv6](#)
- (8) Bridging – IPv6 (Not Supported)
- (9) [E2.8 PPP over ATM \(PPPoA\) – IPv6](#)
- (10) IPoA – IPv6 (Not Supported)

The subsections that follow continue the WAN service setup procedure.

## E2.1 PPP over ETHERNET (PPPoE) – IPv4

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

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

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

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO** ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

The settings shown above are described below.

### PPP SETTINGS

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

### **ENABLE FULLCONE NAT**

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

### **DIAL ON DEMAND**

The VR-3030 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

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

### **PPP IP EXTENSION**

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

PPP IP Extension does the following:

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

### **ENABLE NAT**

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

### **ENABLE FIREWALL**

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

### **USE STATIC IPv4 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in [Section 3.2](#).

**FIXED MTU**

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

**ENABLE PPP DEBUG MODE**

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

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

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

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The VR-3025u supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

**ENABLE IGMP MULTICAST PROXY**

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

**NO MULTICAST VLAN FILTER**

Tick the checkbox  to Enable/Disable multicast VLAN filter.

**Enable WAN interface with base MAC**

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

---

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

**Routing -- Default Gateway**

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

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

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



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

**DNS Server Configuration**

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

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

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

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	PPPoE
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

## E2.2 IP over ETHERNET (IPoE) – IPv4

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

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

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

**WAN IP Settings**

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

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

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

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

**Network Address Translation Settings**

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

Enable NAT

Enable Fullcone NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

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

Enable WAN interface with base MAC

### **ENABLE NAT**

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

### **ENABLE FULLCONE NAT**

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

### **ENABLE FIREWALL**

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

### **ENABLE IGMP MULTICAST**

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

### **Enable WAN interface with base MAC**

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

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

### Routing -- Default Gateway

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

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

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

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

**DNS Server Configuration**

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

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

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

Selected DNS Server Interfaces

atm0.1

->

<-

Available WAN Interfaces

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	IPoE
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

## E2.3 Bridging – IPv4

**NOTE:** This connection type is not available on the Ethernet WAN interface.

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

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

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

**WAN Setup - Summary**

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

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

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

**NOTE:** If this bridge connection is your only WAN service, the VR-3030 will be inaccessible for remote management or technical support from the WAN.



## E2.4 PPP over ATM (PPPoA) – IPv4

WAN Service Configuration

Enter Service Description:

Network Protocol Selection:

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

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

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.  
NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:

PPP Password:

Authentication Method: **AUTO** ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

Fixed MTU

MTU:

Enable PPP Debug Mode

**Multicast Proxy**

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

## PPP SETTINGS

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

### **ENABLE FULLCONE NAT**

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

### **DIAL ON DEMAND**

The VR-3030 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

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

### **PPP IP EXTENSION**

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

PPP IP Extension does the following:

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

### **ENABLE NAT**

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

### **ENABLE FIREWALL**

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

### **USE STATIC IPv4 ADDRESS**

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

**Fixed MTU**

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

**ENABLE PPP DEBUG MODE**

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

**ENABLE IGMP MULTICAST PROXY**

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

**NO MULTICAST VLAN FILTER**

Tick the checkbox  to Enable/Disable multicast VLAN filter.

**Enable WAN interface with base MAC**

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

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

**Routing -- Default Gateway**

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
pppoa0	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	
	<input type="button" value="Back"/> <input type="button" value="Next"/>	

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

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

### DNS Server Configuration

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

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

Selected DNS Server Interfaces		Available WAN Interfaces
pppoa0	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

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

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click the **Reboot** button.

## E2.5 IP over ATM (IPoA) – IPv4

**WAN Service Configuration**

Enter Service Description:

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

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

**WAN IP Settings**

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

WAN IP Address:

WAN Subnet Mask:

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

**Network Address Translation Settings**

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

Enable NAT

Enable Fullcone NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

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

Enable WAN interface with base MAC

### **ENABLE NAT**

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

### **ENABLE FULLCONE NAT**

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

### **ENABLE FIREWALL**

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

### **ENABLE IGMP MULTICAST**

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

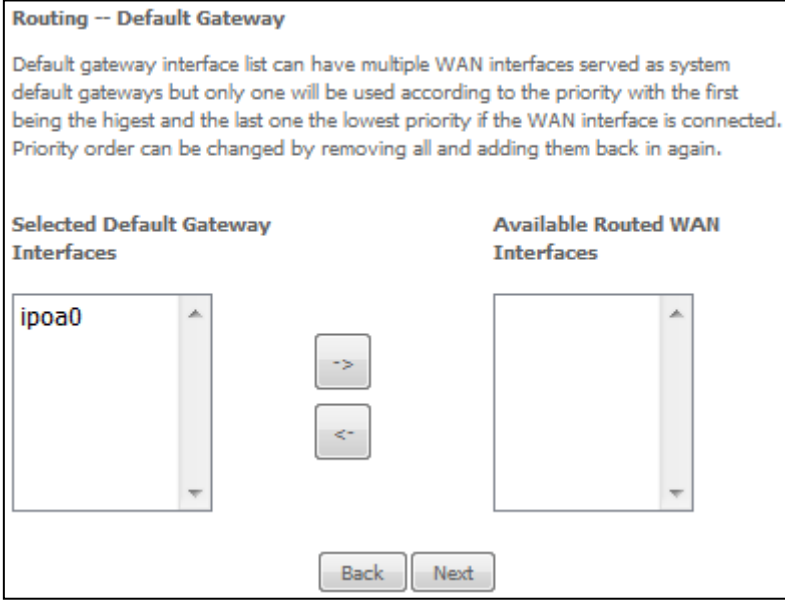


### Enable WAN interface with base MAC

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

---

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



**Routing -- Default Gateway**

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

**Selected Default Gateway Interfaces**

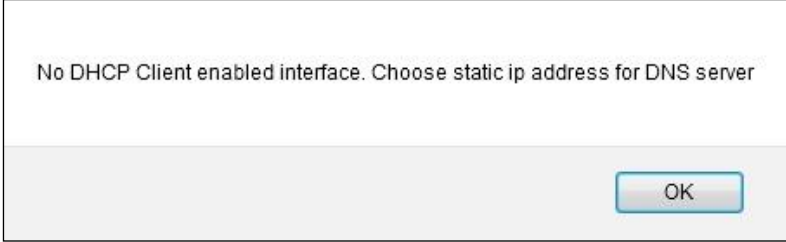
ipoa0

**Available Routed WAN Interfaces**

Back Next

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

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



No DHCP Client enabled interface. Choose static ip address for DNS server

OK

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

**DNS Server Configuration**

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

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

Selected DNS Server Interfaces

->

<-

Available WAN Interfaces

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

Primary DNS server:

Secondary DNS server:

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

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	IPoA
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

## E2.6 PPP over ETHERNET (PPPoE) – IPv6

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

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

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

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:   
PPP Password:   
PPPoE Service Name:   
Authentication Method: **AUTO** ▼

- Enable Fullcone NAT
  - Dial on demand (with idle timeout timer)
  - PPP IP extension
  - Enable Firewall
  - Use Static IPv4 Address
  - Use Static IPv6 Address
  - Enable IPv6 Unnumbered Model
  - Launch Dhcp6c for Address Assignment (IANA)
  - Launch Dhcp6c for Prefix Delegation (IAPD)
  - Fixed MTU
- MTU:
- Enable PPP Debug Mode
  - Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

- Enable IGMP Multicast Proxy
- No Multicast VLAN Filter
- Enable MLD Multicast Proxy

**WAN interface with base MAC.**

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

- Enable WAN interface with base MAC

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

The settings shown above are described below.

### **PPP SETTINGS**

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

### **ENABLE FULLCONE NAT**

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

### **DIAL ON DEMAND**

The VR-3030 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

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

### **PPP IP EXTENSION**

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

PPP IP Extension does the following:

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

### **ENABLE FIREWALL**

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

### **USE STATIC IPv4 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).

### **USE STATIC IPv6 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv6 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).

### **ENABLE IPv6 UNNUMBERED MODEL**

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

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

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

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

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

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

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

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

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources. An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

### **FIXED MTU**

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

**ENABLE PPP DEBUG MODE**

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

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

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

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The VR-3030 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

**Enable IGMP Multicast Proxy**

Tick the checkbox  to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

**No Multicast VLAN Filter**

Tick the checkbox  to Enable/Disable multicast VLAN filter.

**ENABLE MLD MULTICAST PROXY**

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

**WAN interface with base MAC**

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

---

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

**Routing -- Default Gateway**

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

<b>Selected Default Gateway Interfaces</b>		<b>Available Routed WAN Interfaces</b>
ppp0.1	 ->  <-	

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

Selected WAN Interface

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



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

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

**DNS Server Configuration**

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

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

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

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

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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

## E2.7 IP over ETHERNET (IPoE) – IPv6

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

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

**STEP 2:** The WAN IP settings screen provides access to the DHCP server settings.

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

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

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

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

**WAN IP Settings**

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

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

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

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Dhcpv6 Rapid Commit

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

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

WAN Next-Hop IPv6 Address:

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

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

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

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

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

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

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

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

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

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources. An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

### **DHCP6C FOR RAPID COMMIT**

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

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

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

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

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

**Network Address Translation Settings**

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

Enable NAT

Enable Firewall

**IGMP Multicast**

Enable IGMP Multicast

Enable MLD Multicast Proxy

**WAN interface with base MAC.**

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

Enable WAN interface with base MAC

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

### **ENABLE NAT**

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

### **ENABLE FIREWALL**

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

### **Enable IGMP Multicast**

Tick the checkbox  to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

### **ENABLE MLD MULTICAST PROXY**

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

### WAN interface with base MAC

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

**STEP 4:** To choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).

**Routing -- Default Gateway**

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

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

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

Selected WAN Interface:

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

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

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

**DNS Server Configuration**

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

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

Selected DNS Server Interfaces		Available WAN Interfaces
atm0.1	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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



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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	IPoE
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

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

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

## E2.8 PPP over ATM (PPPoA) – IPv6

**STEP 1:** Select IPv6 Only from the drop-down box at the bottom of this screen and click **Next**.

**WAN Service Configuration**

Enter Service Description:

Internet Protocol Selection:

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

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.  
NOTE: IP extension can not be enabled when you enable 3G backup.

PPP Username:

PPP Password:

Authentication Method: **AUTO**

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable Firewall

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Fixed MTU

MTU:

Enable PPP Debug Mode

### Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

Enable MLD Multicast Proxy

### WAN interface with base MAC.

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

Enable WAN interface with base MAC

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

### PPP SETTINGS

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

### ENABLE FULLCONE NAT

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

### DIAL ON DEMAND

The VR-3030 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text" value="0"/>

### PPP IP EXTENSION

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

PPP IP Extension does the following:

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

### ENABLE FIREWALL

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

### USE STATIC IPv4 ADDRESS

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

### **USE STATIC IPv6 ADDRESS**

Unless your service provider specially requires it, do not select this checkbox . If selected, enter the static IP address in the **IPv6 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in section [3.2 IP Configuration](#).

### **ENABLE IPv6 UNNUMBERED MODEL**

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

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

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

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

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

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

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

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

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources. An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

### **FIXED MTU**

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

### ENABLE PPP DEBUG MODE

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

### Enable IGMP Multicast Proxy

Tick the checkbox  to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

### No Multicast VLAN Filter

Tick the checkbox  to Enable/Disable multicast VLAN filter.

### ENABLE MLD MULTICAST PROXY

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

### WAN interface with base MAC

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

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

#### Routing -- Default Gateway

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
<input type="text" value="pppoa0"/>	<input type="button" value="-&gt;"/> <input type="button" value="-&lt;"/>	<input type="text"/>

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

Selected WAN Interface

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

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

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

### DNS Server Configuration

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

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

Selected DNS Server Interfaces		Available WAN Interfaces
pppoa0	<input type="button" value="-&gt;"/> <input type="button" value="&lt;-"/>	

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

Primary DNS server:

Secondary DNS server:

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

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

WAN Interface selected:

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

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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

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

**WAN Setup - Summary**

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

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

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

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