

VR-3031u

Multi-DSL Router

User Manual

Version A1.0, November 12, 2013



Preface

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

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

For product update, new product release, manual revision, or software upgrades, please visit our website at <http://www.comtrend.com>

Important Safety Instructions

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

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

CAUTION:

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



WARNING

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

Copyright

Copyright©2013 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

NOTE: This document is subject to change without notice.

Protect Our Environment



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



separate from domestic waste.

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

Table of Contents

CHAPTER 1 INTRODUCTION.....	5
CHAPTER 2 INSTALLATION.....	6
2.1 HARDWARE SETUP.....	6
2.2 LED INDICATORS.....	8
CHAPTER 3 WEB USER INTERFACE.....	10
3.1 DEFAULT SETTINGS	10
3.2 IP CONFIGURATION.....	11
3.3 WIZARD SETUP.....	13
3.4 LOGIN TO ADVANCED WEB USER INTERFACE.....	21
CHAPTER 4 DEVICE INFORMATION.....	23
4.1 WAN	24
4.2 STATISTICS.....	25
4.2.1 LAN Statistics.....	25
4.2.2 WAN Service	26
4.2.3 ATM Statistics.....	26
4.2.4 xDSL Statistics	28
4.3 ROUTE.....	34
4.4 ARP.....	35
4.5 DHCP.....	36
4.6 NAT SESSION	37
4.7 IGMP INFO.....	38
4.8 3G	39
CHAPTER 5 ADVANCED SETUP.....	40
5.1 LAYER 2 INTERFACE	40
5.1.1 ATM Interface.....	40
5.1.2 PTM Interface.....	40
5.1.3 ETH WAN INTERFACE.....	41
5.2 WAN	42
5.2.1 3G Service Setup.....	43
5.3 AUTO-DETECTION SETUP	45
5.4 NAT	46
5.4.1 Virtual Servers	46
5.4.2 Port Triggering.....	48
5.4.3 DMZ Host	50
5.4.4 IP Address Map	51
5.4.5 SIP ALG.....	53
5.4.6 IPSEC ALG.....	53
5.5 SECURITY	54
5.5.1 IP Filtering	54
5.5.2 MAC Filtering.....	57
5.6 PARENTAL CONTROL.....	59
5.6.1 Time Restriction.....	59
5.6.2 URL Filter.....	60
5.7 QUALITY OF SERVICE (QoS).....	62
5.7.1 QoS Queue Setup.....	63
5.7.2 QoS Policer	65
5.7.3 QoS Classification.....	67
5.8 ROUTING	69
5.8.1 Default Gateway.....	69
5.8.2 Static Route.....	70
5.8.3 Policy Routing	71
5.8.4 RIP.....	73
5.9 DNS	74
5.9.1 DNS Server	74
5.9.2 Dynamic DNS.....	75

5.10 DSL.....	76
5.11 UPNP.....	78
5.12 DNS PROXY/RELAY	79
5.13 PRINT SERVER	80
5.14 INTERFACE GROUPING.....	81
5.15 IPSEC	84
5.15.1 IPsec Tunnel Mode Connections	84
5.16 CERTIFICATE.....	88
5.16.1 Local.....	88
5.16.2 Trusted CA.....	90
5.17 POWER MANAGEMENT	91
5.18 MULTICAST.....	92
CHAPTER 6 WIRELESS.....	94
6.1 BASIC	94
6.2 SECURITY	96
6.3 MAC FILTER	99
6.4 WIRELESS BRIDGE.....	100
6.5 ADVANCED	101
6.6 SITE SURVEY	104
6.7 STATION INFO	105
CHAPTER 7 DIAGNOSTICS.....	106
CHAPTER 8 MANAGEMENT	108
8.1 SETTINGS.....	108
8.1.1 Backup Settings.....	108
8.1.2 Update Settings.....	108
8.1.3 Restore Default.....	109
8.2 SYSTEM LOG	110
8.3 TR-069 CLIENT	112
8.4 INTERNET TIME	114
8.5 ACCESS CONTROL	115
8.5.1 Passwords.....	115
8.5.2 Services.....	116
8.5.3 IP Address.....	117
8.6 UPDATE SOFTWARE	118
8.7 REBOOT.....	119
APPENDIX A - FIREWALL	120
APPENDIX B - PIN ASSIGNMENTS.....	123
APPENDIX C - SPECIFICATIONS.....	124
APPENDIX D - SSH CLIENT	126
APPENDIX E - WSC EXTERNAL REGISTRAR.....	127
APPENDIX F - PRINTER SERVER.....	131
APPENDIX G - CONNECTION SETUP	138

Chapter 1 Introduction

The VR-3031u is an 802.11n compliant 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-3031u comes with four 10/100 Base-T Ethernet ports, and one USB host, combining wired LAN connectivity and an integrated 802.11n WiFi WLAN Access Point (AP) for wireless connectivity.

The VR-3031u 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-3031u 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.



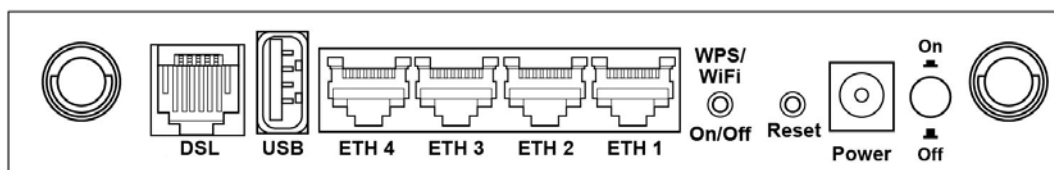
DO NOT STACK

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-3031u 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.

WPS/WiFi Button

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

Press and hold WPS-WIFI button more than 5 seconds to enable/disable WiFi.

Ethernet (LAN) Ports

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

USB Host Port (Type A)

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

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.
ETH 1 to 4	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
WLAN	Green	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.
WPS	Green	On	WPS enabled and PC connected to WLAN.
		Off	WPS disabled when WPS configured. After clients are connected to router for about 5 minutes, LED is OFF.
		Blink	The router is searching for WPS clients or WPS is un-configured.
USB	Green	On	USB mass storage, USB hub or USB printer is connected; or 3G USB dongle connection is UP.
		Off	No USB device connected.
	Red	On	3G USB dongle attached, 3G connection is DOWN.
DSL	Green	On	xDSL Link is established.
		Off	xDSL Link is not established.
		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: **admin**, password: as created in your wizard)
See section [3.3 Wizard Setup](#) for details
- Remote access (username: **admin**, password: as created in your wizard)
- WLAN access: **enabled**

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the VR-3031u 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.

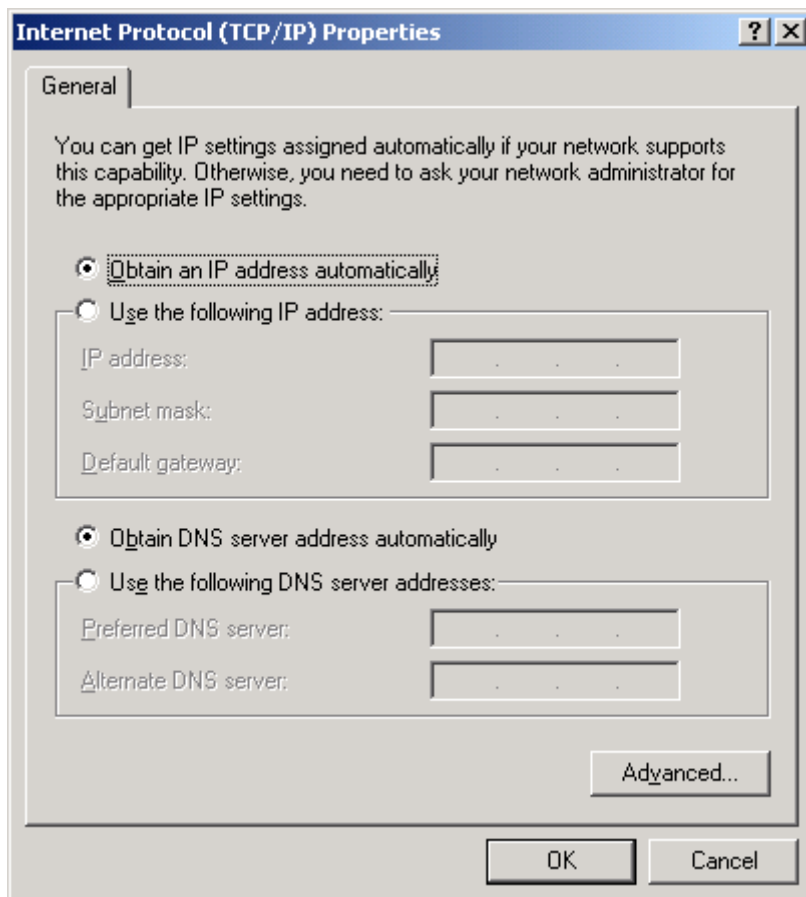
To obtain an IP address from the DHCP server, follow the steps provided below.

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.

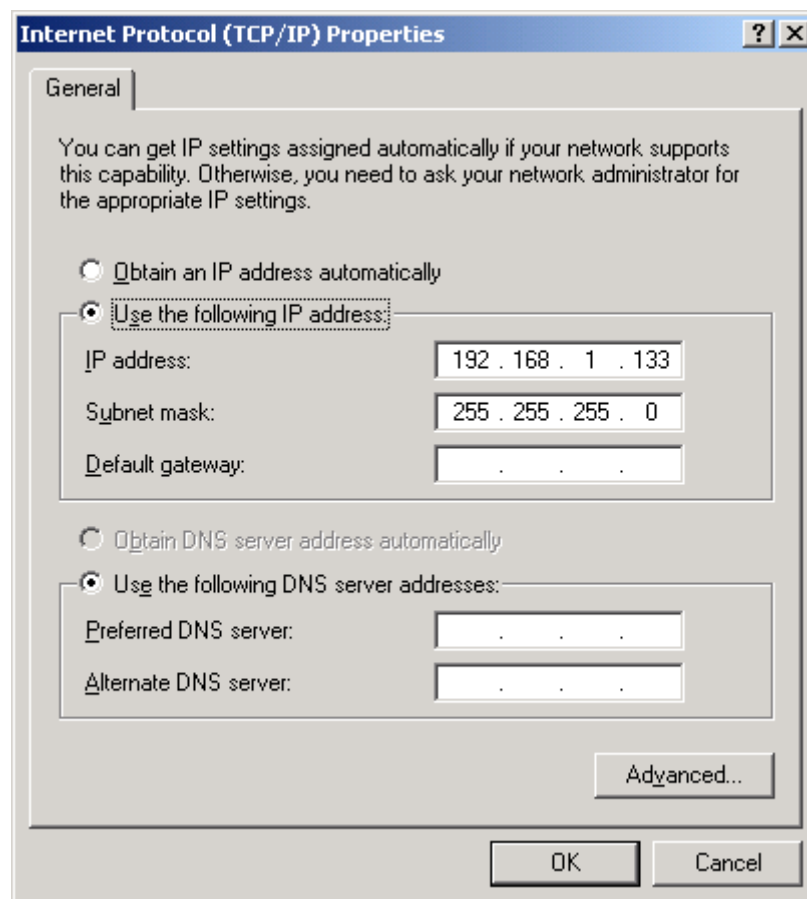
STATIC IP MODE

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.

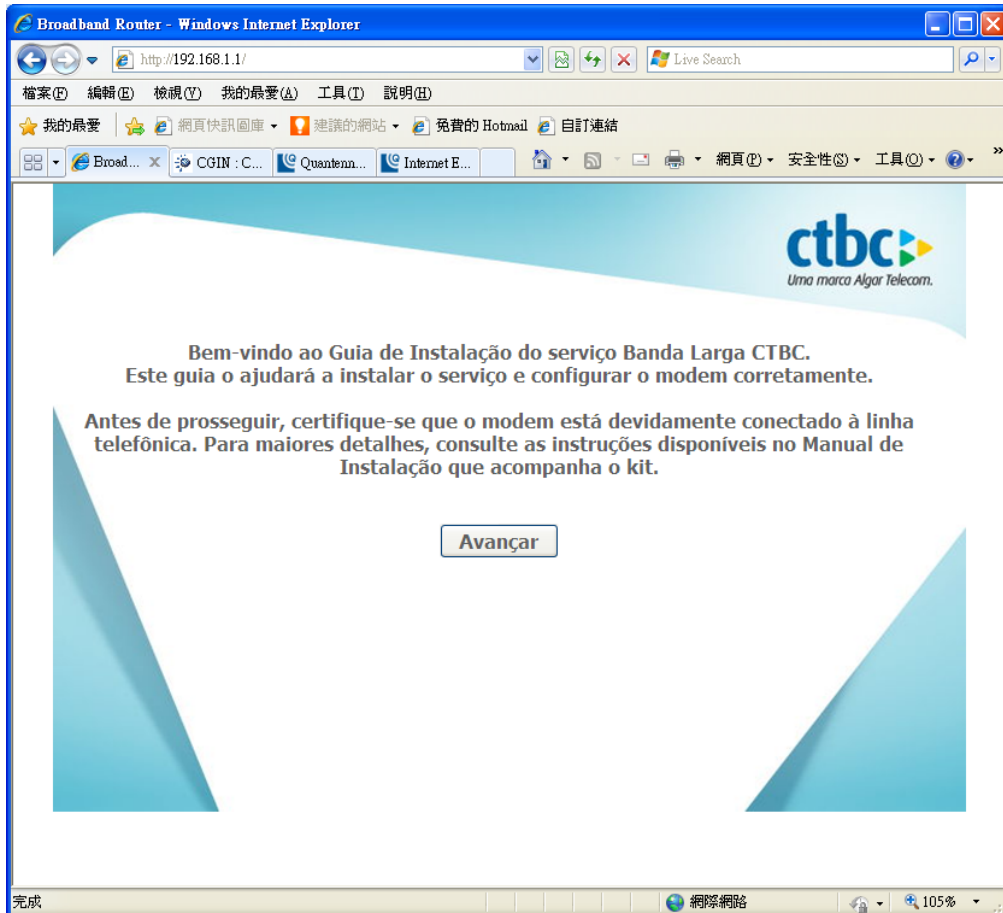
- STEP 1:** From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- STEP 2:** Select Internet Protocol (TCP/IP) **and click the** Properties button.
- STEP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

After starting the Wizard you will be brought to the Welcome page. Click the Continue button.



Set new login password and click the Continue button. The new password must have a minimum of 6 characters and a maximum of 16. Letters or numbers can be used. Passwords with characters repeated more than 2 times such as 111 or eee for example are not permitted.

Broadband Router - Windows Internet Explorer

http://192.168.1.1/

ctbc
Uma marca Algar Telecom.

Para maior segurança será necessário trocar a senha de acesso do modem. Esta senha somente será necessária caso você queira alterar alguma configuração avançada após a instalação do modem. Recomendamos o uso de uma senha robusta, portanto evite usar caracteres repetidos ou sequenciais. A senha pode ser composta por números, letras maiúsculas e/ou minúsculas. Não serão aceitos caracteres especiais (\$, %, *, @, &). Entre com uma senha de no mínimo 6 e no máximo 16 caracteres.

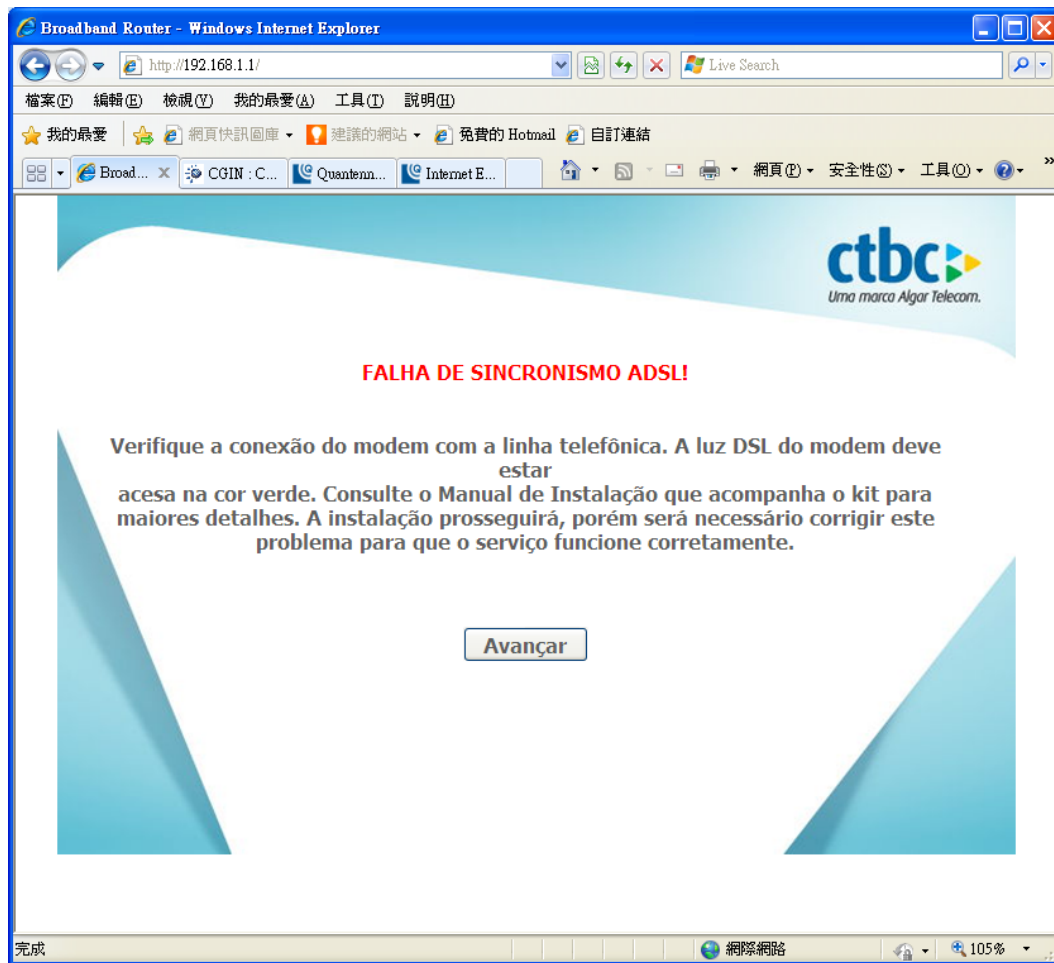
IMPORTANTE! Anote e guarde esta senha.

Usuário:

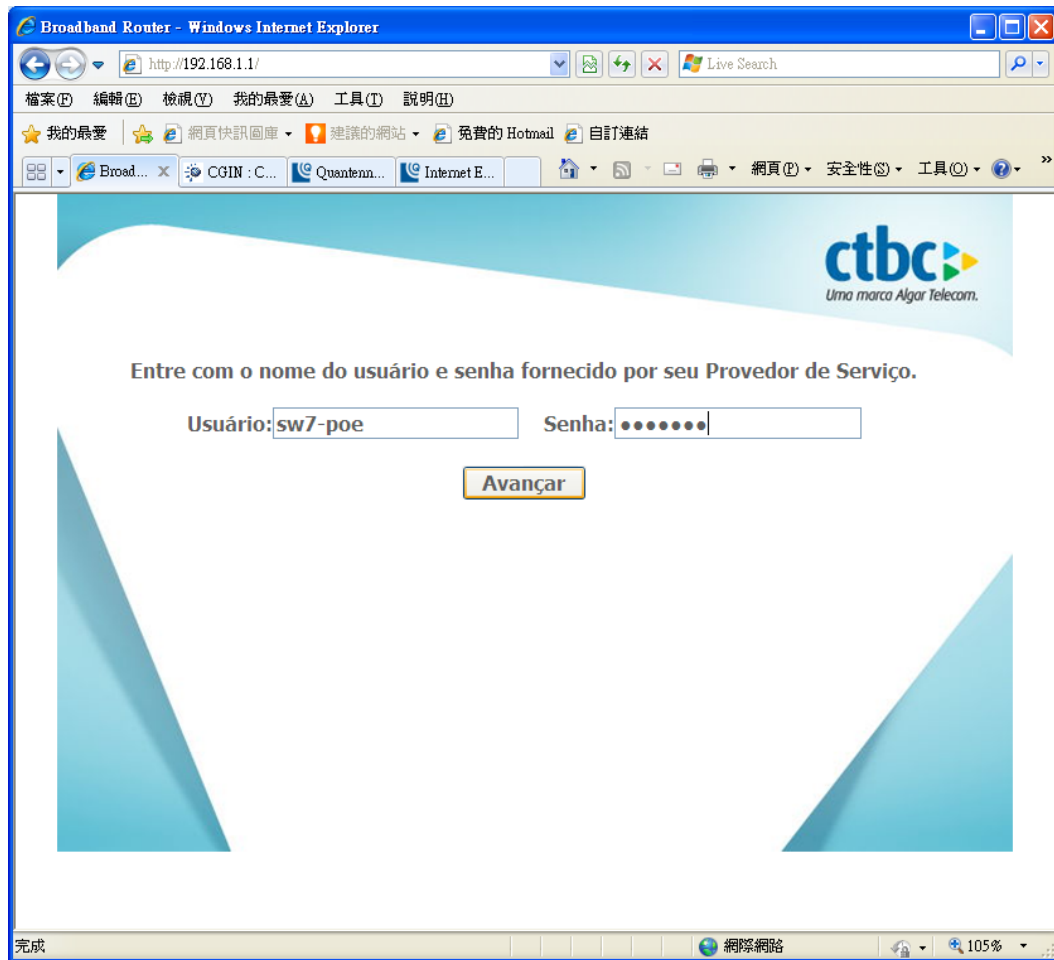
Senha:

完成 國際網路 105%

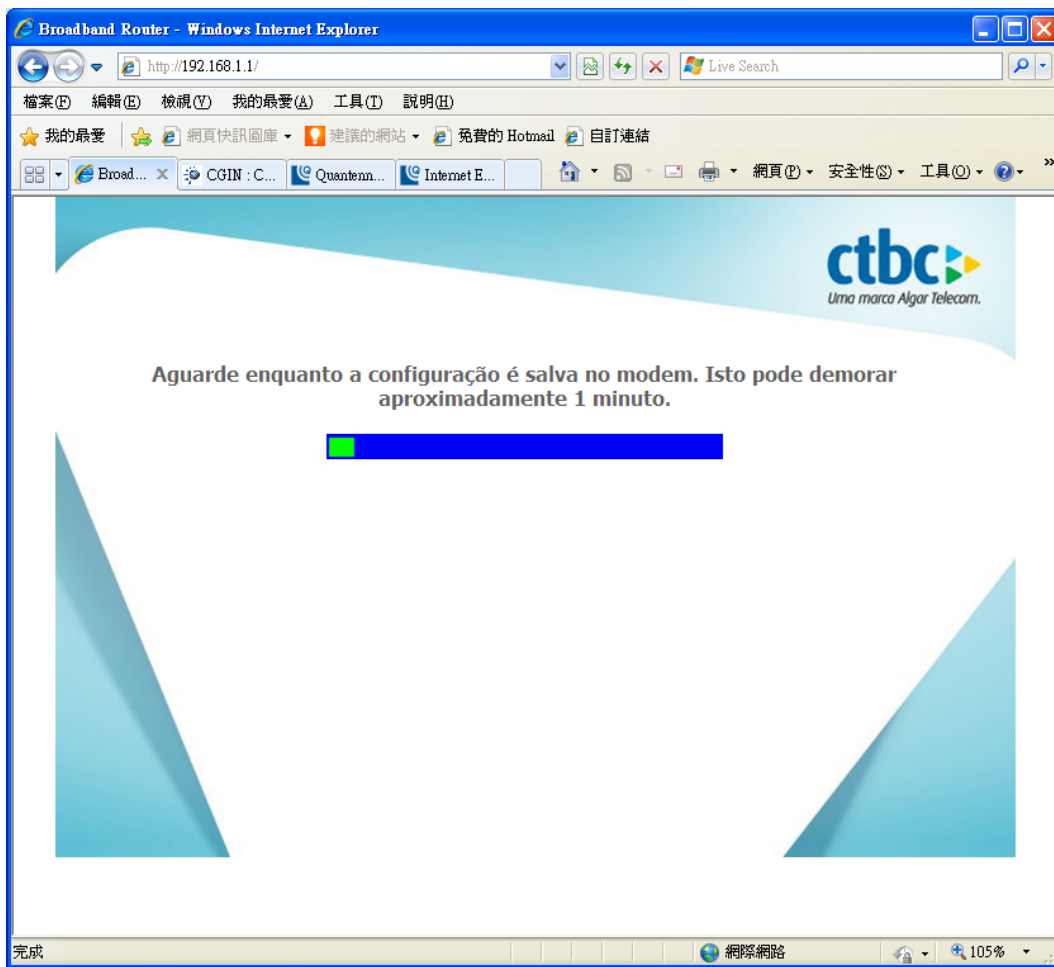
If there is no DSL connection, the following page will pop up to inform you. (For reference)



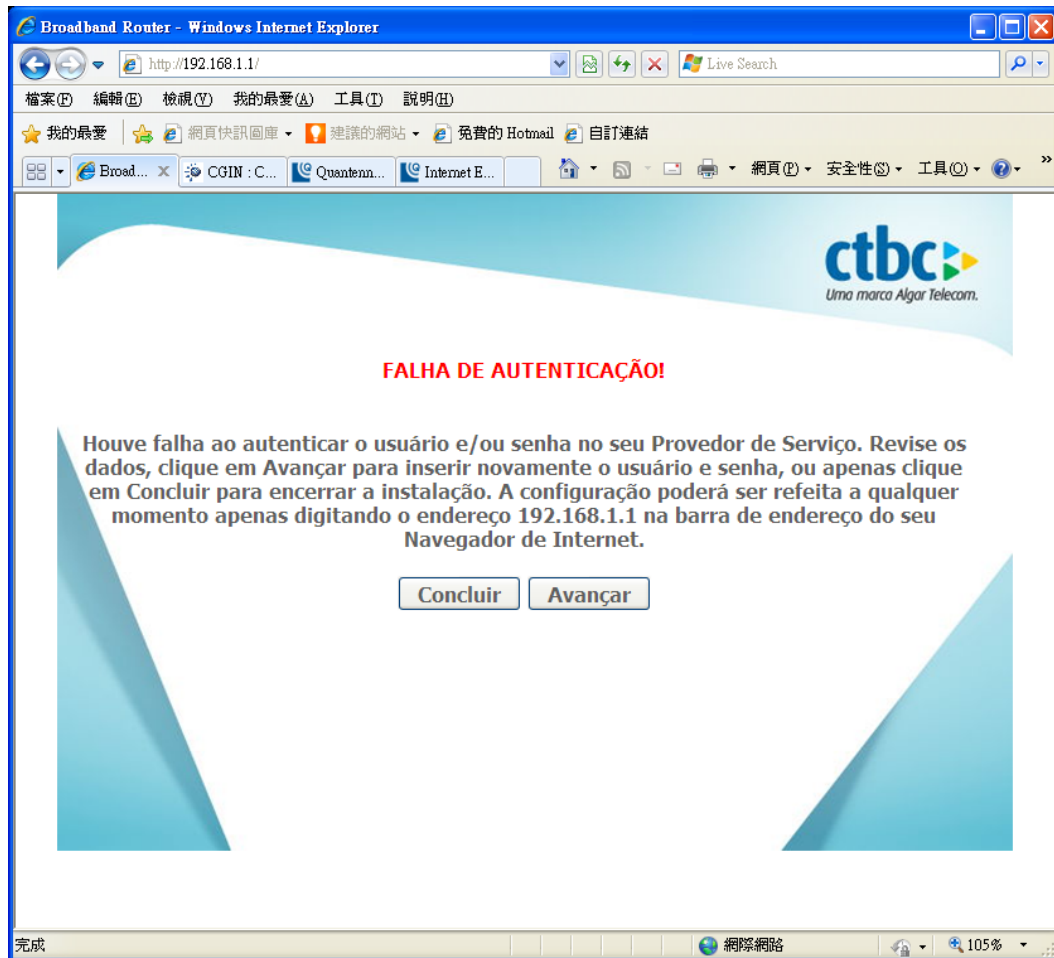
Input the Username and Password as provided by your ISP (Internet Service Provider). Click the Continue button.



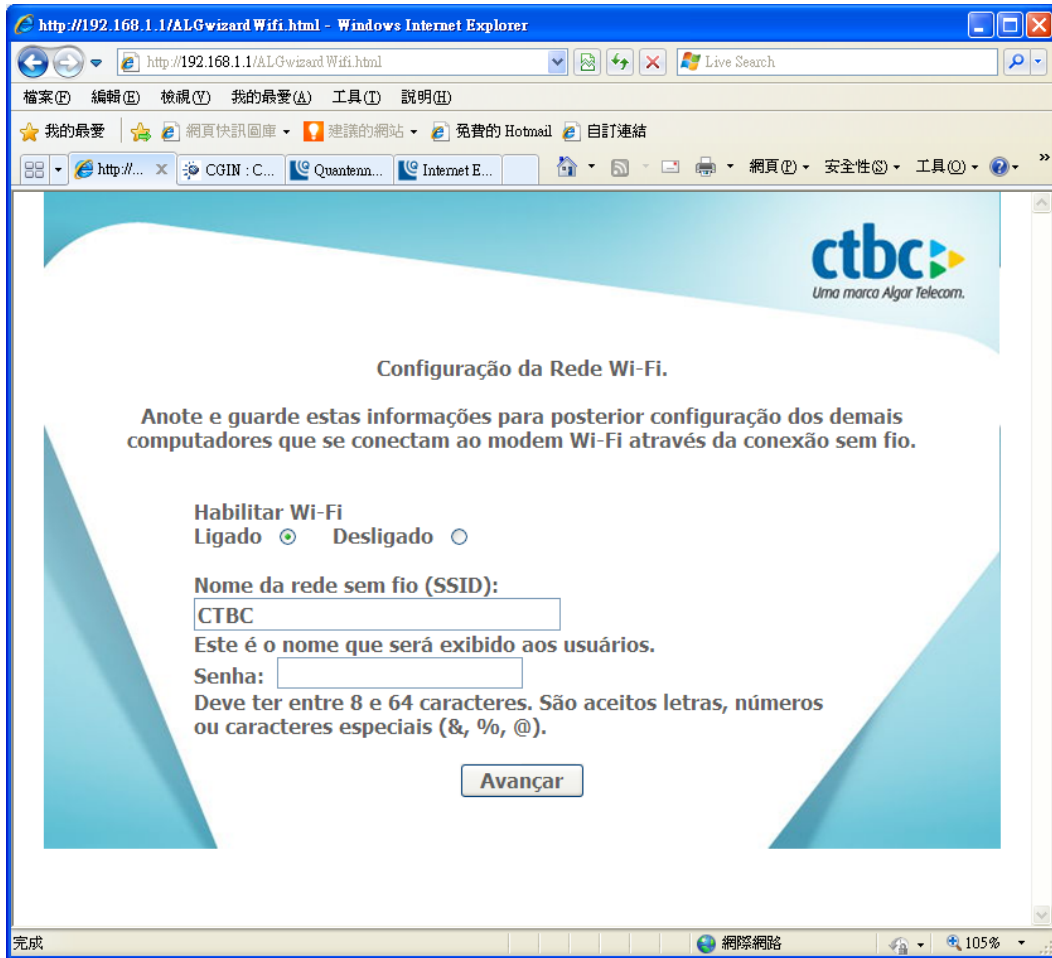
This page informs you that the settings are being saved.



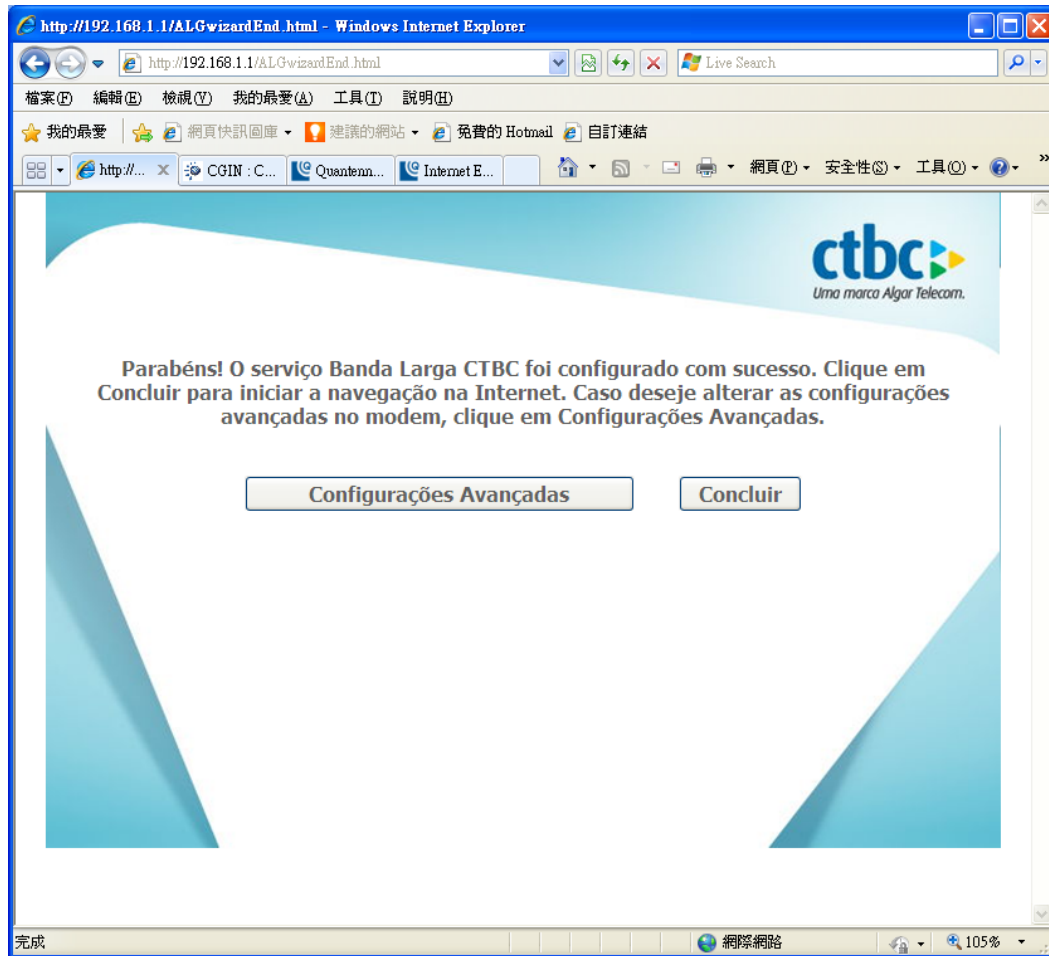
If the wrong Username and/or Password are used the following page will pop up to inform you. (For reference)



Upon Username and Password authentication, you will be asked to set a new WiFi Password. Input the new Password and click the Continue button. The new password must have a minimum of 8 characters and a maximum of 64.



If WiFi was set up correctly, it goes to end of wizard page. Click on the Advanced Configuration button to bring you to the Advanced Settings Page. If you click the Complete button you will be brought to the ctbc company web page.



3.4 Login to Advanced Web User Interface

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

NOTE: Before accessing this page, make sure to complete the Wizard Setup.

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/main.html>

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.

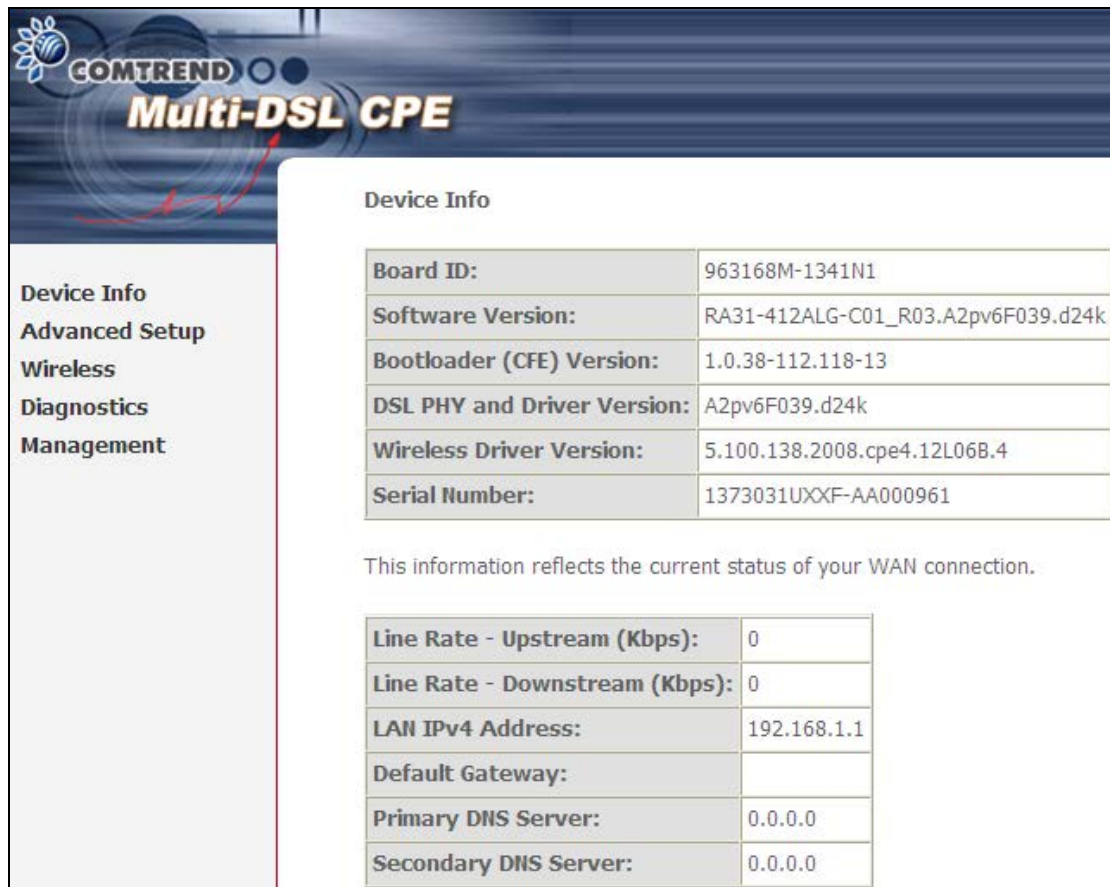
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as created in the Wizard Setup. See Section [3.3 Wizard Setup](#) for details.



Click **OK** to continue.

NOTE: The login password can be changed by using the wizard.

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



The screenshot displays the GOMTREND Multi-DSL CPE web interface. The top header features the GOMTREND logo and the product name "Multi-DSL CPE". On the left, a navigation menu lists "Device Info", "Advanced Setup", "Wireless", "Diagnostics", and "Management". The main content area is titled "Device Info" and contains a table with the following details:

Board ID:	963168M-1341N1
Software Version:	RA31-412ALG-C01_R03.A2pv6F039.d24k
Bootloader (CFE) Version:	1.0.38-112.118-13
DSL PHY and Driver Version:	A2pv6F039.d24k
Wireless Driver Version:	5.100.138.2008.cpe4.12L06B.4
Serial Number:	1373031UXXF-AA000961

Below this table, a note states: "This information reflects the current status of your WAN connection." This is followed by another table showing WAN connection details:

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

Chapter 4 Device Information

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

NOTE: The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

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

The Device Info Summary screen displays at startup.

Device Info

Board ID:	963168M-1341N1
Software Version:	RA31-412ALG-C01_R03.A2pv6F039.d24k
Bootloader (CFE) Version:	1.0.38-112.118-13
DSL PHY and Driver Version:	A2pv6F039.d24k
Wireless Driver Version:	5.100.138.2008.cpe4.12L06B.4
Serial Number:	1373031UXXF-AA000961

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

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

4.1 WAN

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

WAN Info									
Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address	PPP connect/disconnect
ppp0.1	pppoe_ATM_0	PPPoE	Disabled	Disabled	Enabled	Disabled	Unconfigured		
ppp1.1	pppoe_PTM_0	PPPoE	Disabled	Disabled	Enabled	Disabled	Unconfigured		

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
IGMP	Shows Internet Group Management Protocol (IGMP) 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
PPP connect/disconnect	Shows the PPP connection status

4.2 Statistics

This selection provides LAN, WAN, ATM/PTM 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.

The screenshot shows the 'Statistics -- LAN' page. On the left is a navigation menu with options: Device Info, Summary, WAN, Statistics, LAN (highlighted), WAN Service, xTM, xDSL, Route, and ARP. The main content area displays a table with the following data:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ENET1	487135	4565	0	0	762091	2646	0	0
ENET2	0	0	0	0	0	0	0	0
ENET3	0	0	0	0	0	0	0	0
ENET4	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

Below the table is a 'Reset Statistics' button.

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

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.

COMTREND Multi-DSL CPE

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0.1	pppoe_ATM_0	0	0	0	0	0	0	0	0
ppp1.1	pppoe_PTM_0	0	0	0	0	0	0	0	0

Reset Statistics

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

4.2.3 ATM Statistics

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

COMTREND Multi-DSL CPE

Interface Statistics

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

Reset

ATM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

4.2.4 xDSL Statistics

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

VDSL

Statistics -- xDSL

Mode:	VDSL2		
Traffic Type:	PTM		
Status:	Up		
Link Power State:	L0		
	Downstream	Upstream	
PhyR Status:	Off	Off	
Line Coding(Trellis):	On	Off	
SNR Margin (0.1 dB):	177	70	
Attenuation (0.1 dB):	0	0	
Output Power (0.1 dBm):	128	84	
Attainable Rate (Kbps):	152637	61599	
	Path 0	Path 1	
	Downstream	Upstream	Downstream Upstream
Rate (Kbps):	104997	61109	0 0
B (# of bytes in Mux Data Frame):	79	239	0 0
M (# of Mux Data Frames in an RS codeword):	1	1	0 0
T (# of Mux Data Frames in an OH sub-frame):	59	64	0 0
R (# of redundancy bytes in the RS codeword):	14	0	0 0
S (# of data symbols over which the RS code word spans):	0.0242	0.1250	0.0000 0.0000
L (# of bits transmitted in each data symbol):	31016	15360	0 0
D (interleaver depth):	1055	1	0 0
I (interleaver block size in bytes):	94	120	0 0
N (RS codeword size):	94	240	0 0
Delay (msec):	6	0	0 0
INP (DMT symbol):	1.50	0.00	0.00 0.00
OH Frames:	217555	32471	0 0
OH Frame Errors:	0	0	0 0
RS Words:	38351946	2278816	0 0
RS Correctable Errors:	0	2	0 0
RS Uncorrectable Errors:	0	0	0 0
HEC Errors:	0	0	0 0
OCD Errors:	0	0	0 0
LCD Errors:	0	0	0 0
Total Cells:	37844654	0	0 0
Data Cells:	14	0	0 0
Bit Errors:	0	0	0 0
Total ES:	0	0	
Total SEs:	0	0	
Total UAs:	32	32	

ADSL

COMTREND Multi-DSL CPE

Statistics -- xDSL

Mode:	ADSL_2plus			
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):	109	77		
Attenuation (0.1 dB):	35	32		
Output Power (0.1 dBm):	115	71		
Attainable Rate (Kbps):	27464	1319		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	25904	1311	3808	416
MSGc (# of bytes in overhead channel message):	56	13	0	0
B (# of bytes in Mux Data Frame):	119	13	0	0
M (# of Mux Data Frames in FEC Data Frame):	2	16	0	0
T (Mux Data Frames over sync bytes):	7	10	0	0
R (# of check bytes in FEC Data Frame):	14	8	0	0
S (ratio of FEC over PMD Data Frame length):	0.2961	5.4269	0.0000	0.0000
L (# of bits in PMD Data Frame):	6862	342	0	0
D (interleaver depth):	64	8	0	0
Delay (msec):	5	11	0	0
INP (DMT symbol):	0.50	0.50	0.00	0.00
Super Frames:	7616	7502	0	0
Super Frame Errors:	0	0	0	0
RS Words:	1652398	89266	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	2	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	4681233	226405	0	0
Data Cells:	120	0	0	0
Bit Errors:	348	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	27	27		

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

Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin

Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain
Rate (Kbps)	Current sync rates downstream/upstream

In VDSL mode, the following section is inserted.

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

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

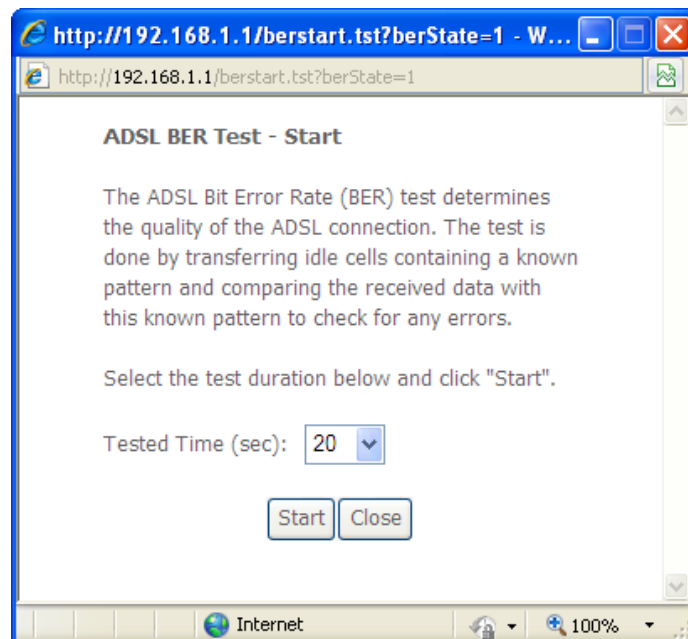
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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

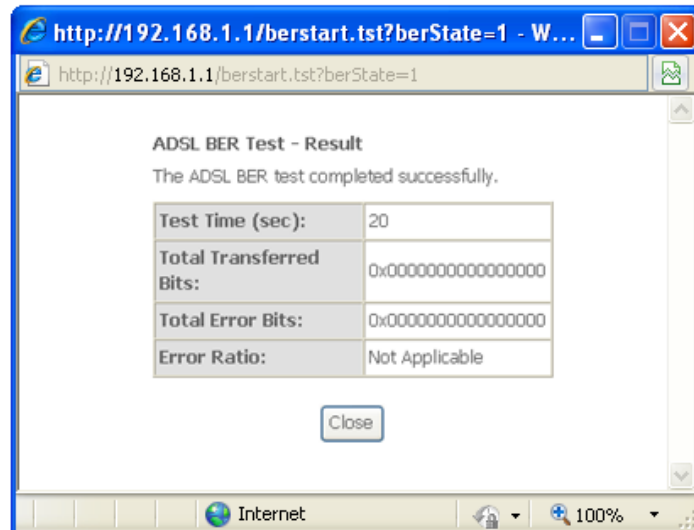
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

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.

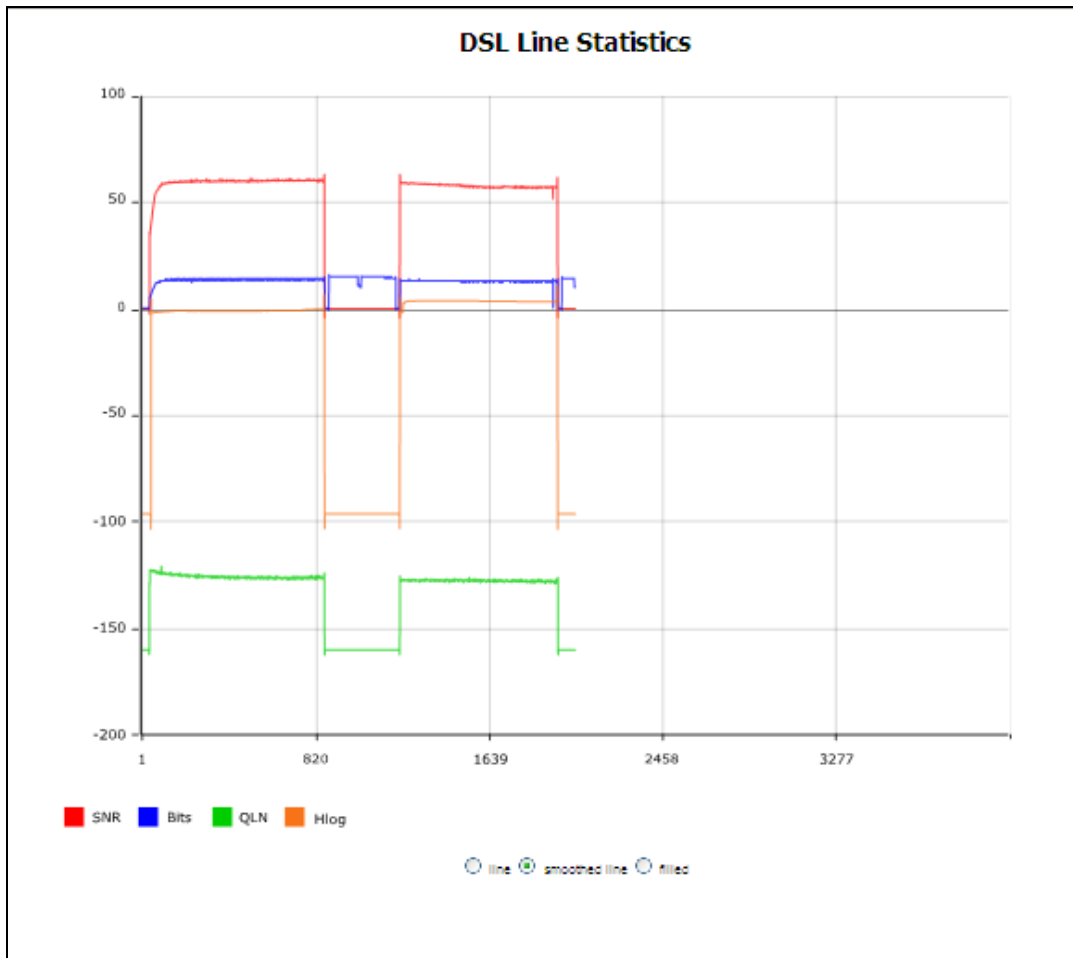


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



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.



4.3 Route

Choose **Route** to display the routes that the VR-3031u has found.

Device Info -- Route

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

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

Field	Description
Destination	Destination network or destination host
Gateway	Next hub 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 Multi-DSL CPE web interface. The main content area is titled "Device Info -- ARP" and displays a table with the following data:

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

On the left side of the interface, there is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, Route, and **ARP** (highlighted in red).

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 GOMTREND Multi-DSL CPE web interface. On the left is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP, DHCP, and DHCPv4 (highlighted in red). The main content area is titled "Device Info -- DHCP Leases" and contains a table with the following data:

Hostname	MAC Address	IP Address	Expires In
trevorowens01	00:25:11:af:fd:f8	192.168.1.2	43 seconds

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

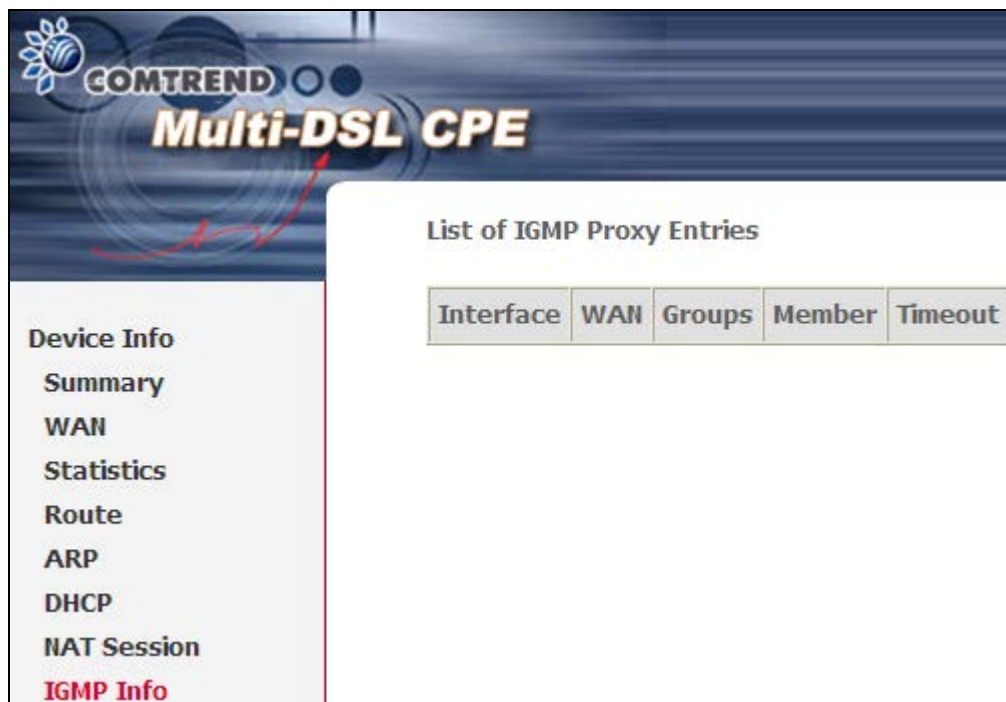
4.6 NAT Session

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

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.2	3541	157.56.52.21	80	tcp	59
192.168.1.2	3639	157.55.235.146	80	tcp	116
192.168.1.2	3605	91.190.216.57	80	tcp	93
192.168.1.2	3602	213.199.179.147	80	tcp	91
192.168.1.2	3509	91.190.216.55	80	tcp	2
192.168.1.2	3565	111.221.74.19	80	tcp	69
192.168.1.2	3549	65.55.223.40	80	tcp	65

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

4.7 IGMP Info



COMTREND
Multi-DSL CPE

List of IGMP Proxy Entries

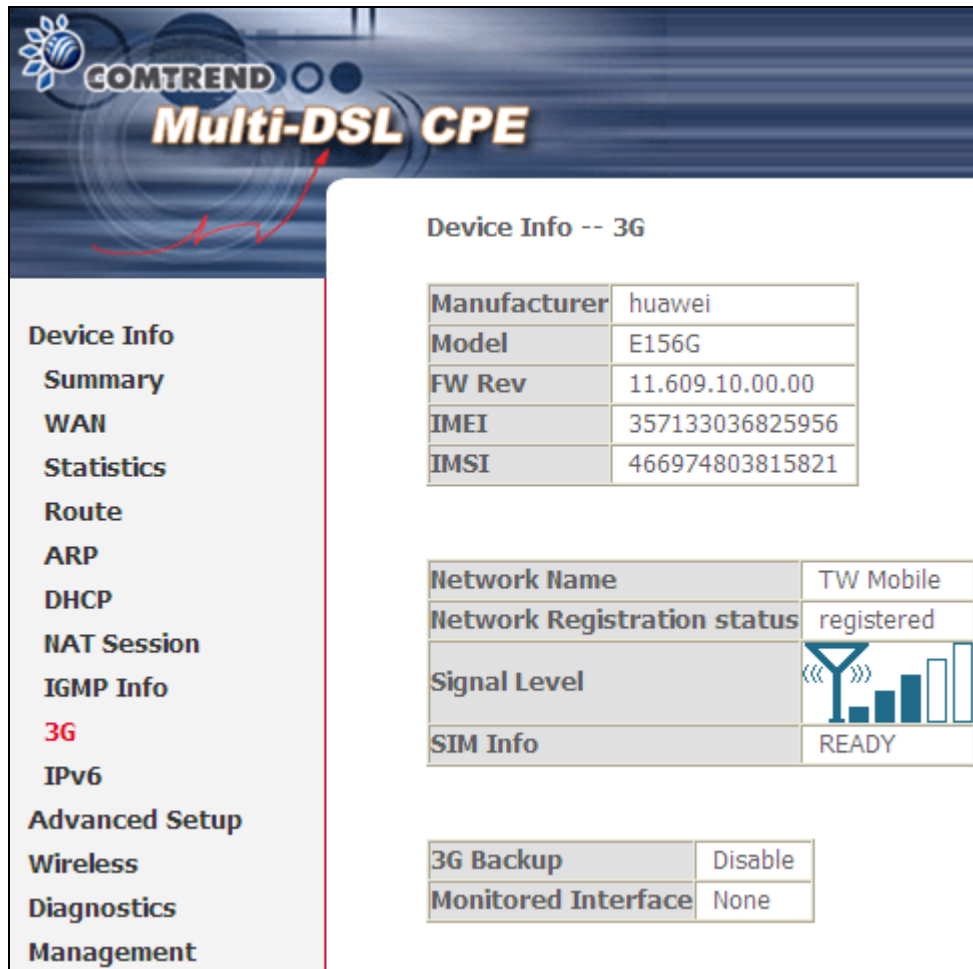
Interface	WAN	Groups	Member	Timeout
-----------	-----	--------	--------	---------

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

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 3G


Device needs to be attached in order to display the information for the 3G device.



The screenshot displays the COMTREND Multi-DSL CPE web interface. The top header features the COMTREND logo and the product name "Multi-DSL CPE". A left-hand navigation menu lists various configuration sections, with "3G" highlighted in red. The main content area is titled "Device Info -- 3G" and contains several data tables and a signal level indicator.

Device Info -- 3G

Manufacturer	huawei
Model	E156G
FW Rev	11.609.10.00.00
IMEI	357133036825956
IMSI	466974803815821

Network Name	TW Mobile
Network Registration status	registered
Signal Level	
SIM Info	READY

3G Backup	Disable
Monitored Interface	None

Chapter 5 Advanced Setup

5.1 Layer 2 Interface

The ATM, PTM and ETH WAN interface screens are described here.

5.1.1 ATM Interface

Add or remove ATM interface connections here.

COMTREND Multi-DSL CPE

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

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	<input type="checkbox"/>

Add Remove

Click **Add** to create a new ATM interface (see [Appendix G - 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**.

5.1.2 PTM Interface

Add or remove PTM interface connections here.

COMTREND Multi-DSL CPE

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

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

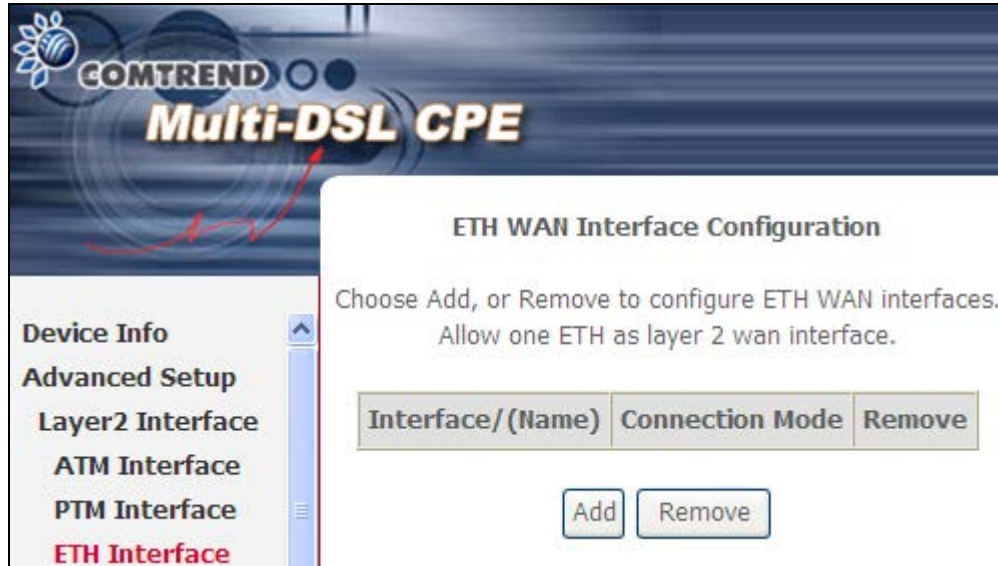
Add Remove

Click **Add** to create a new connection (see [Appendix G](#)). To remove a connection, select its Remove column radio button and click **Remove**.

5.1.3 ETH WAN INTERFACE

This screen displays the Ethernet WAN Interface configuration.

NOTE: This option only applies to models with an Ethernet WAN port.



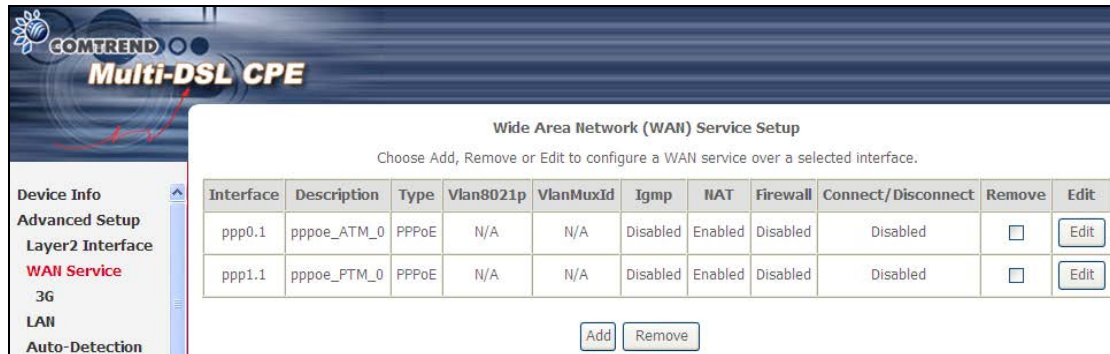
Click **Add** to create a new connection (see [Appendix G](#)).

NOTE: One Ethernet WAN interface can be created and saved in flash memory.

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

5.2 WAN

This screen allows for the configuration of WAN interfaces.



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

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

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
Connect/Disconnect	Shows the status of PPP manual mode If PPP Manual mode is enabled, the connect/disconnect in Device Info->Wan can be used to establish/terminate a PPP connection
Remove	Select interfaces to remove

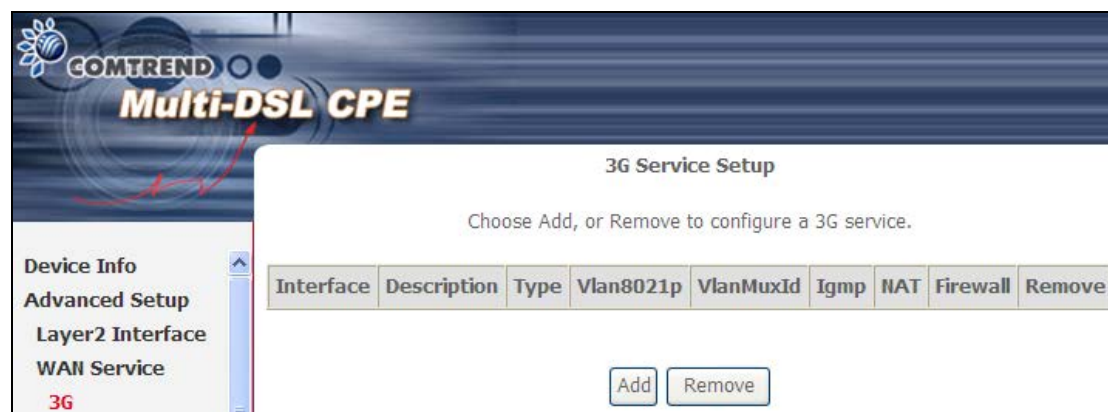
To remove a connection, select its Remove column radio button and click **Remove**.

To **Add** a new WAN connection, click the **Add** button and follow the instructions.

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

5.2.1 3G Service Setup

This page is used to configure 3G service, and let route access internet via 3G. If users don't insert 3G dongle, users can not configure the 3G WAN interface.



Click the **Add** button to create a new connection.

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
Remove	Select interfaces to remove

COMTREND
Multi-DSL CPE

WAN Service Configuration

3G WAN service type:
 PPP over Usb(TTY)

Service Description:

3G Configuration

APN:

Dial Number:

Input your Access Point Name and Dial Number and click **Next**. For further setup instructions please see [Appendix G - Connection Setup](#).

5.3 Auto-detection setup

COMTREND Multi-DSL CPE

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. 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

Apply/Save Restart

Tick the Enable auto-detect to display the following:

COMTREND Multi-DSL CPE

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. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.

Enable auto-detect

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

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

PPP Username:

PPP Password:

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

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

Select Service:

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

Apply/Save Restart

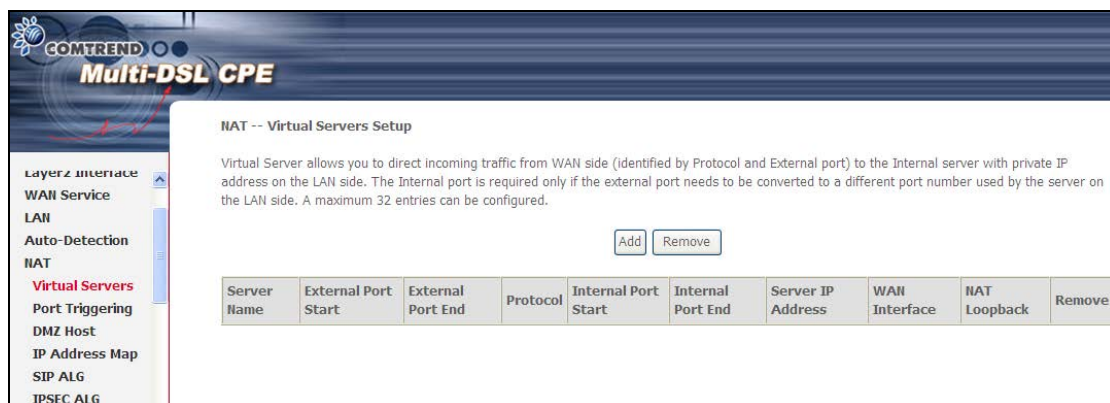
Follow the onscreen instructions to configure the interfaces that are available within your network, specify the wan parameters to be used and click the Apply/Save button to activate the auto-detection function.

5.4 NAT

To display this option, NAT must be enabled in at least one PVC shown on the [Advanced Setup - WAN](#) screen. *NAT is not an available option in Bridge mode.*

5.4.1 Virtual Servers

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



NAT -- Virtual Servers Setup

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

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

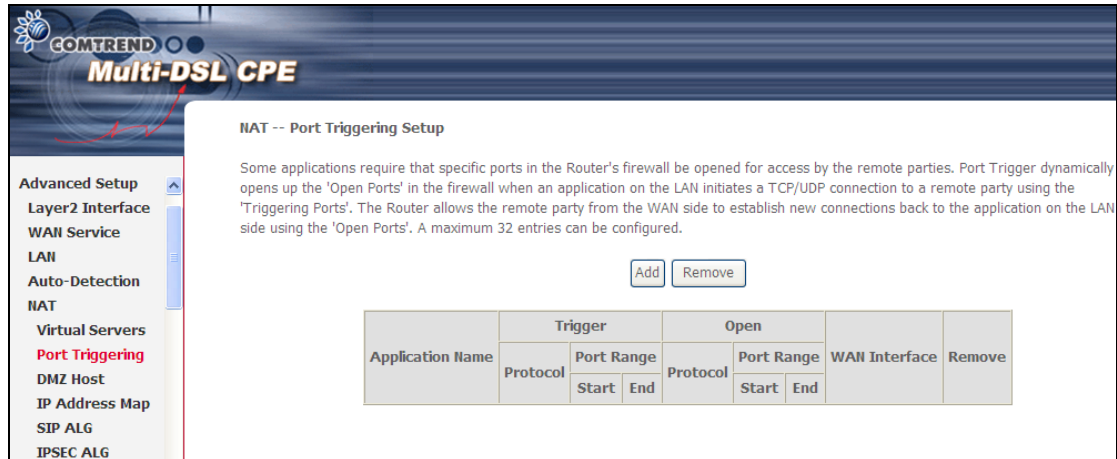
To add a Virtual Server, click **Add**. The following will be displayed.

Consult the table below for field and header descriptions.

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

5.4.2 Port Triggering

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



NAT -- Port Triggering Setup

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

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

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

NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

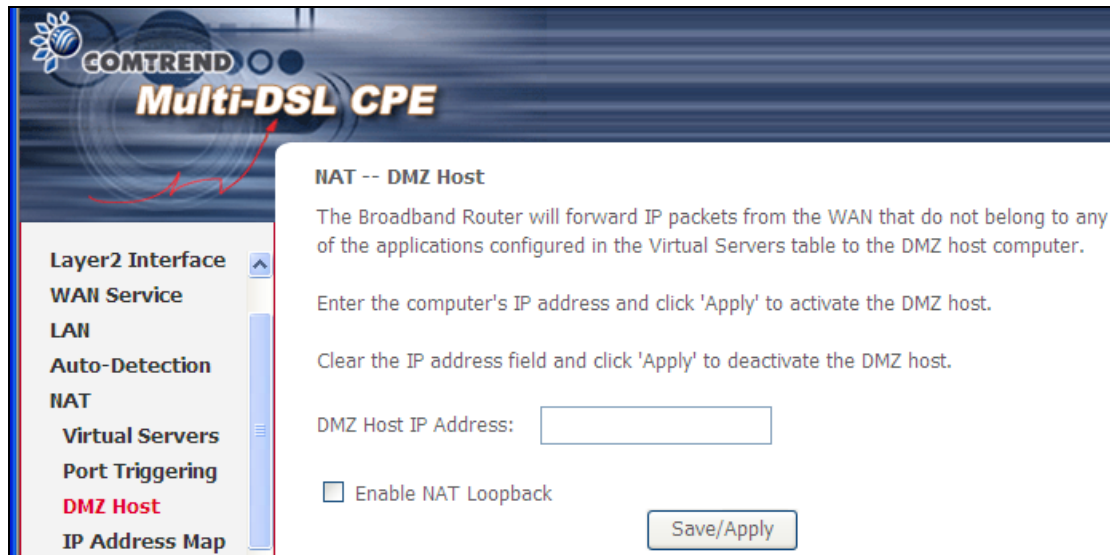
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Consult the table below for field and header descriptions.

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

5.4.3 DMZ Host

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

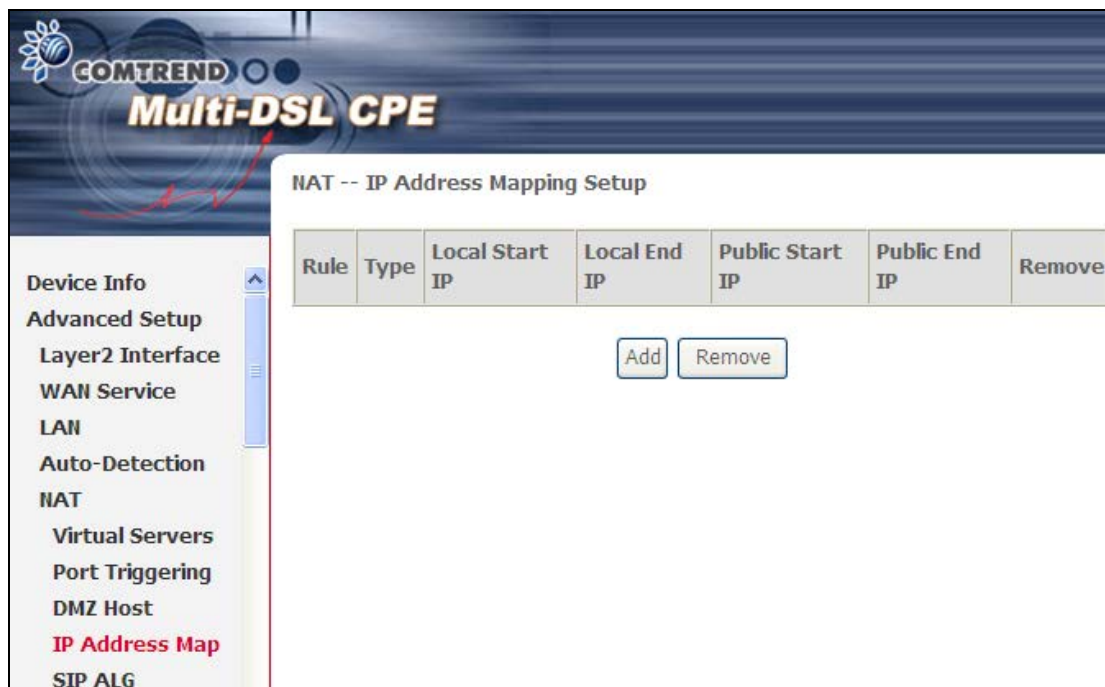


To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

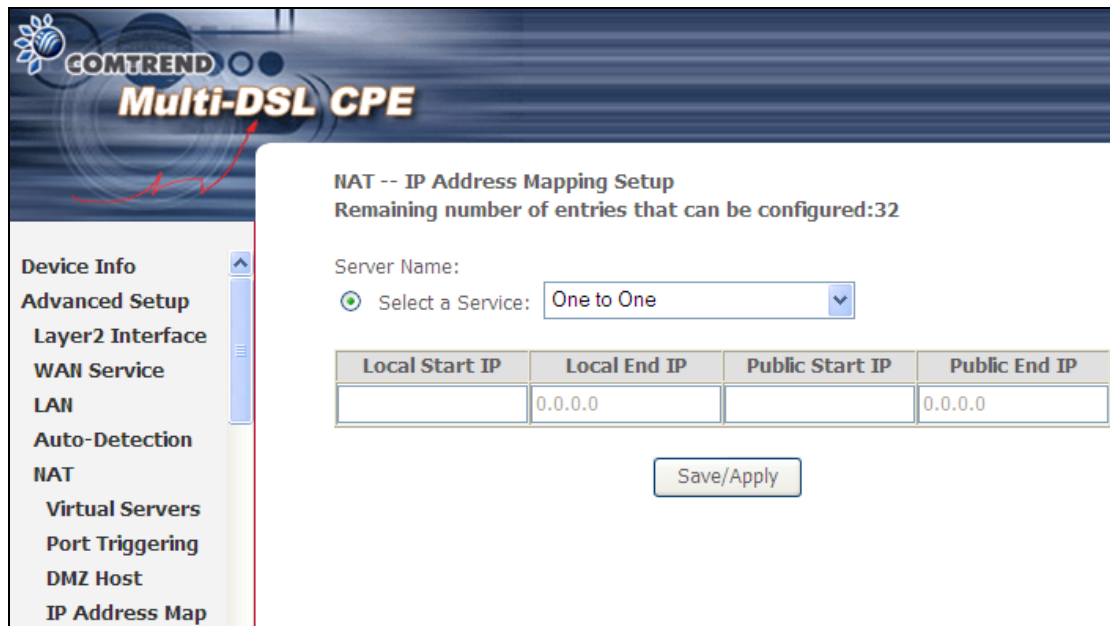
To **Deactivate** the DMZ host, clear the IP address field and click **Save/Apply**.

5.4.4 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



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

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

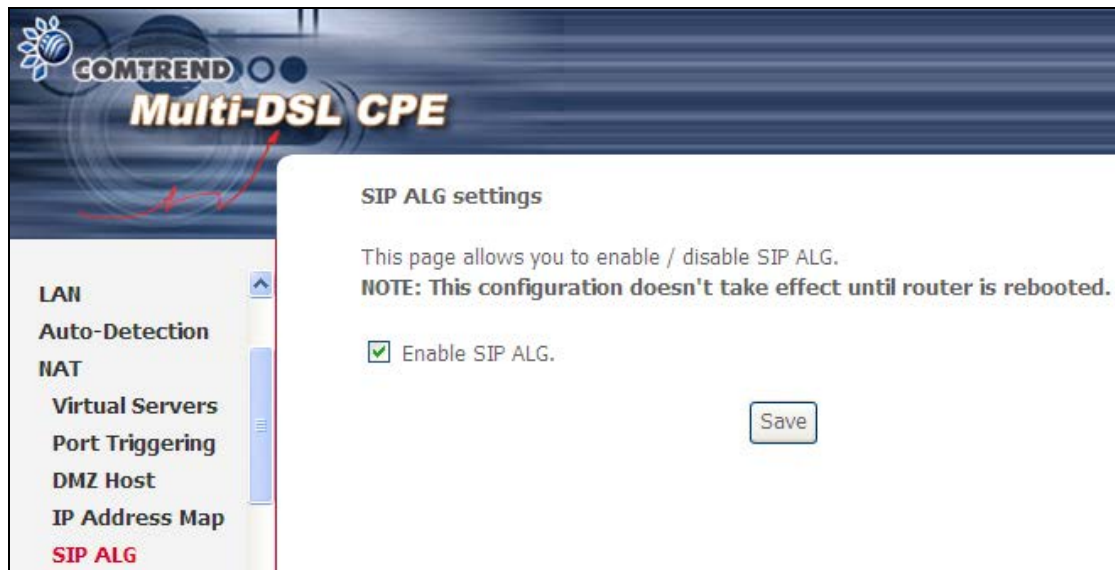
Many to one: mapping a range of local IP to a specific public IP

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

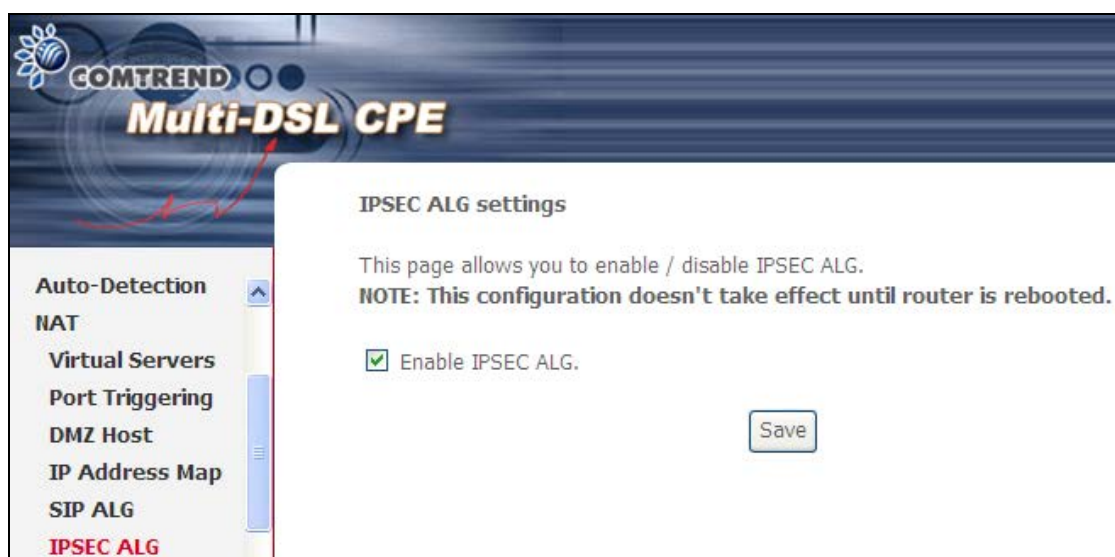
5.4.5 SIP ALG

This page allows you to enable / disable SIP ALG.



5.4.6 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.



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

5.5 Security

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

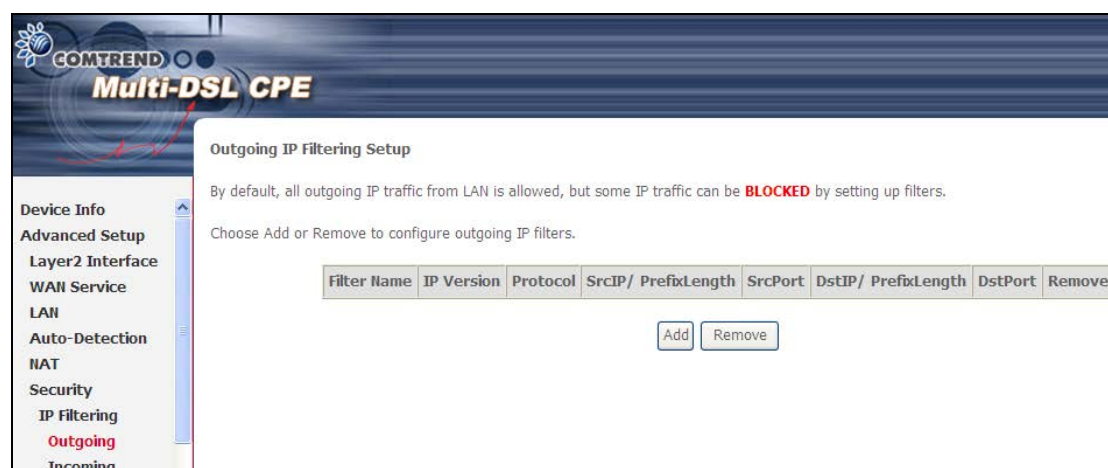
5.5.1 IP Filtering

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

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

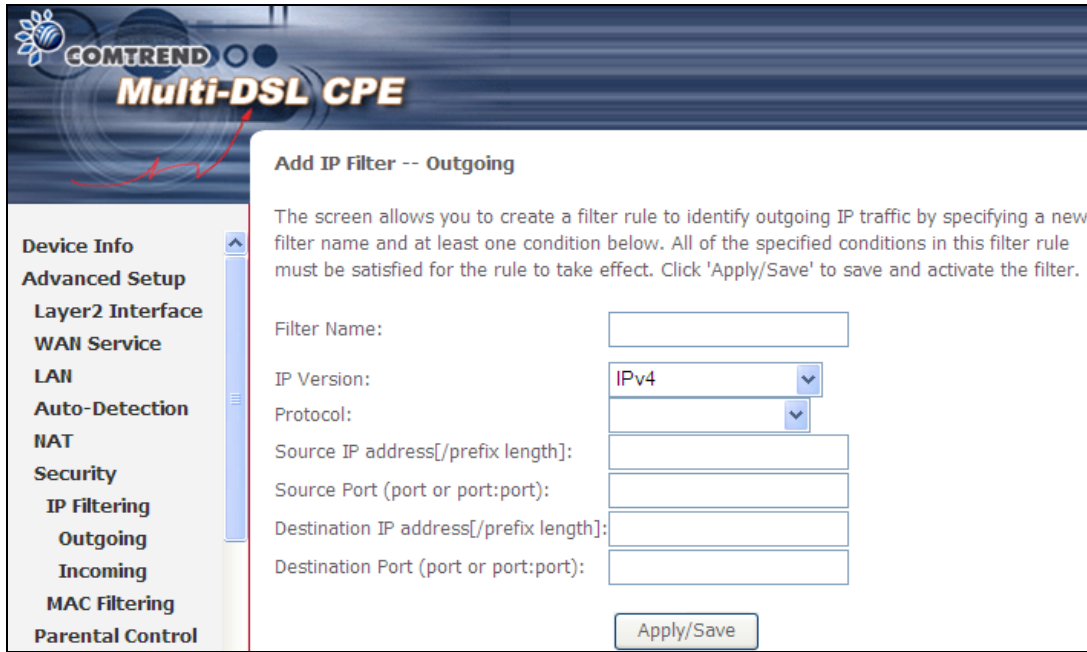
OUTGOING IP FILTER

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



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

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

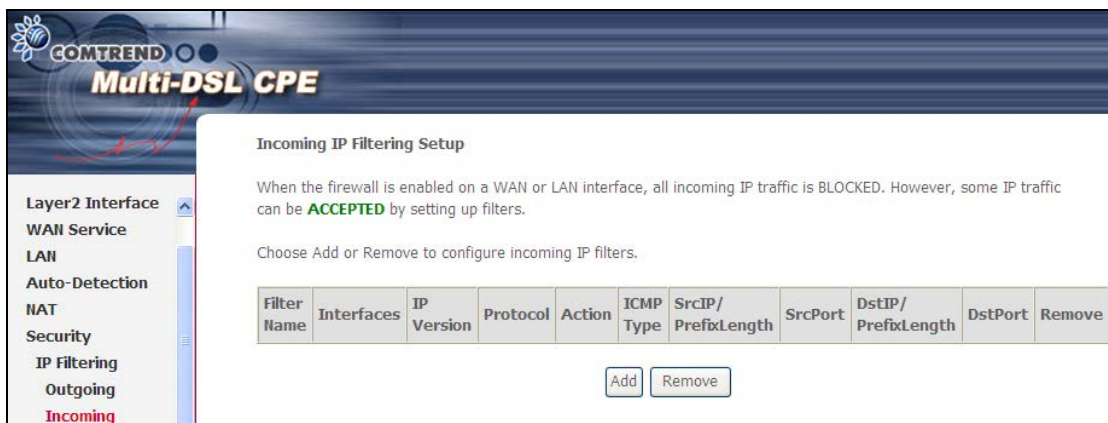


Consult the table below for field descriptions.

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.
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.

5.5.2 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-3031u 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 Multi-DSL CPE

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
eth1.1	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

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

Consult the table below for detailed field descriptions.

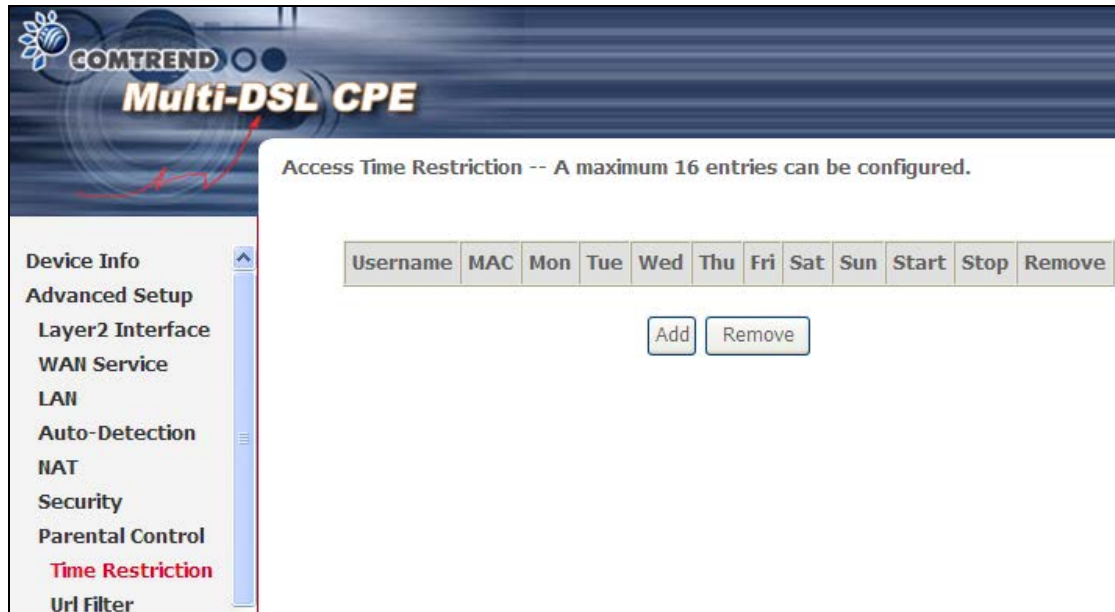
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

5.6 Parental Control

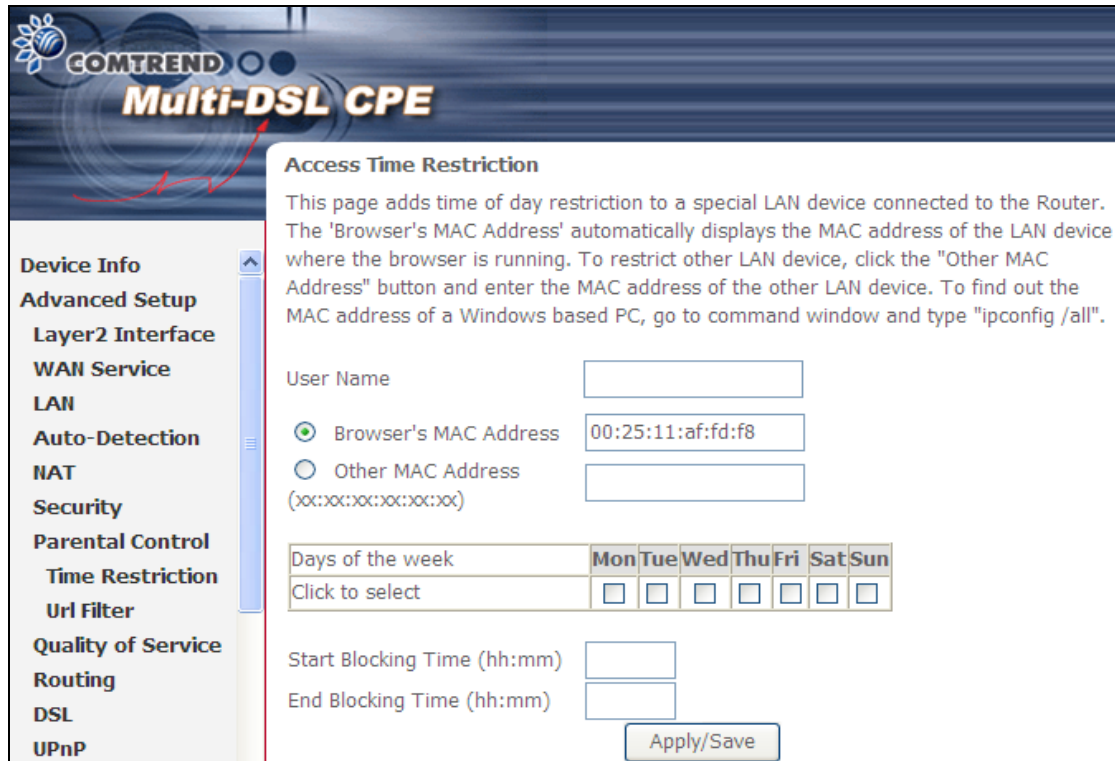
This selection provides WAN access control functionality.

5.6.1 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 8.4](#), 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.

5.6.2 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.

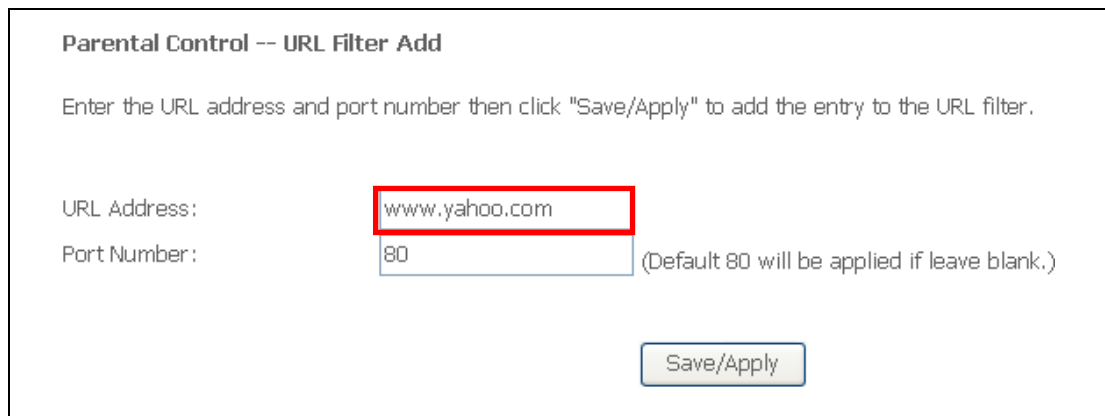


The screenshot shows the 'URL Filter' configuration page in the COMTREND Multi-DSL CPE web interface. The page title is 'URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.' Below the title, there are two radio buttons for 'URL List Type': 'Exclude' and 'Include'. Below these are two rows of buttons: the first row has 'Address', 'Port', and 'Remove' buttons; the second row has 'Add' and 'Remove' buttons. On the left side, there is a navigation menu with the following items: 'Device Info', 'Advanced Setup', 'Layer2 Interface', 'WAN Service', 'LAN', 'Auto-Detection', 'NAT', 'Security', 'Parental Control', 'Time Restriction', and 'Url Filter' (which is highlighted in red).

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.

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



The screenshot shows the 'Parental Control -- URL Filter Add' screen. It contains the following text: 'Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.' Below this, there are two input fields: 'URL Address:' with the value 'www.yahoo.com' (highlighted with a red box) and 'Port Number:' with the value '80'. A note next to the port number field says '(Default 80 will be applied if leave blank.)'. At the bottom right, there is a 'Save/Apply' button.

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

URL Filter -- A maximum 100 entries can be configured.

URL List Type: Exclude Include

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

Add

Remove

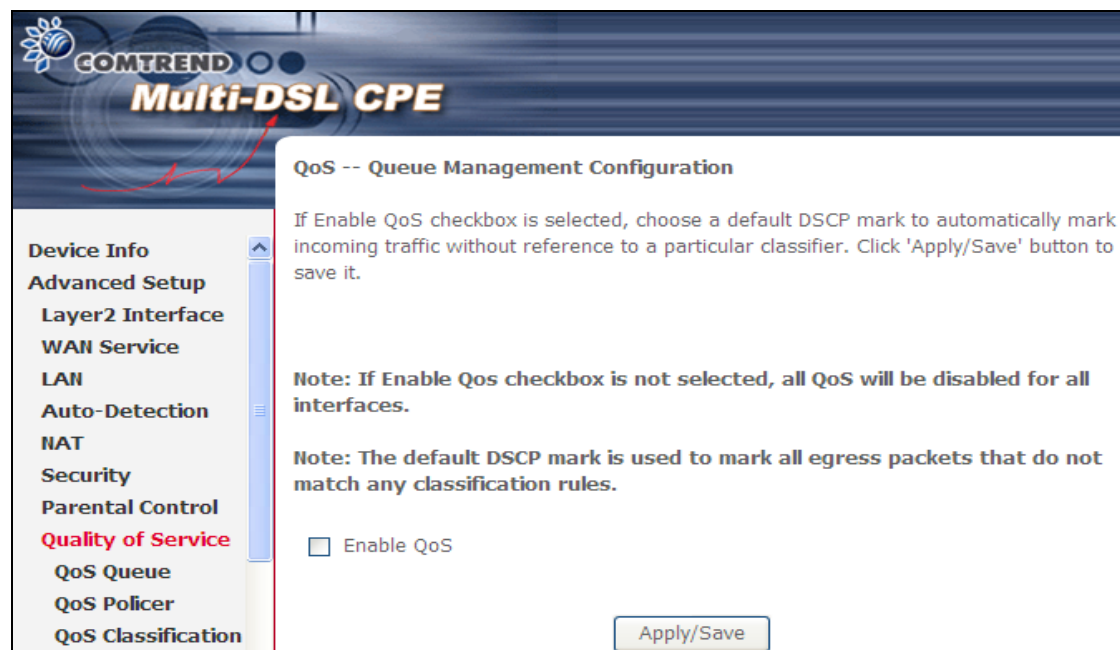
A maximum of 100 entries can be added to the URL Filter list.

5.7 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(see [Appendix G](#) 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.

5.7.1 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.
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

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
Default Queue	1	atm0	1	8/WRR/1	Path0				<input type="checkbox"/>	
Default Queue	2	ptm0	1	8/WRR/1	Path0	Low			<input type="checkbox"/>	
WMM Voice Priority	3	wl0	1	1/SP					Enabled	
WMM Voice Priority	4	wl0	2	2/SP					Enabled	
WMM Video Priority	5	wl0	3	3/SP					Enabled	
WMM Video Priority	6	wl0	4	4/SP					Enabled	
WMM Best Effort	7	wl0	5	5/SP					Enabled	
WMM Background	8	wl0	6	6/SP					Enabled	
WMM Background	9	wl0	7	7/SP					Enabled	
WMM Best Effort	10	wl0	8	8/SP					Enabled	

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 **Add** to display the following screen.

QoS Queue Configuration

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

Name:

Enable:

Interface:

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

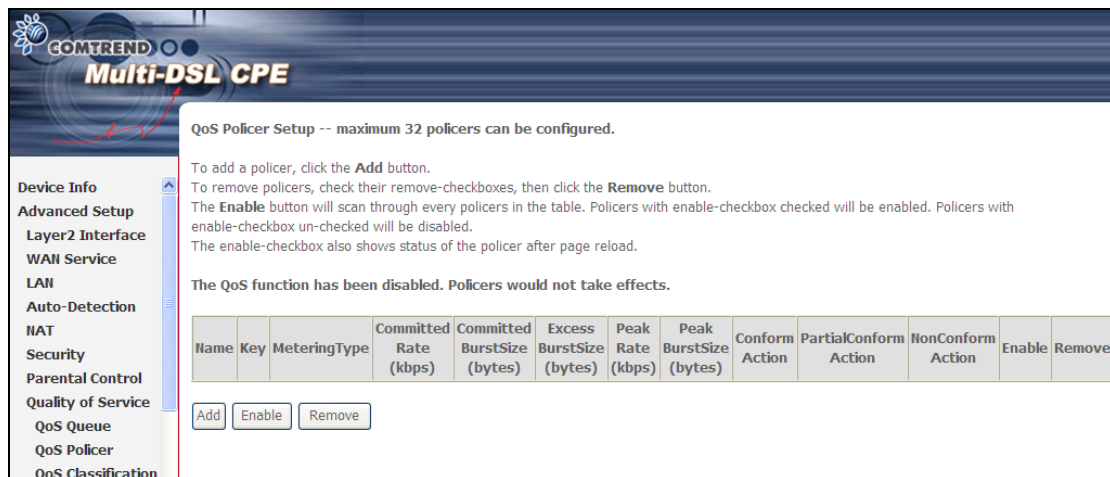
Interface: Assign the entry to a specific network interface (QoS enabled).

5.7.2 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.



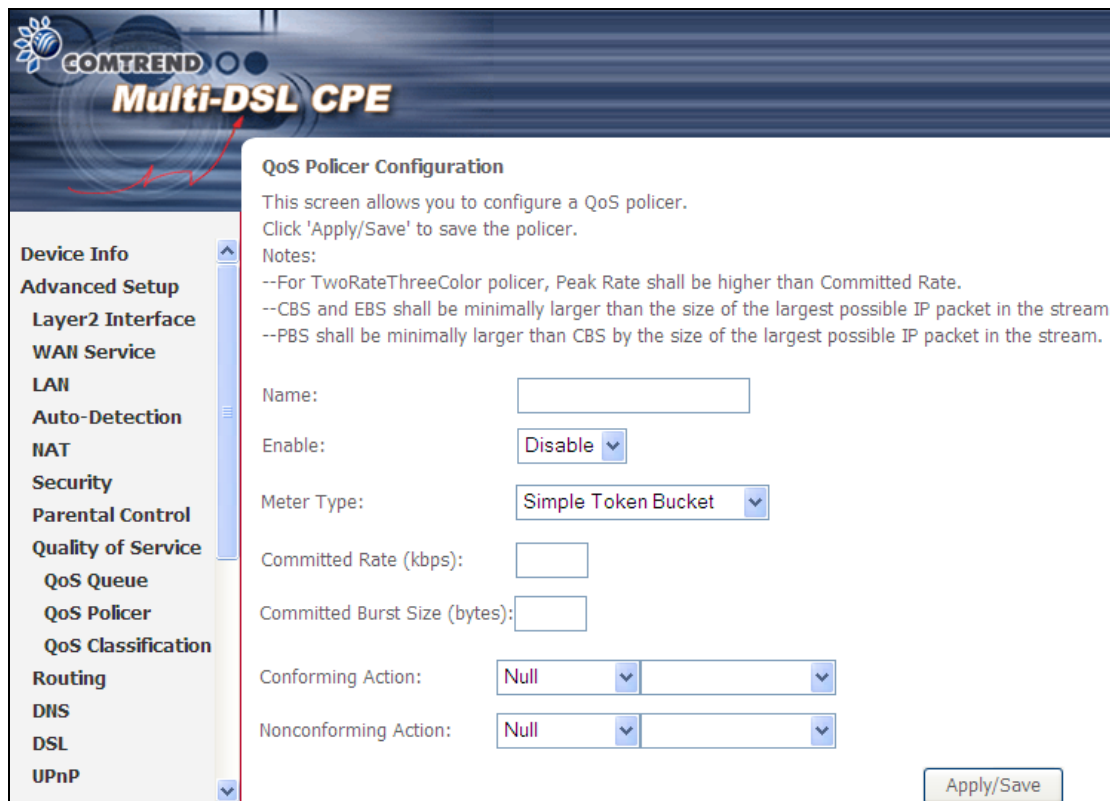
QoS Policer Setup -- maximum 32 policers can be configured.

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):

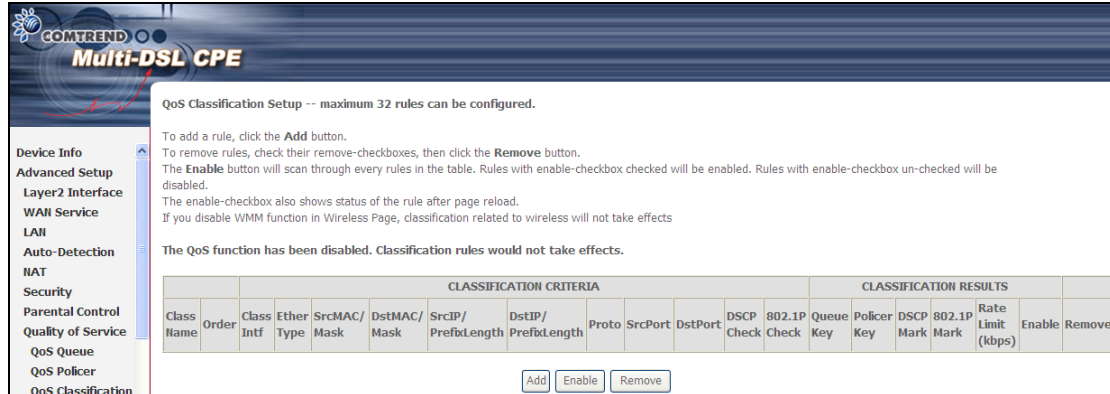
Conforming Action:

Nonconforming Action:

Field	Description
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

5.7.3 QoS Classification

The network traffic classes are listed in the following table.



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

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

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]

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, w10)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
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. Lower values have higher priority.
Set Rate Limit	The data transmission rate limit in kbps.

5.8 Routing

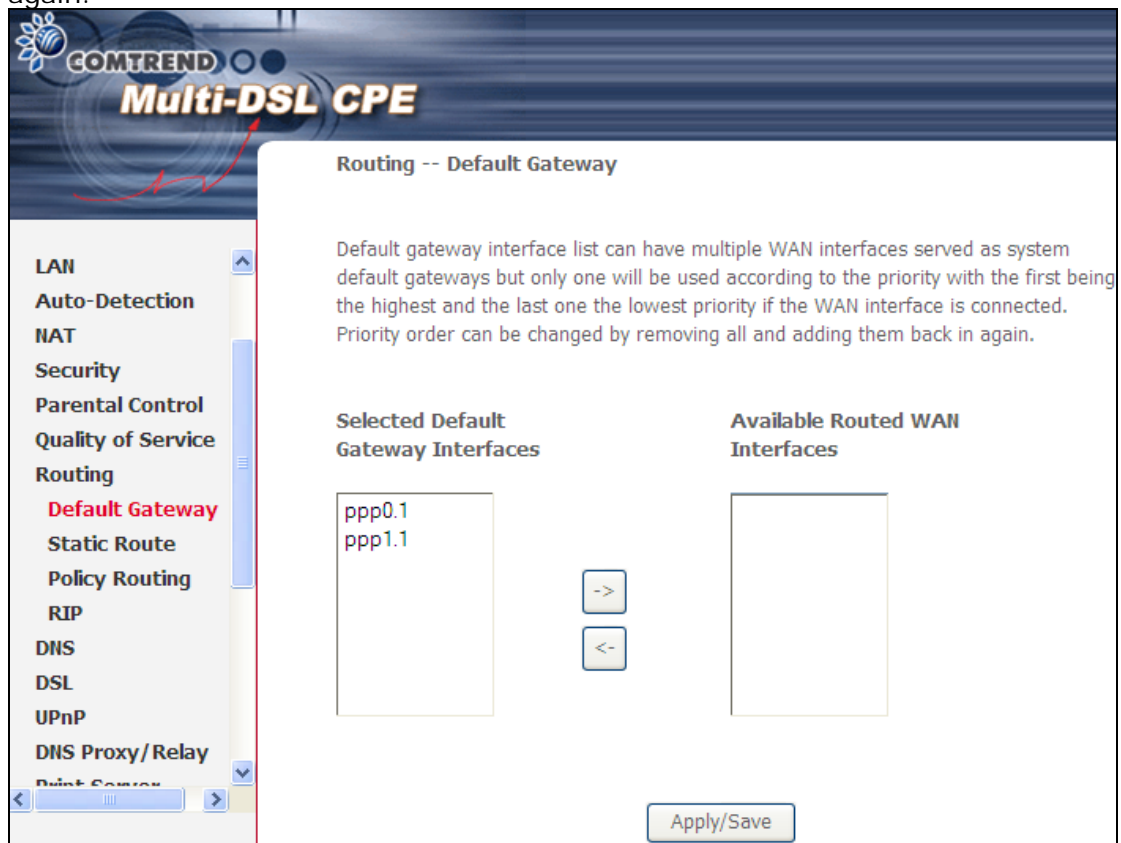
The following routing functions are accessed from this menu:

Default Gateway, Static Route, Policy Routing, RIP and IPv6 Static Route.

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

5.8.1 Default Gateway

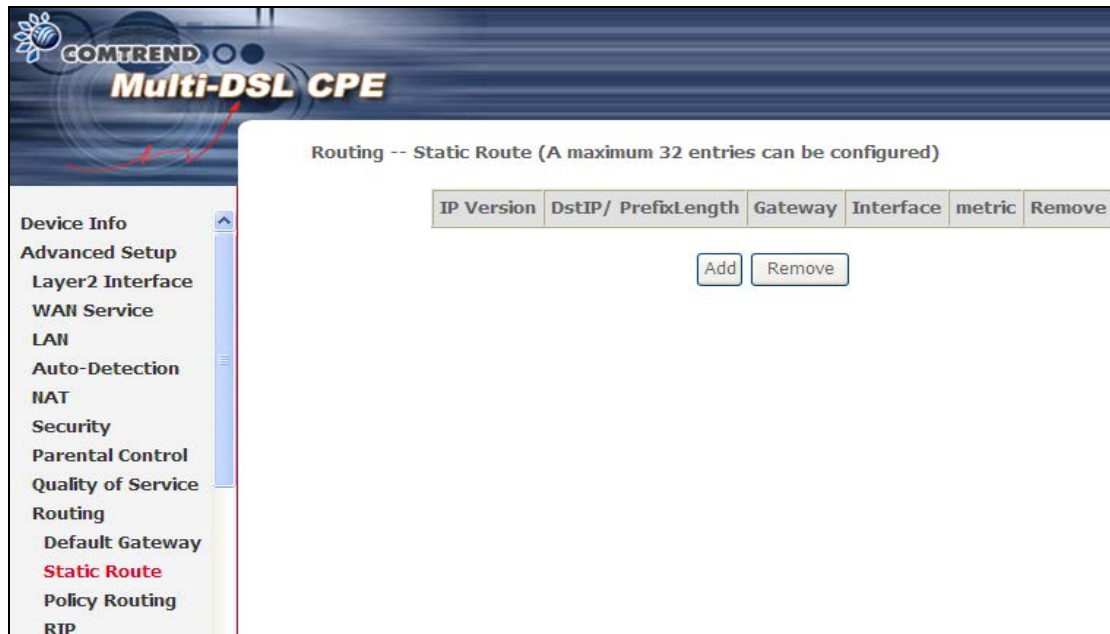
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all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



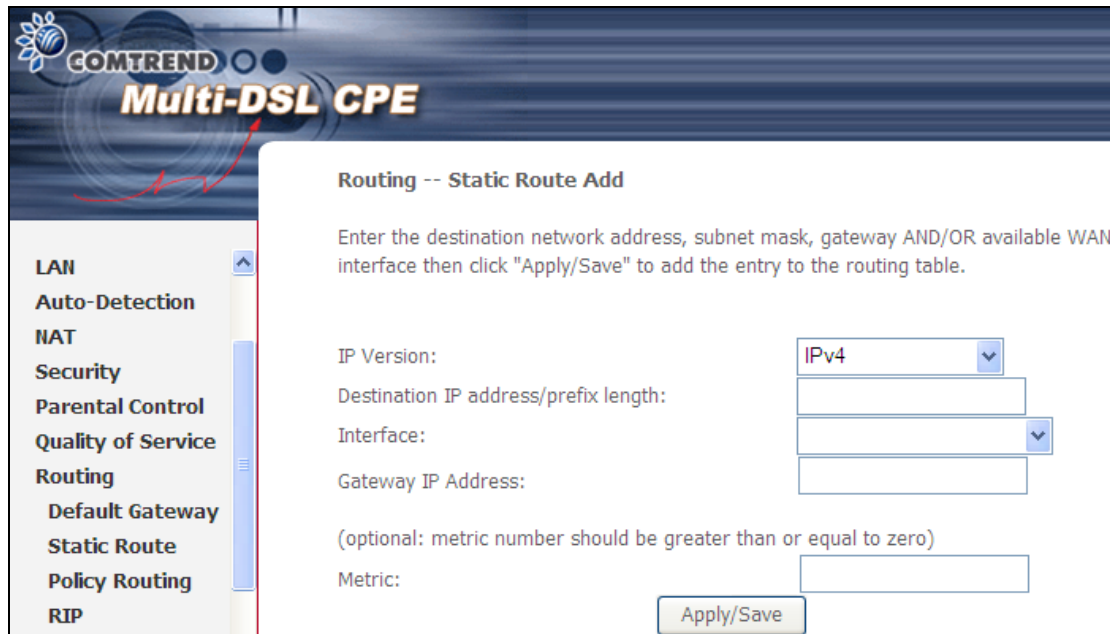
The screenshot displays the web management interface for a COMTREND Multi-DSL CPE. The left sidebar contains a navigation menu with the following items: LAN, Auto-Detection, NAT, Security, Parental Control, Quality of Service, Routing, **Default Gateway** (highlighted in red), Static Route, Policy Routing, RIP, DNS, DSL, UPnP, DNS Proxy/Relay, and Print Server. The main content area is titled "Routing -- Default Gateway" and includes the following text: "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." Below this text are two columns: "Selected Default Gateway Interfaces" containing a list box with "ppp0.1" and "ppp1.1", and "Available Routed WAN Interfaces" which is currently empty. Between these columns are two buttons: "->" and "<-" for moving interfaces. An "Apply/Save" button is located at the bottom right of the configuration area.

5.8.2 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 screen 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 save and apply the settings.

5.8.3 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 Multi-DSL CPE

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
-------------	-----------	----------	-----	------------	--------

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP

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

COMTREND Multi-DSL CPE

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:

LAN
Auto-Detection
NAT
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
DSL
UPnP
DNS Proxy/Relay

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

5.8.4 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 Multi-DSL CPE

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.

Interface	Version	Operation	Enabled
eth1.1	2	Passive	<input type="checkbox"/>

Apply/Save

5.9 DNS

5.9.1 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 inputted.

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, ppp1.1

Available WAN Interfaces:

Use the following Static DNS IP address:

Primary DNS server:

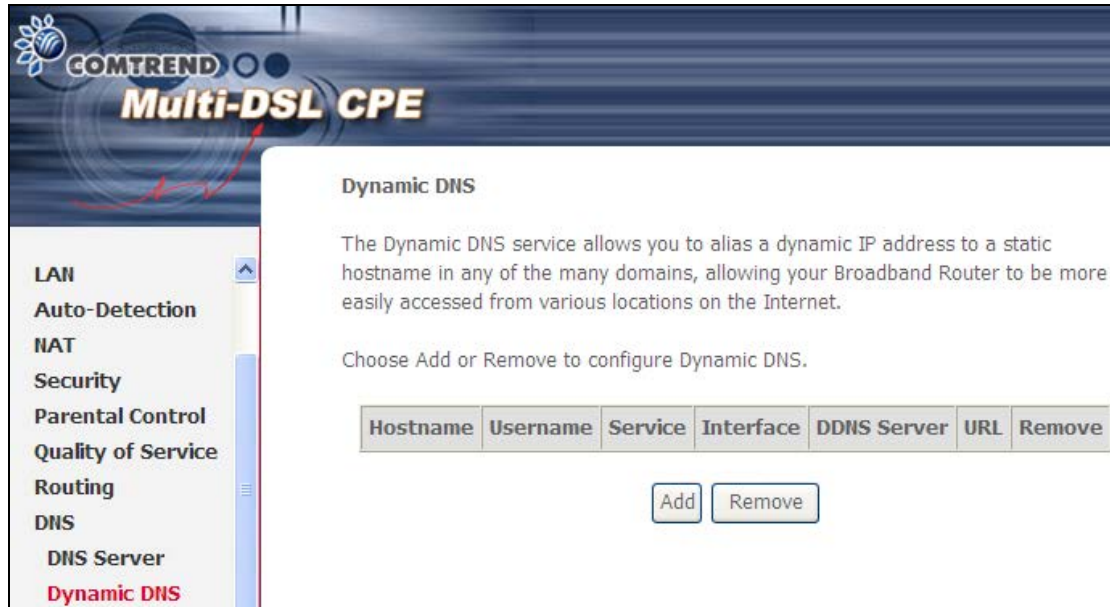
Secondary DNS server:

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

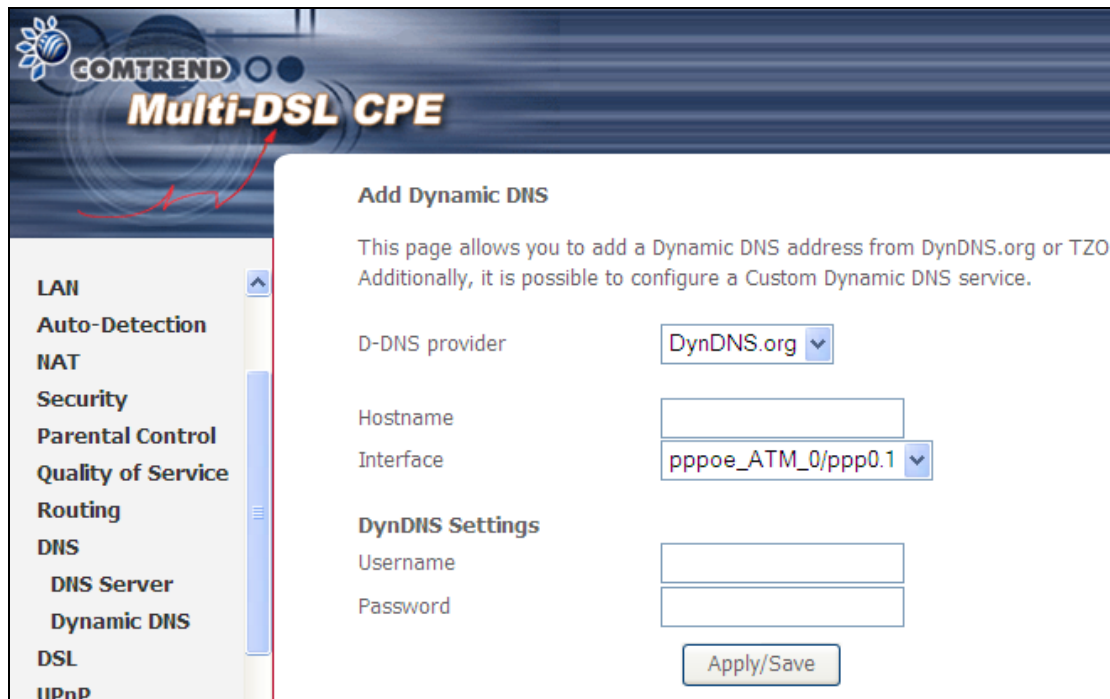
NOTE: You must reboot the router to make the new configuration effective.

5.9.2 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-3031u to be more easily accessed from various locations on the Internet.



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



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.

Consult the table below for field descriptions.

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

5.10 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 Multi-DSL CPE

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

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

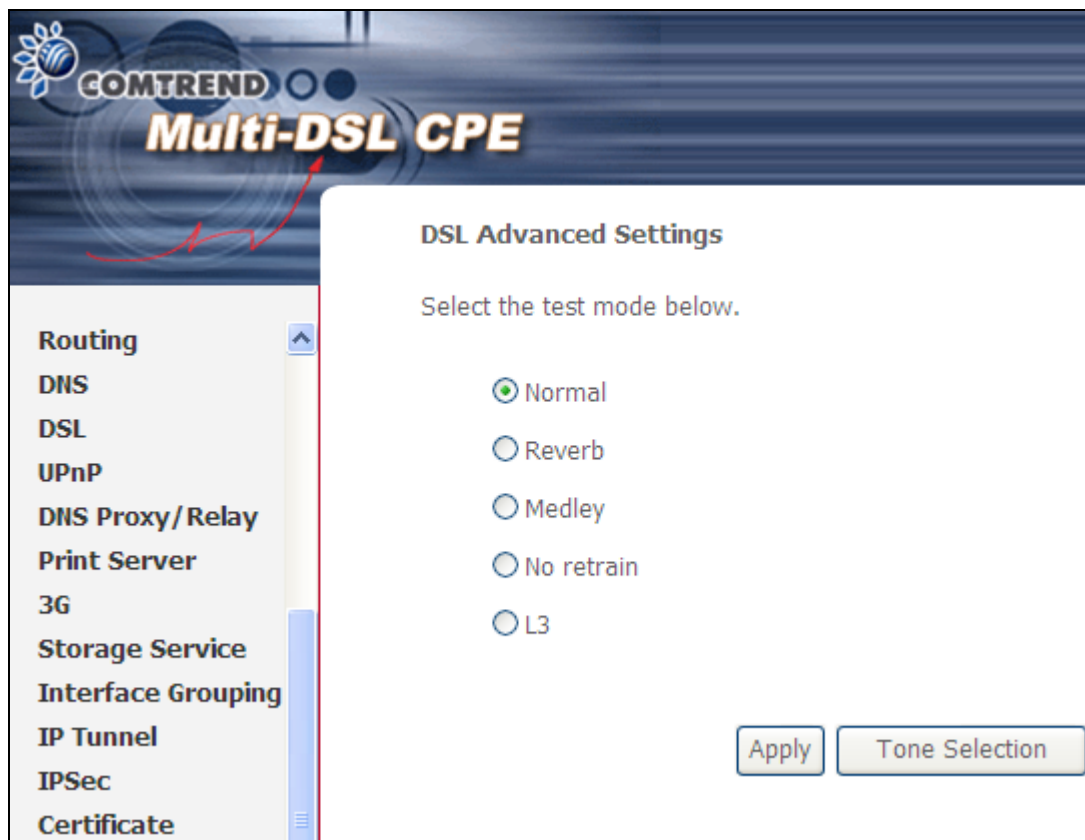
- Bitswap Enable
- SRA Enable

Apply/Save Advanced Settings

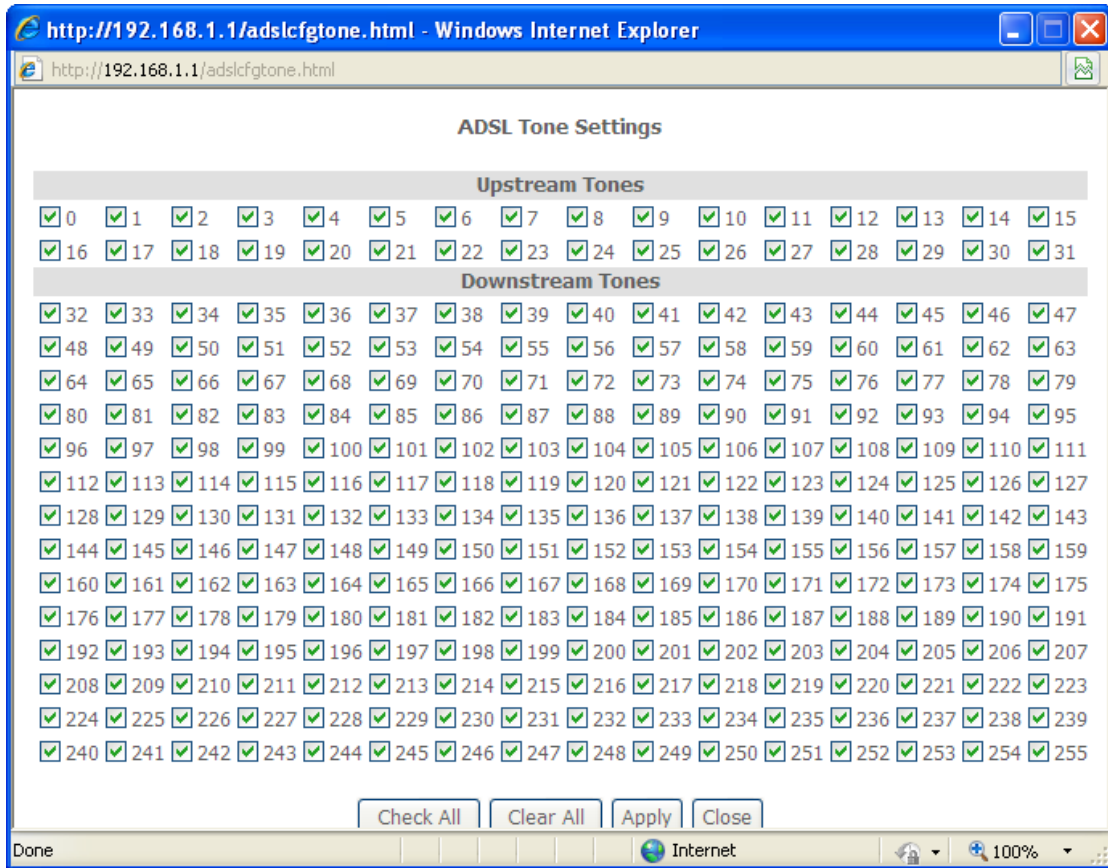
DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates	
ADSL2+	Downstream: 24 Mbps	Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps	Upstream: 3.5 Mbps
VDSL2	Downstream: 100 Mbps	Upstream: 60 Mbps
Options	Description	
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)	
Bitswap Enable	Enables adaptive handshaking functionality	
SRA Enable	Enables Seamless Rate Adaptation (SRA)	
G.997.1 EOC xTU-R Serial Number	This is an ID used to identify devices, and it can be found in embedded operations channel (EOC).	
Profile Selection	8a-d, 12a-b, 17a, US0	

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options. On the following screen you can select a test mode or modify tones by clicking **Tone Selection**. Click **Apply** to implement these settings and return to the previous screen.

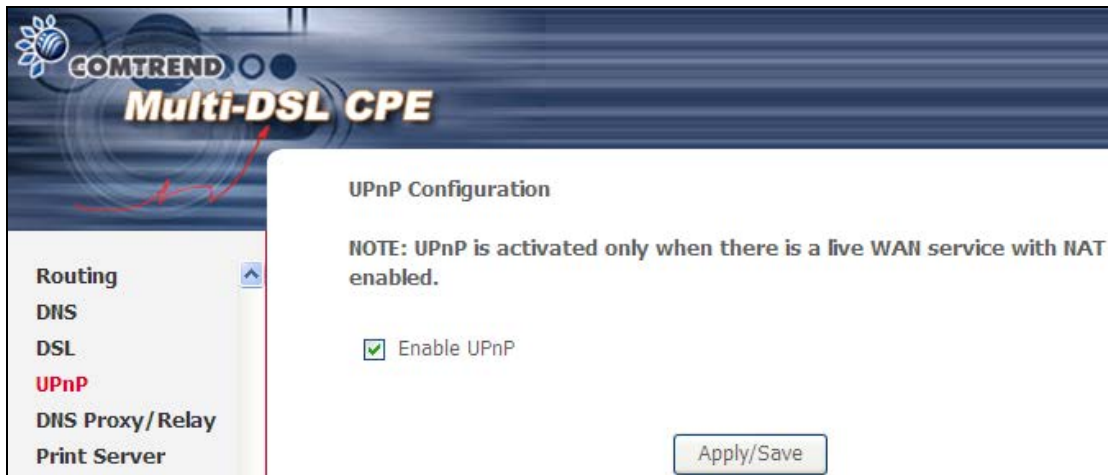


On this screen you select the tones you want activated, then click **Apply** and **Close**.



5.11 UPnP

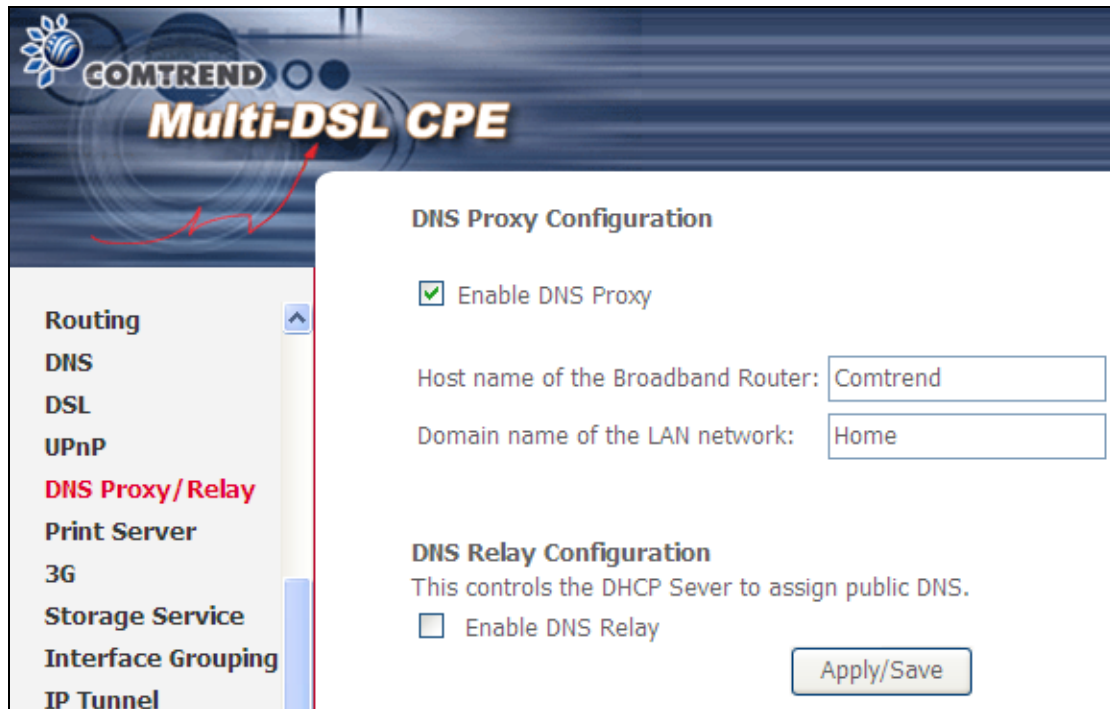
Select the checkbox provided and click **Apply/Save** to enable UPnP protocol.



5.12 DNS Proxy/Relay

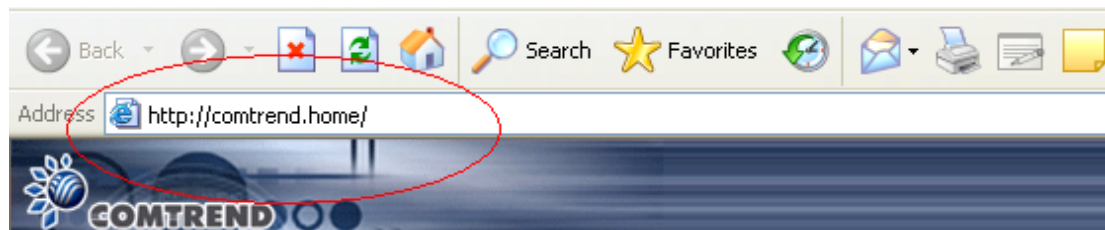
To enable DNS Proxy, select the corresponding checkbox and then enter Host and Domain names, as the example shown below. Click **Apply/Save** to continue.

Enabling the DNS Relay function allows the cpe to relay public DNS servers received from WAN interface to DHCP clients. To enable DNS Relay Configuration, select the corresponding checkbox and Click **Apply/Save** to continue.



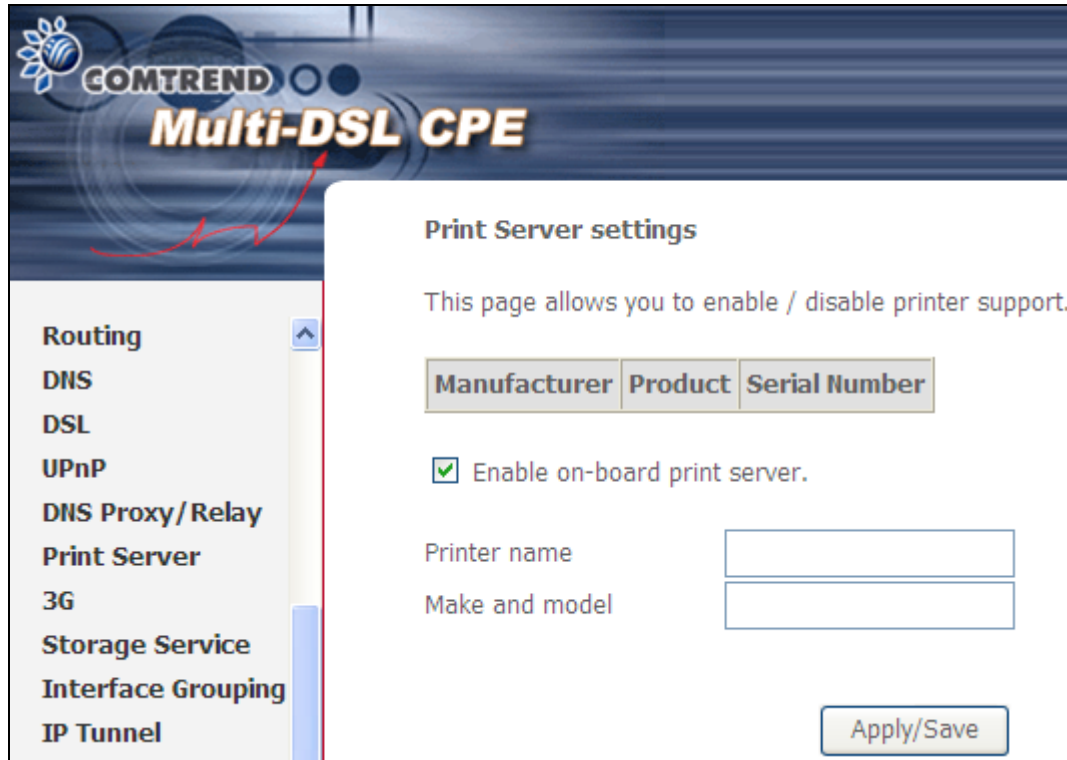
See below for further details.

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



5.13 Print Server

The VR-3031u can provide printer support through an optional USB2.0 host port. If your device has this port, refer to [Appendix F - Printer Server](#) for detailed setup instructions.

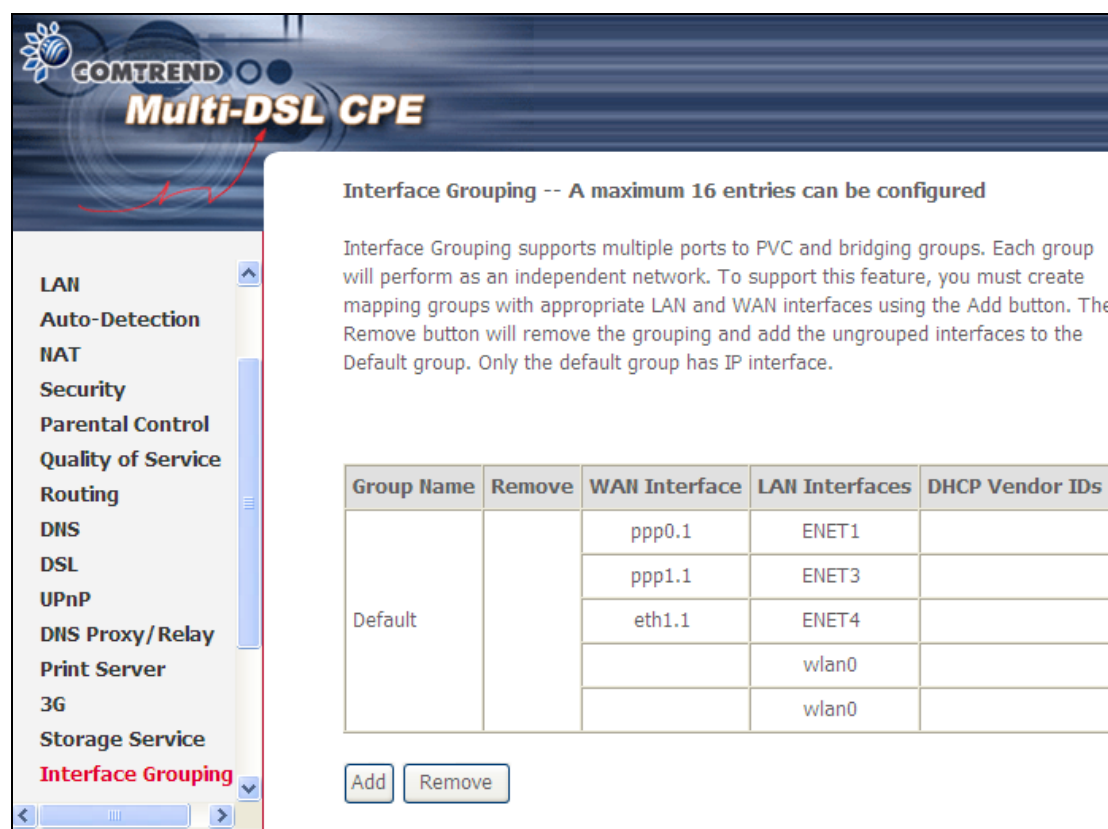


The screenshot displays the GOMTREND Multi-DSL CPE web interface. The top banner features the GOMTREND logo and the text "Multi-DSL CPE". A left-hand navigation menu lists various settings: Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Print Server (highlighted), 3G, Storage Service, Interface Grouping, and IP Tunnel. The main content area is titled "Print Server settings" and includes the following elements:

- A descriptive text: "This page allows you to enable / disable printer support."
- Three input fields for "Manufacturer", "Product", and "Serial Number".
- A checked checkbox labeled "Enable on-board print server."
- Two input fields: "Printer name" and "Make and model".
- An "Apply/Save" button at the bottom right.

5.14 Interface Grouping

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



Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	ENET1	
		ppp1.1	ENET3	
		eth1.1	ENET4	
			wlan0	
			wlan0	

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

COMTREND Multi-DSL CPE

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

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

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces	Available LAN Interfaces
<div style="border: 1px solid black; height: 100px;"></div>	<div style="border: 1px solid black; padding: 5px;"> ENET1 ENET3 ENET4 wlan0 wlan0 </div>

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients With Following DHCP Vendor IDs:

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

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

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

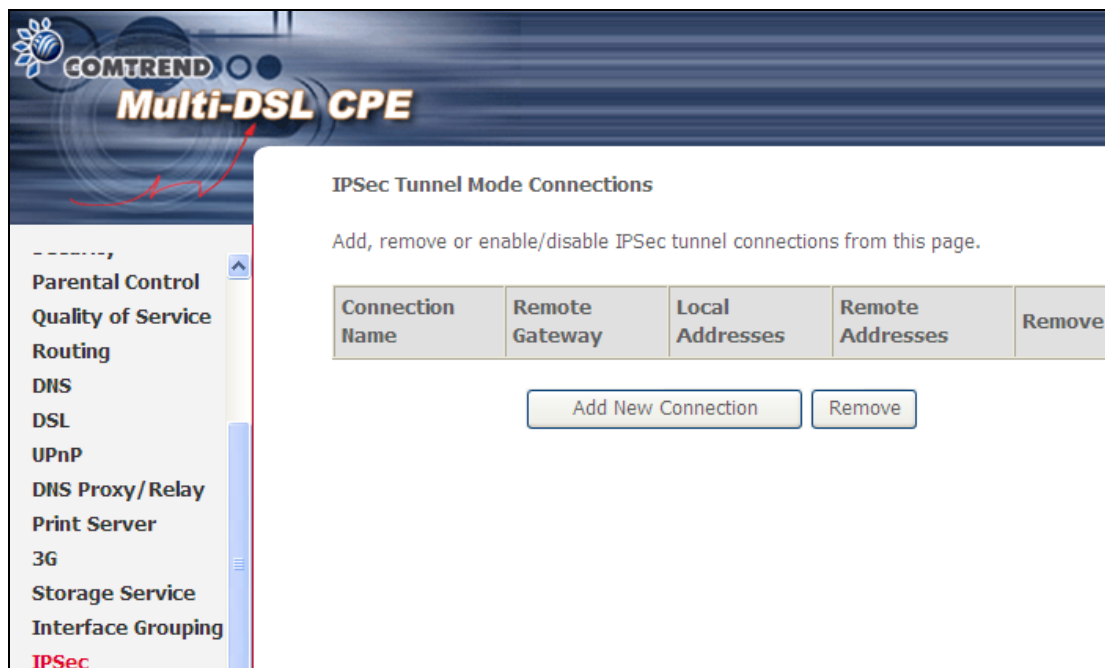
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

5.15 IPSec

5.15.1 IPSec Tunnel Mode Connections

You can add, edit or remove IPSec tunnel mode connections from this page.



The screenshot displays the Comtrend Multi-DSL CPE web interface. The header features the Comtrend logo and the text "Multi-DSL CPE". On the left, a navigation menu lists various settings: Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Print Server, 3G, Storage Service, Interface Grouping, and IPSec (highlighted in red). The main content area is titled "IPSec Tunnel Mode Connections" and includes the instruction: "Add, remove or enable/disable IPSec tunnel connections from this page." Below this is a table with the following columns: Connection Name, Remote Gateway, Local Addresses, Remote Addresses, and Remove. Underneath the table are two buttons: "Add New Connection" and "Remove".

Click **Add New Connection** to add a new IPSec termination rule.

The following screen will display.

COMTREND Multi-DSL CPE

IPSec Settings

IPSec Connection Name:

Tunnel Mode:

Remote IPSec Gateway Address (IPv4 address in dotted decimal):

Tunnel access from local IP addresses:

IP Address for VPN:

IP Subnetmask:

Tunnel access from remote IP addresses:

IP Address for VPN:

IP Subnetmask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Advanced IKE Settings:

IPSec Connection Name	User-defined label
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select Show Advanced Settings to reveal the advanced settings options shown below.
<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> Advanced IKE Settings Hide Advanced Settings </div> <div style="margin-top: 10px;"> <p>Phase 1</p> <p>Mode: Main</p> <p>Encryption Algorithm: 3DES</p> <p>Integrity Algorithm: MD5</p> <p>Select Diffie-Hellman Group for Key Exchange: 1024bit</p> <p>Key Life Time: 3600 Seconds</p> <hr/> <p>Phase 2</p> <p>Encryption Algorithm: 3DES</p> <p>Integrity Algorithm: MD5</p> <p>Select Diffie-Hellman Group for Key Exchange: 1024bit</p> <p>Key Life Time: 3600 Seconds</p> <div style="text-align: right; margin-top: 10px;">Apply/Save</div> </div> </div>	
Advanced IKE Settings	Select Hide Advanced Settings to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

The Manual key exchange method options are summarized in the table below.

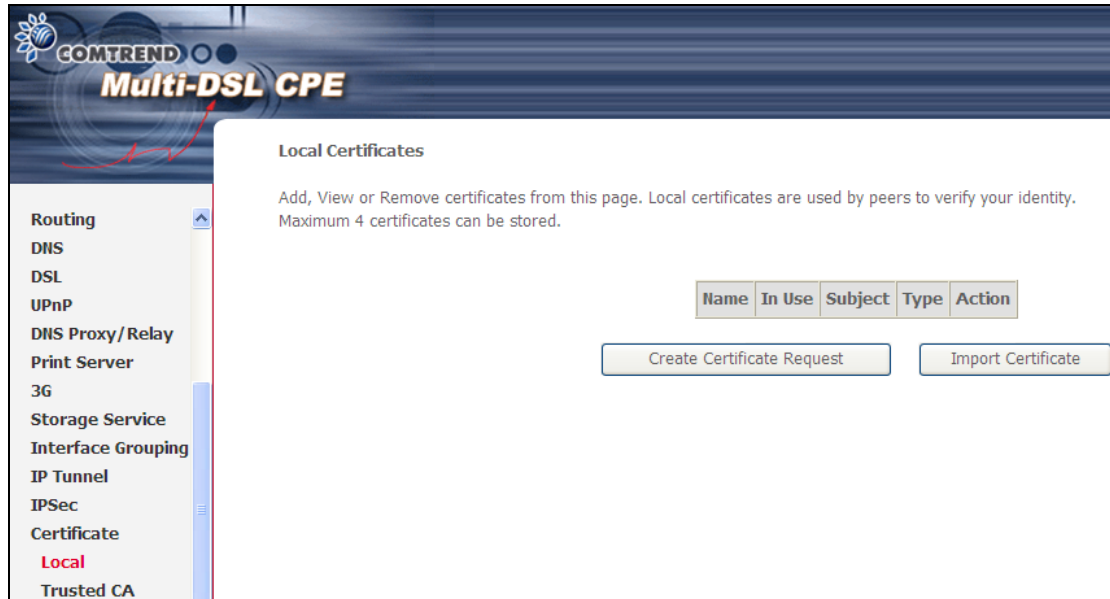
Manual Key Exchange Method	
Key Exchange Method	Manual
Encryption Algorithm	3DES
Encryption Key	<input type="text"/> DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5
Authentication Key	<input type="text"/> MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI	101 Hex 100-FFFFFFFF
Apply/Save	

Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

5.16 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.

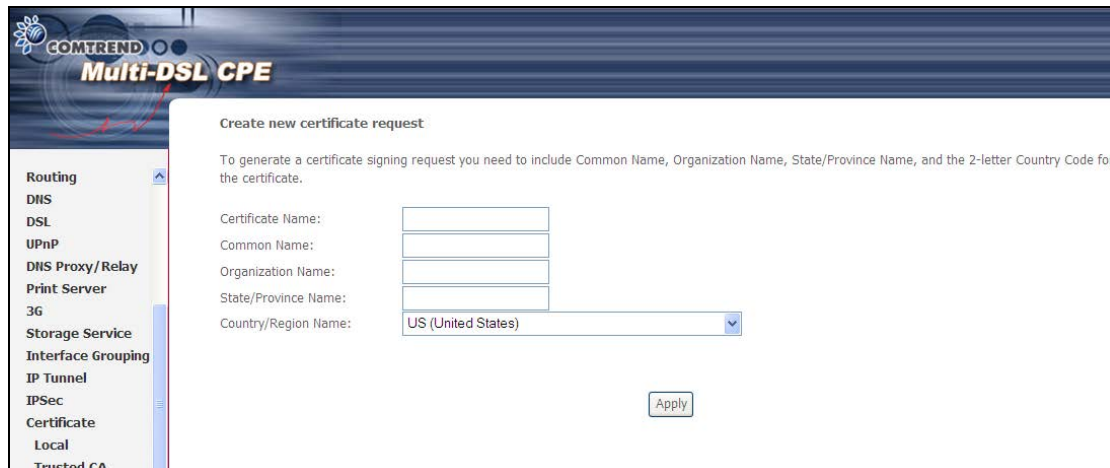
5.16.1 Local



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.

The screenshot shows the 'Import certificate' form in the COMTREND Multi-DSL CPE web interface. The form is titled 'Import certificate' and includes the instruction 'Enter certificate name, paste certificate content and private key.' The form has three main input areas:

- Certificate Name:** A text input field.
- Certificate:** A large text area containing the placeholder text:


```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```
- Private Key:** A large text area containing the placeholder text:

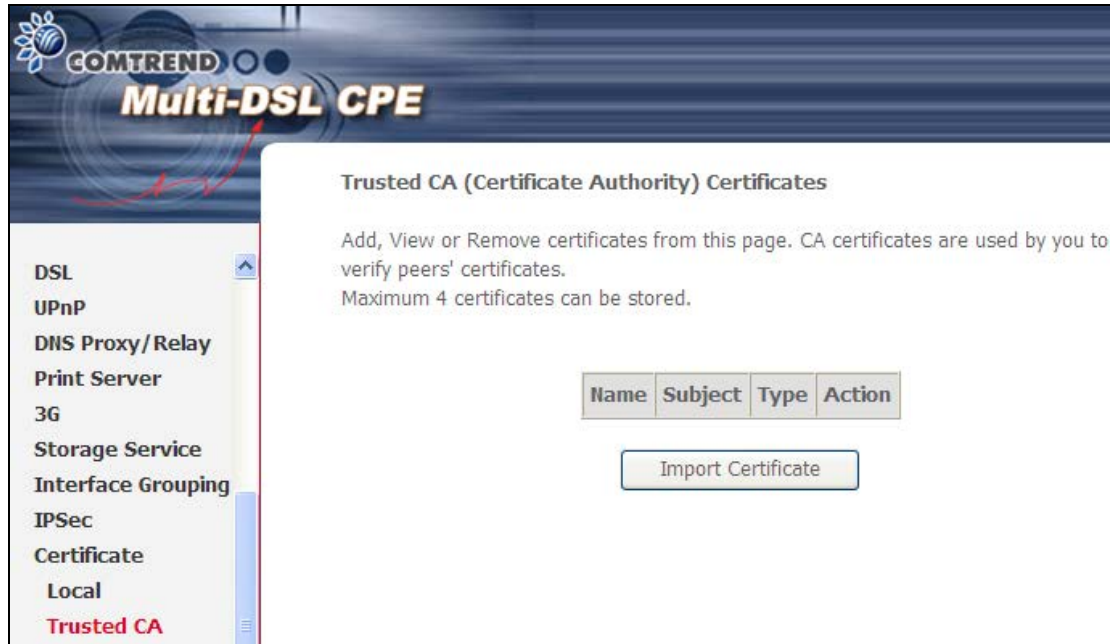

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

An 'Apply' button is located at the bottom right of the form. On the left side of the interface, a navigation menu is visible with the following items: Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Print Server, 3G, Storage Service, Interface Grouping, IPsec, Certificate (selected), Local, Trusted CA, Power Management, Multicast, and Wireless.

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

5.16.2 Trusted CA

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



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



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

5.17 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 'Power Management' configuration page in the COMTREND Multi-DSL CPE web interface. The page title is 'Power Management' and it includes a descriptive paragraph: '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.'

The left sidebar contains a navigation menu with the following items: Routing, DNS, DSL, UPnP, DNS Proxy/Relay, Print Server, 3G, Storage Service, Interface Grouping, IPSec, Certificate, **Power Management** (highlighted in red), Multicast, Wireless, Diagnostics, and Management.

The main content area lists several power management settings, each with an 'Enable' checkbox and a 'Status' field:

- MIPS CPU Clock divider when Idle**: Enable, Status: **Enabled**
- Wait instruction when Idle**: Enable, Status: **Enabled**
- DRAM Self Refresh**: Enable, Status: **Enabled**
- Energy Efficient Ethernet**: Enable, Status: **Disabled**
- Ethernet Auto Power Down and Sleep**: Enable, Status: **Enabled**. To the right, it shows 'Number of ethernet interfaces: Powered up: 1, Powered down: 3'.
- Adaptive Voltage Scaling**: Enable, Status: **Enabled**

At the bottom right of the page, there are two buttons: 'Apply' and 'refresh'.

5.18 Multicast

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

COMTREND Multi-DSL CPE

IGMP Configuration

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

Default Version:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input type="checkbox"/>
Membership Join Immediate (IPTV):	<input type="checkbox"/>

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.
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.

Field	Description
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 6 Wireless

The Wireless menu provides access to the wireless options discussed below.

6.1 Basic

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

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

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox <input checked="" type="checkbox"/> that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.

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

6.2 Security

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

Wireless -- Security

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

WPS Setup

Enable WPS

Manual Setup AP

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

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

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

WIRELESS SECURITY

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

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

Network Authentication

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

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

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

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

Apply/Save

The settings for WPA authentication are shown below.

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled

Apply/Save

The settings for WPA2/WPA-PSK authentication are shown next.

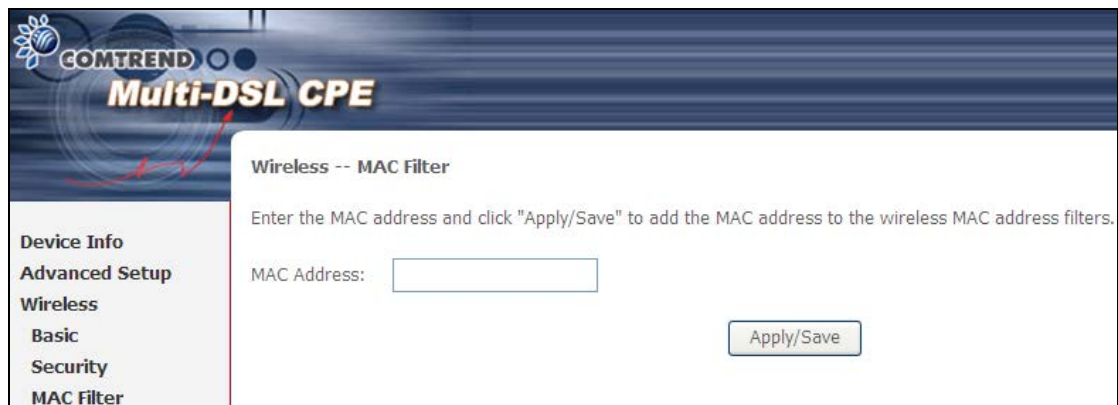
WPA/WAPI passphrase:
WPA-PSK uses a simple and consistent method to secure your network using a passphrase (also referred to as a shared secret) that needs to be inputted in both the wireless access point/router and the WPA clients. The shared secret can consist of between 8 and 63 characters and can include spaces. It should consist of a random sequence of letters (upper and lowercase and punctuation) at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. The more varied your WPA preshared key, the safer it is to utilize.
WPA Group Rekey Interval:
WPA-PSK is an encryption method where the encryption keys are automatically changed (called rekeying) and after a specified amount of time are authenticated between devices, or after a stated number of packets has been transmitted (which is referred to as the rekey interval . The Default is "0".
WPA/WAPI Encryption:
Select the encryption algorithm you want to use: AES or TKIP+AES.
WEP Encryption
This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.
Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.
When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.
Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.
Encryption Strength
This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.3 MAC Filter

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

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

After clicking the **Add** button, the following screen appears. Enter the MAC address in the box provided and click **Save/Apply**.



The screenshot shows the COMTREND Multi-DSL CPE web interface. The page title is "Wireless -- MAC Filter". Below the title, there is a text box with the instruction: "Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters." Below this instruction, there is a text label "MAC Address:" followed by an empty input field. To the right of the input field is a button labeled "Apply/Save". On the left side of the page, there is a navigation menu with the following items: "Device Info", "Advanced Setup", "Wireless", "Basic", "Security", and "MAC Filter". The "Wireless" item is currently selected.

6.4 Wireless Bridge

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

The screenshot shows the 'Wireless -- Bridge' configuration page. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, **Wireless Bridge**, Advanced, Site Survey, Station Info, Diagnostics, and Management. The main content area has a title 'Wireless -- Bridge' and a descriptive paragraph: 'This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.'

The configuration fields are:

- AP Mode: A dropdown menu currently set to 'Access Point'.
- Bridge Restrict: A dropdown menu currently set to 'Enabled'.
- Remote Bridges MAC Address: Two input fields for MAC addresses.

At the bottom right, there are two buttons: 'Refresh' and 'Apply/Save'.

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

Feature	Description
AP Mode	Selecting Wireless Bridge (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

6.5 Advanced

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

COMTREND Multi-DSL CPE

Wireless -- Advanced

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


Band:	2.4GHz	
Channel:	Auto	Current: 11 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz/40MHz Mixed Mode	Current: 20MHz
Control Sideband:	Lower	Current: N/A
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Auto	
OBSS Coexistence:	Enable	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.
RIFS Advertisement	Reduced Interframe Space is the creation of a short time delay between PDUs to improve wireless efficiency.
OBSS Co-Existence	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.

Field	Description
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

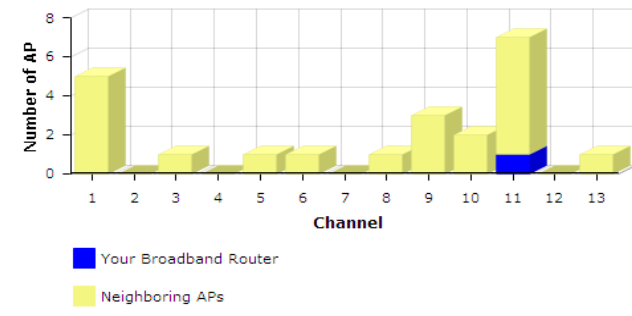
6.6 Site Survey

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



Wireless -- Channel Graph

The following graph displays wireless APs found in your neighborhood by channel. Your broadband router is transmitting on channel 11.



Channel	Number of AP
1	5
2	0
3	1
4	0
5	1
6	1
7	0
8	1
9	4
10	2
11	8
12	0
13	1

Wireless -- Site Survey

List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
	ComtrendFEEC88-1	3A:72:C0:FE:EC:89	9
	ComtrendFEEC88-3	42:72:C0:FE:EC:89	9
	Jason_WiMAX	20:10:7A:F1:F2:13	11
	wl0_Guest1	62:1D:20:FF:E1:54	11
	wl0_Guest2	62:1D:20:FF:E1:55	11
	wl0_Guest3	62:1D:20:FF:E1:56	11
	LBOX-shuli	00:1D:20:FF:E1:57	11
	nstech_B	FC:75:16:8C:F5:EC	10
	CTMIS-INT	80:1F:02:57:22:9C	13
	Comtrend2238	F8:8E:85:11:22:39	1
	Ext_845	00:1D:20:FF:E7:6F	1
	WAP5860uOutdoorAP	00:1A:2B:99:BC:2E	1
	claridy-E	00:0E:A6:7F:09:10	1
	CTMIS-INT	80:1F:02:57:22:34	1
	EnterpriseAP	00:30:DA:36:33:51	3
	WLAN_6000	00:90:4C:02:60:00	6
	CTMIS-INT	80:1F:02:57:22:54	5
	ACSTest	00:1A:2B:83:D6:0C	8
	ComtrendFEEC88-2	3E:72:C0:FE:EC:89	9
	Comtrend1201	00:1D:20:31:12:02	11
	DIRECT-c1-Android_f6b4	8A:30:8A:66:CA:68	10

Device Info

Advanced Setup

Wireless

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Site Survey

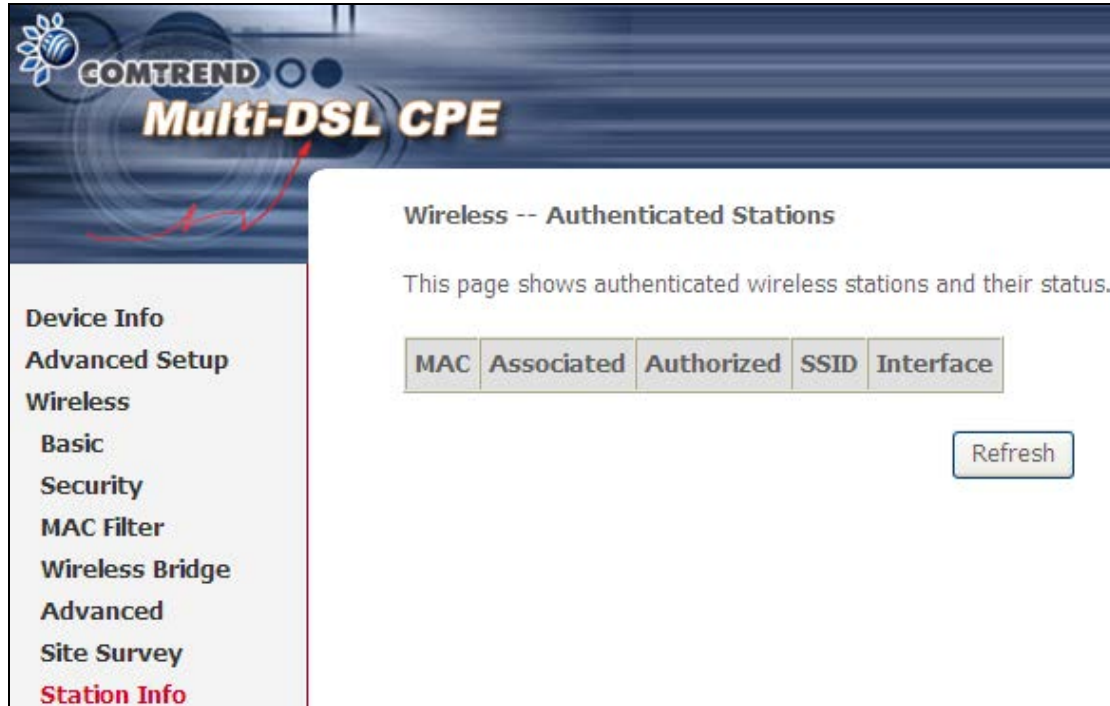
Station Info

Diagnostics

Management

6.7 Station Info

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



The screenshot shows the COMTREND Multi-DSL CPE web interface. The main content area is titled "Wireless -- Authenticated Stations" and contains the text "This page shows authenticated wireless stations and their status." Below this text is a table with the following headers: MAC, Associated, Authorized, SSID, and Interface. To the right of the table is a "Refresh" button. The left navigation menu includes: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Site Survey, and Station Info (highlighted in red).

Consult the table below for descriptions of each column heading.

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

Chapter 7 Diagnostics

The first Diagnostics screen is a dashboard that shows overall connection status. If a test displays a fail status, click the button to retest and confirm the error. If a test continues to fail, click [Help](#) and follow the troubleshooting procedures.

COMTREND Multi-DSL CPE

pppoe_ATM_0 Diagnostics

Your modem is capable of testing your DSL connection. 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 ENET1 Connection:	PASS	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help


Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

Next Connection

Test Test With OAM F4

The second Diagnostics screen (Fault Management) is used for VDSL diagnostics.



802.1ag Connectivity Fault Management
 This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Diagnostics
- Fault Management**
- Management

Chapter 8 Management

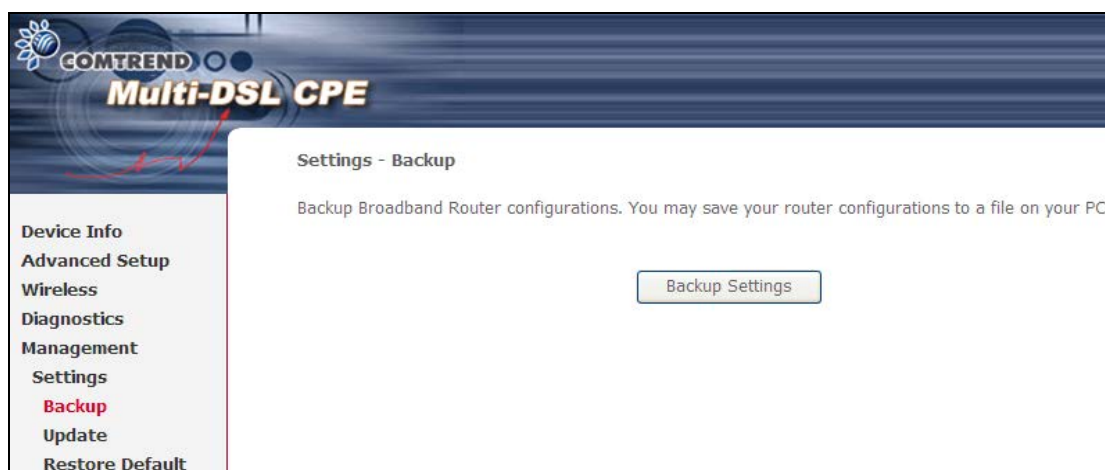
The Management menu has the following maintenance functions and processes:

8.1 Settings

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

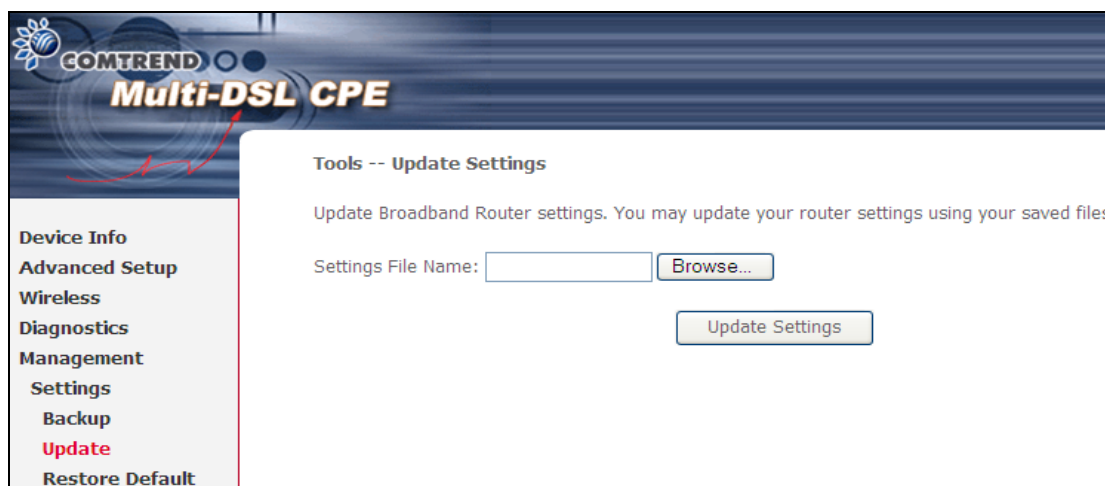
8.1.1 Backup Settings

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



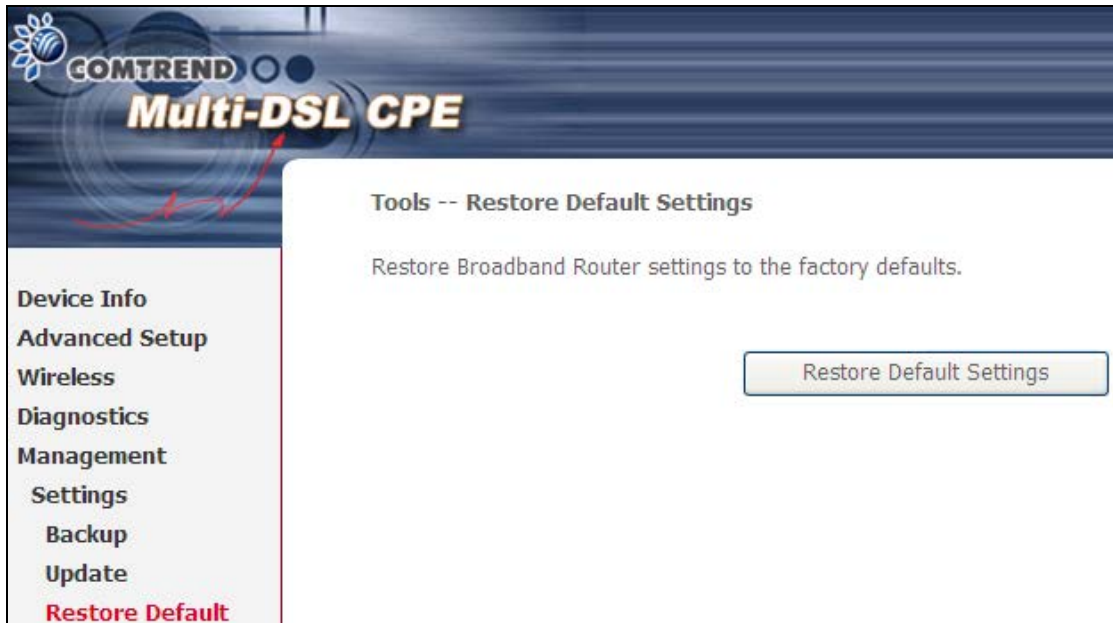
8.1.2 Update Settings

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

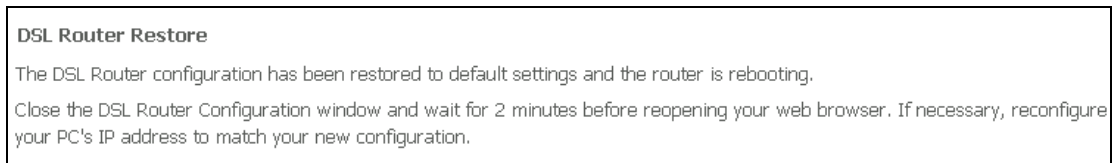


8.1.3 Restore Default

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



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



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

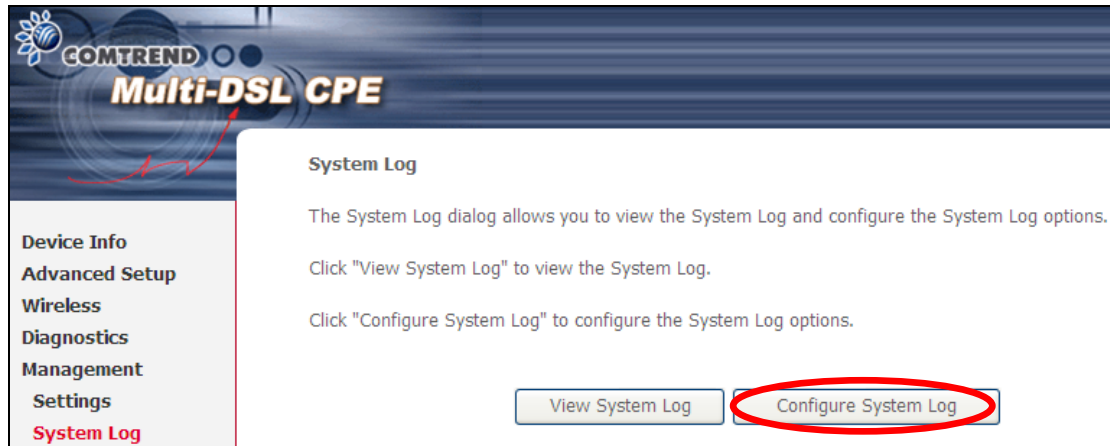
NOTE: This entry has the same effect as the **Reset** button. The VR-3031u board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

8.2 System Log

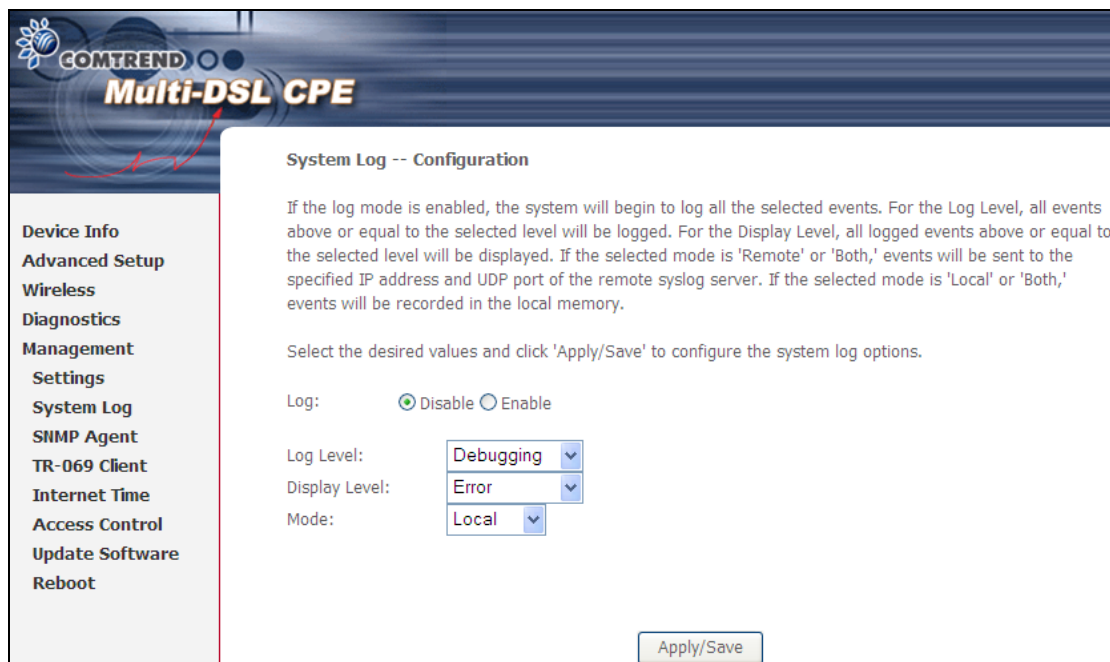
This function allows a system log to be kept and viewed upon request.

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

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



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



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

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

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-3031u SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	Allows the user to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	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.

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 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.

The screenshot shows the 'TR-069 client - Configuration' page in the Comtrend Multi-DSL CPE web interface. The page has a dark blue header with the Comtrend logo and 'Multi-DSL CPE' text. On the left is a navigation menu with options like 'Device Info', 'Advanced Setup', 'Wireless', 'Diagnostics', 'Management', 'Settings', 'System Log', 'SNMP Agent', 'TR-069 Client' (highlighted in red), 'Internet Time', 'Access Control', 'Update Software', and 'Reboot'. The main content area is titled 'TR-069 client - Configuration' and contains the following fields and controls:

- Inform:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Inform Interval:** Text input field containing '300'.
- ACS URL:** Text input field.
- ACS User Name:** Text input field containing 'admin'.
- ACS Password:** Password input field with five dots.
- WAN Interface used by TR-069 client:** Dropdown menu showing 'Any_WAN'.
- Display SOAP messages on serial console:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Connection Request Authentication:** A checked checkbox.
- Connection Request User Name:** Text input field containing 'admin'.
- Connection Request Password:** Password input field with five dots.
- Connection Request URL:** Text input field.

At the bottom of the configuration area are two buttons: 'Apply/Save' and 'GetRPCMethods'.

The table below is provided for ease of reference.

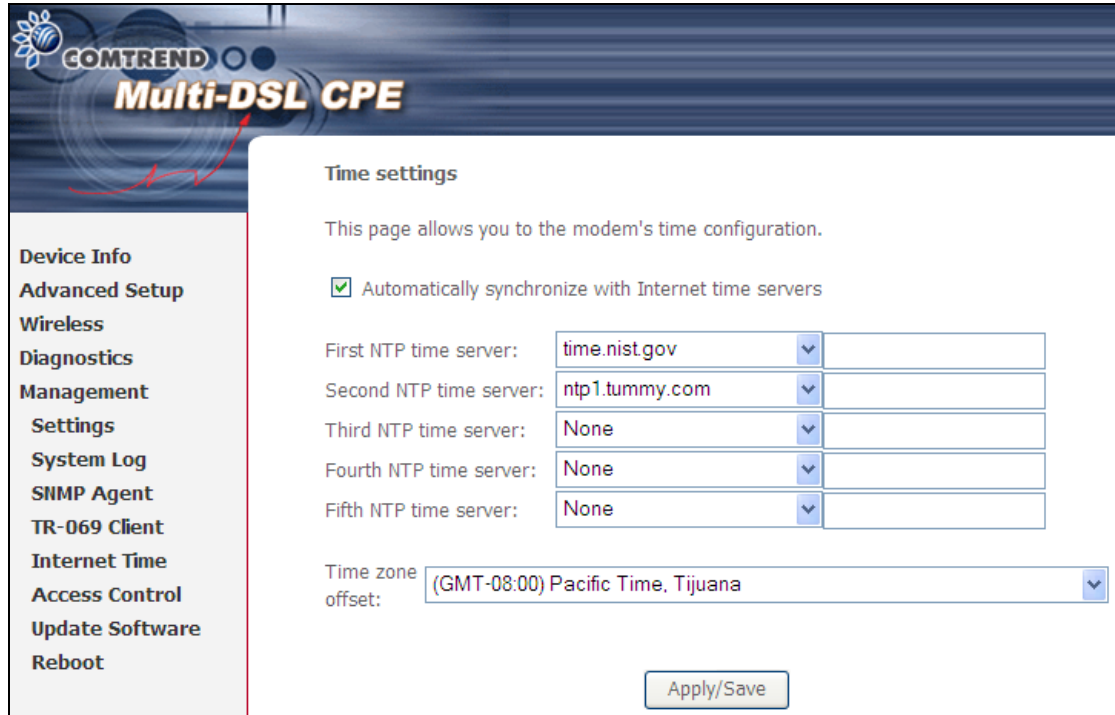
Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter 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.

Option	Description
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.
Display SOAP messages on serial console	Enable/Disable SOAP messages on serial console. This option is used for advanced troubleshooting of the device.
Connection Request	
Authorization	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 VR-3031u.

The **Get RPC Methods** button forces the CPE to establish an immediate connection to the ACS. This may be used to discover the set of methods supported by the ACS or CPE. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods.

8.4 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 **Save/Apply**.



COMTREND Multi-DSL CPE

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:

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Reboot

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.

8.5 Access Control

8.5.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the VR-3031u is controlled through the following three user accounts:

- **root** - unrestricted access to change and view the configuration.
 - **support** - used for remote maintenance and diagnostics of the router
 - **user** - can view configuration settings & statistics and update firmware.
- Use the fields below to change password settings. Click **Save/Apply** to continue.

COMTREND Multi-DSL CPE

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

NOTE: Passwords can be up to 16 characters in length.

8.5.2 Services

COMTREND Multi-DSL CPE

Service Access Control Configuration

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

Service	Current	New
HTTP	Lan	LAN
SSH	Disable	Disable
TELNET	Disable	Disable
SNMP	Disable	Disable
HTTPS	Disable	Disable
FTP	Disable	Disable
TFTP	Disable	Disable
ICMP	Lan+Wan	LAN+WAN

Apply/Save

Select each drop-down menu item and click Apply/Save to configure your Setting.

8.5.3 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 Multi-DSL CPE

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

Click the Add button to display the following.

Access Control

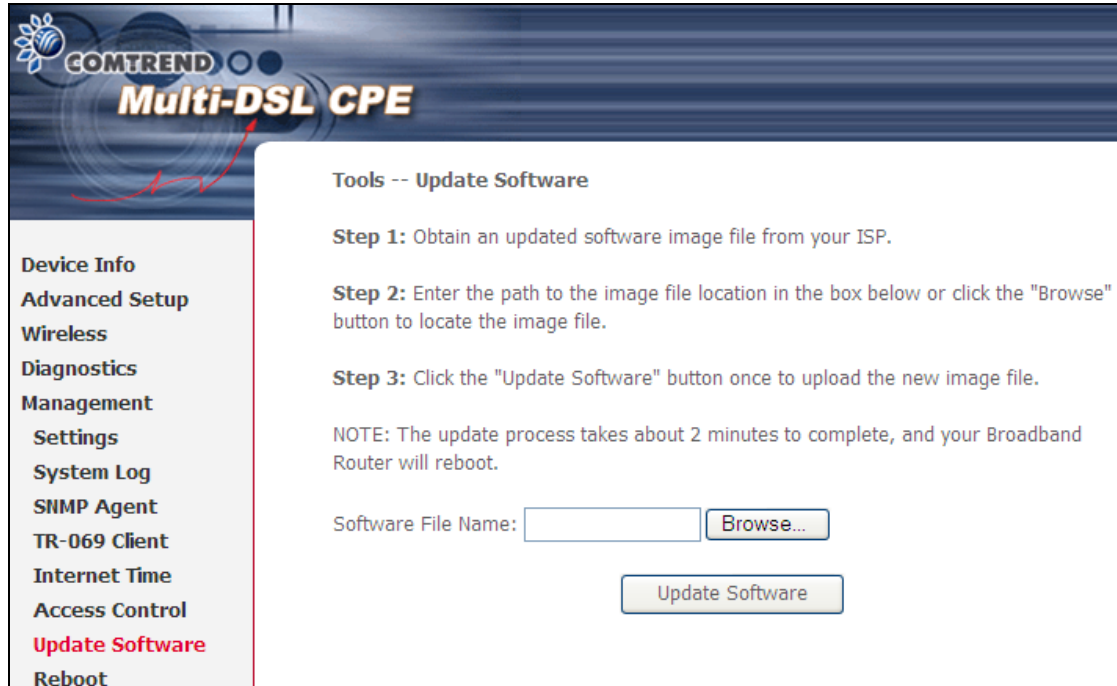
Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

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

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

8.6 Update Software

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



COMTREND Multi-DSL CPE

Tools -- Update Software

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

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

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

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

Software File Name:

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

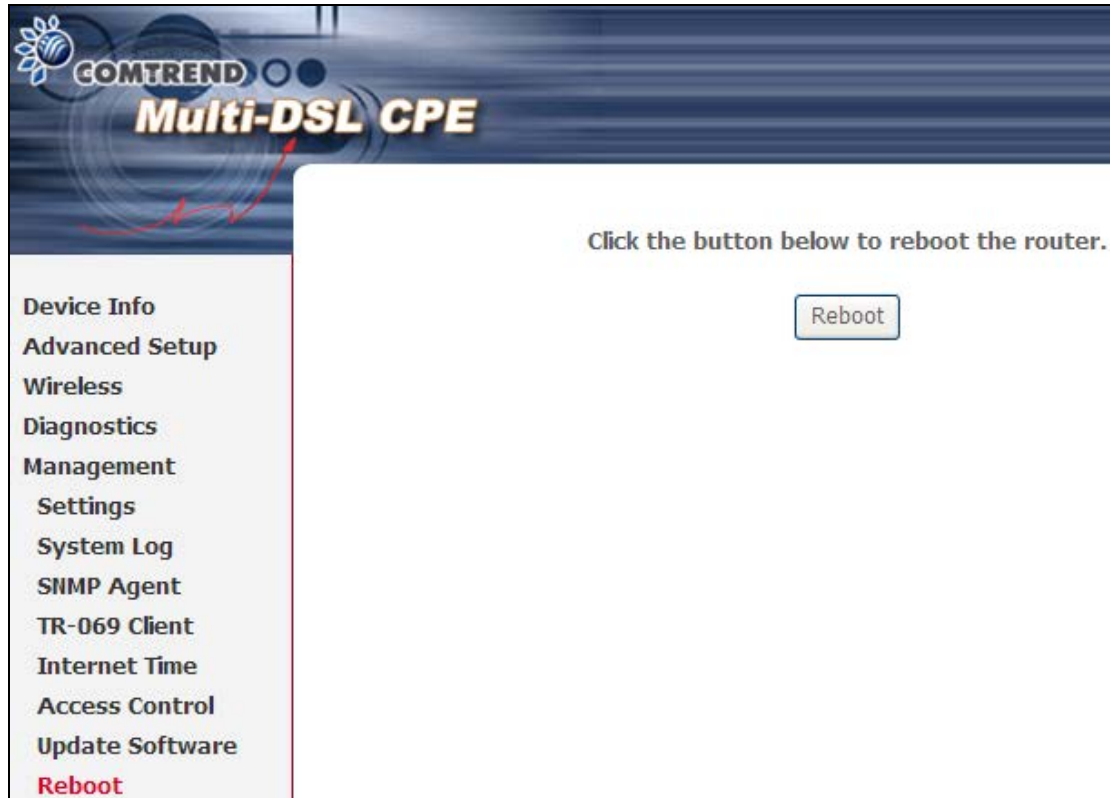
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

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

8.7 Reboot

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

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-3031u, 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 4 for LAN (10/100 Base-T), Reset Button X 1, WPS/WiFi on/off button x1, Wi-Fi Antennas X 2, Power Switch X 1, USB Host

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

VDSL2Downstream : 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 BaseTAuto-sense
MDI/MDX support.....Yes

WLAN Interface

StandardIEEE802.11b/g/n
Encryption.....64/128-bit Wired Equivalent Privacy (WEP)
Channels.....11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate.....Up to 300Mbps
WEPYes
WPAYes
IEEE 802.1xYes
MAC FilteringYes

ATM Attributes

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

PVCs16
AAL typeAAL5
ATM service classUBR/CBR/VBR
ATM UNI supportUNI 3.1/4.0
OAM F4/F5Yes

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 learningIEEE 802.1d
VLAN supportYes
Spanning Tree AlgorithmYes
IGMP ProxyYes

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 SupplyInput: 100 - 240 Vac
Output: 12 Vdc / 1.0 A

Environment Condition

Operating temperature0 ~ 40 degrees Celsius
Relative humidity5 ~ 95% (non-condensing)

Dimensions 171 mm (W) x 39 mm (H) x 122 mm (D)

Kit Weight

(1*VR-3031u, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter) = 0.6 kg

NOTE: Specifications are subject to change without notice
--

Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

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

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

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

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

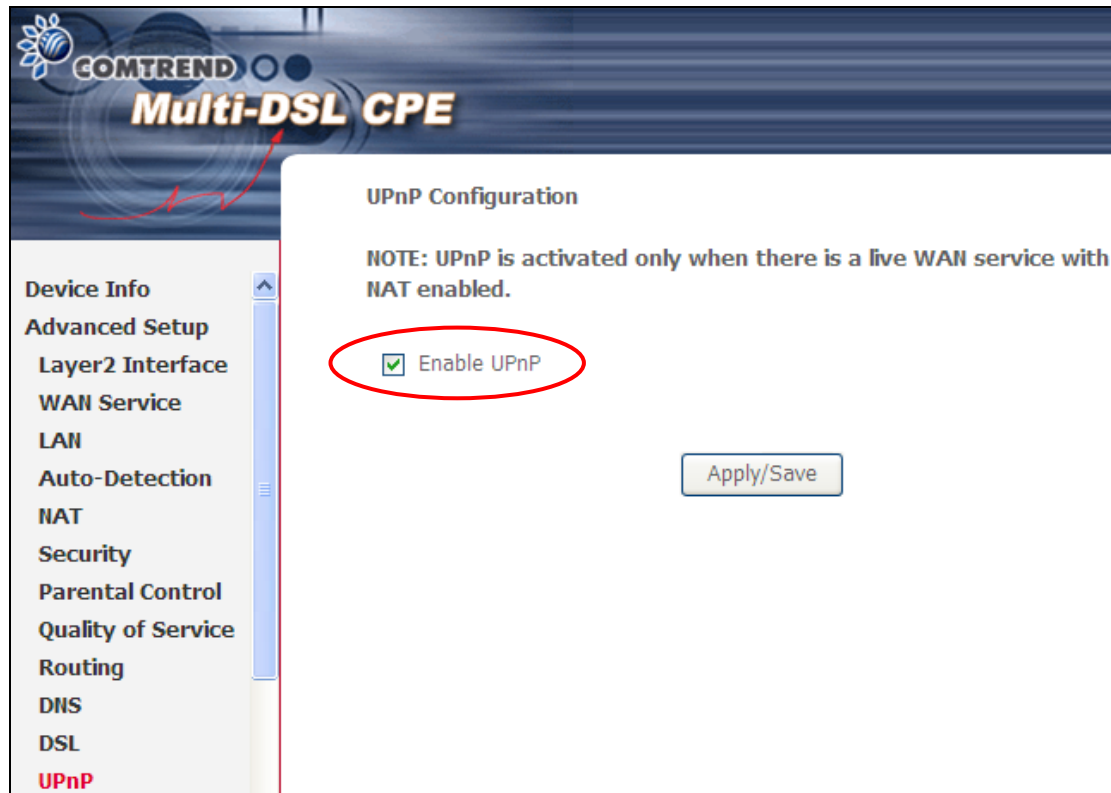
For WAN access, type: `putty -ssh -l support WAN IP address`

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

Appendix E - WSC External Registrar

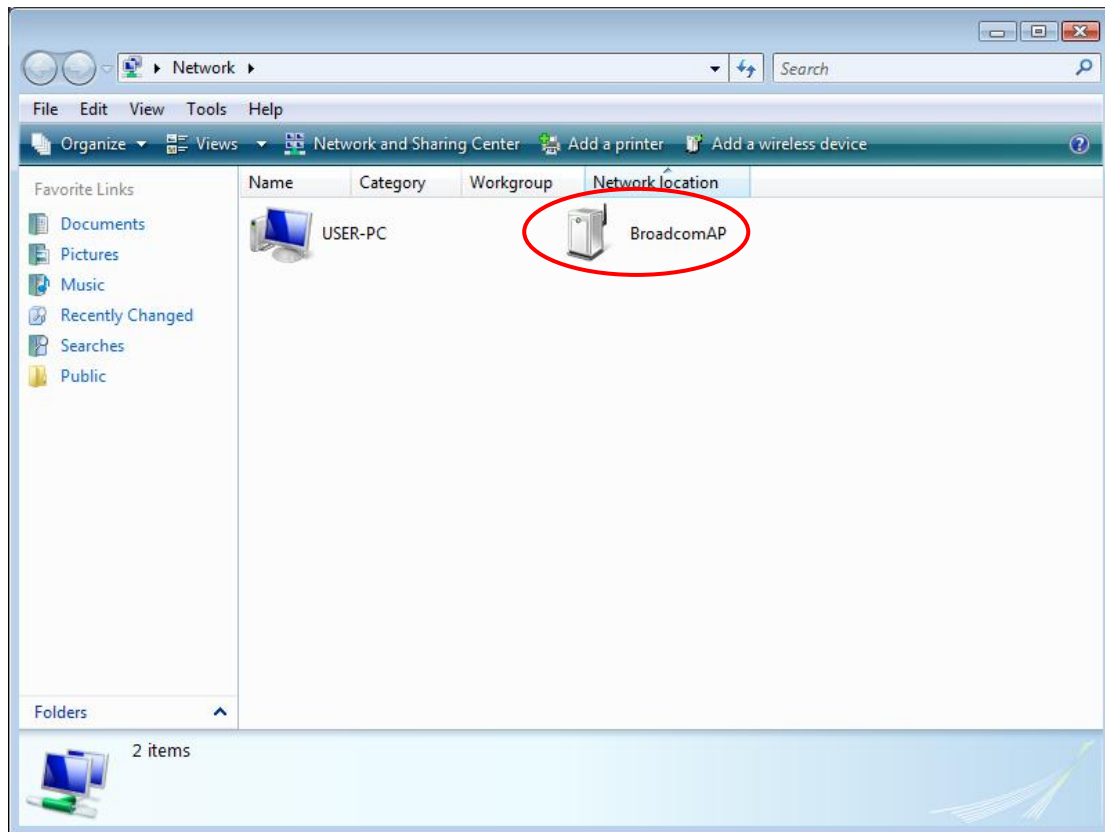
Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows Vista operating system:

Step 1: Enable UPnP on the Advanced Setup → LAN screen in the WUI.



NOTE: A PVC must exist to see this option.

Step 2: Open the Network folder and look for the BroadcomAP icon.



Step 3: On the Wireless → Security screen, enable WSC by selecting **Enabled** from the drop down list box and set the WSC AP Mode to Unconfigured.

COMTREN
Multi-DSL CPE

Device Info
Advanced Setup
Wireless
 Basic
 Security
 MAC Filter
 Wireless Bridge
 Advanced
 Site Survey
 Station Info
Diagnostics
Management

Wireless -- Security

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

WPS Setup

Enable WPS: ▾

Add **Client** (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)

Enter STA PIN Use AP

PIN: [Help](#)

Set **Authorized Station MAC**: [Help](#)

Set **WPS AP Mode**: ▾

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

Lock Device PIN:

Device PIN: [Help](#)

Manual Setup AP

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

Select SSID: ▾

Network Authentication: ▾

WPA/WAPI passphrase: [Click here to display](#)

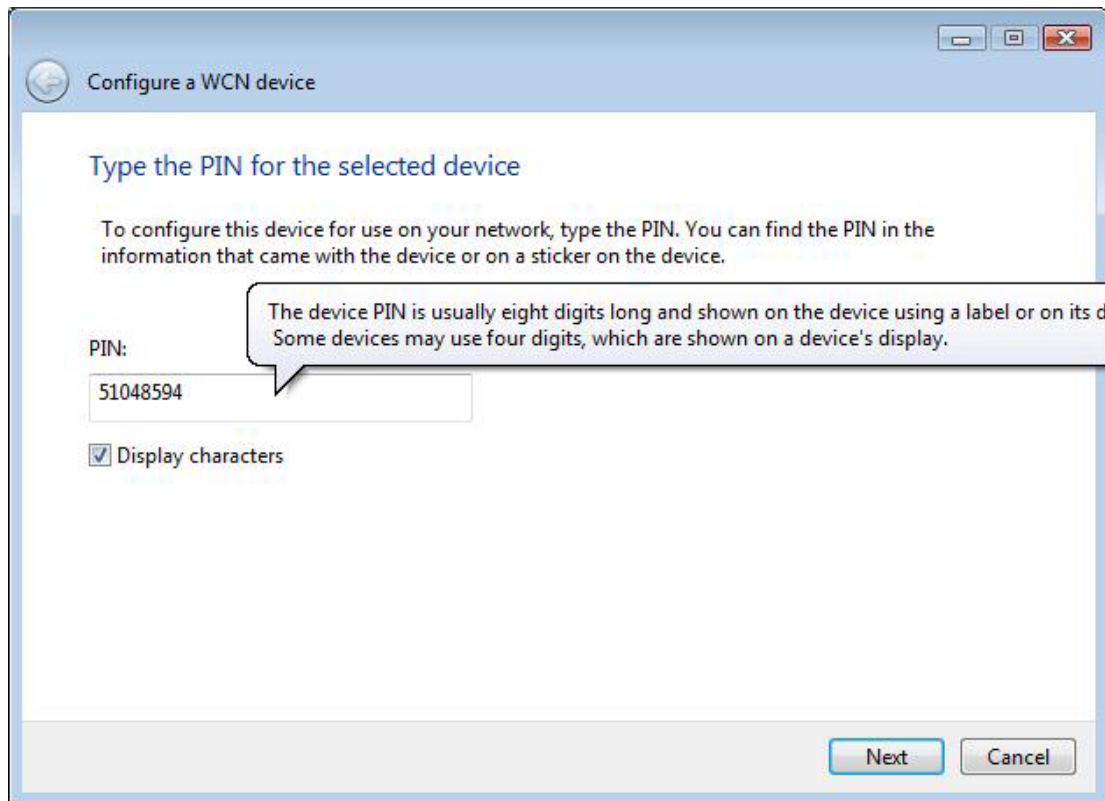
WPA Group Rekey Interval:

WPA/WAPI Encryption: ▾

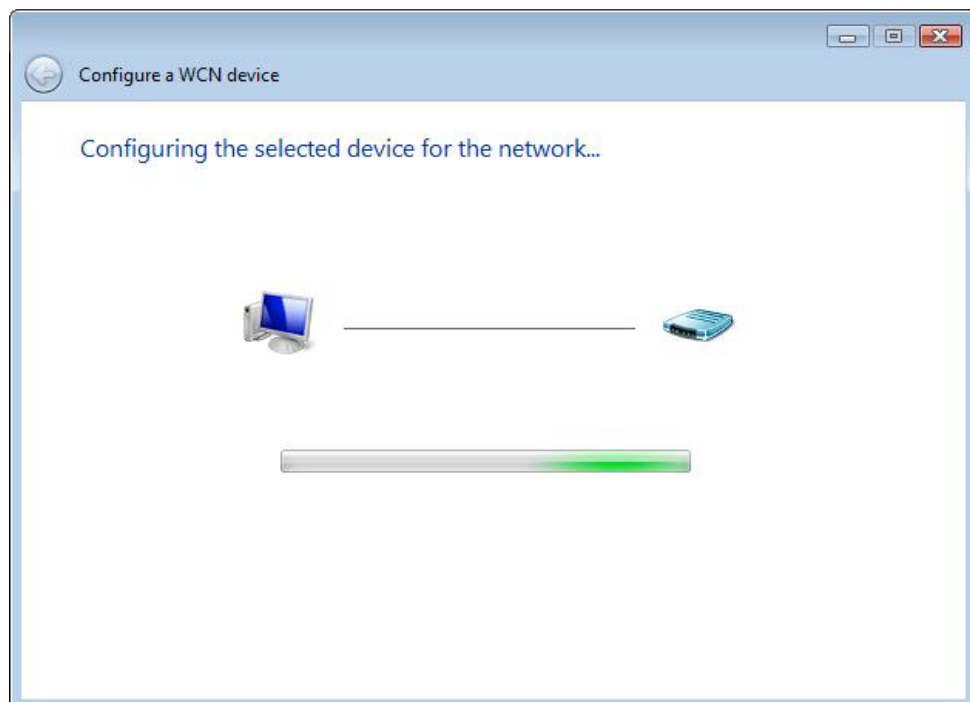
WEP Encryption: ▾

Step 4: Click the **Apply/Save** button at the bottom of the screen. The screen will go blank while the router applies the new Wireless settings.

Step 5: Now return to the Network folder and click the BroadcomAP icon. A dialog box will appear asking for the Device PIN number. Enter the Device PIN as shown on the Wireless → Security screen. Click **Next**.



Step 6: Windows Vista will attempt to configure the wireless security settings.



Step 7: If successful, the security settings will match those in Windows Vista.

Appendix F - Printer Server

These steps explain the procedure for enabling the Printer Server.

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

STEP 1: Enable Print Server from Web User Interface. Select Enable on-board print server checkbox and enter Printer name and Make and model

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

Print Server settings

This page allows you to enable / disable printer support.

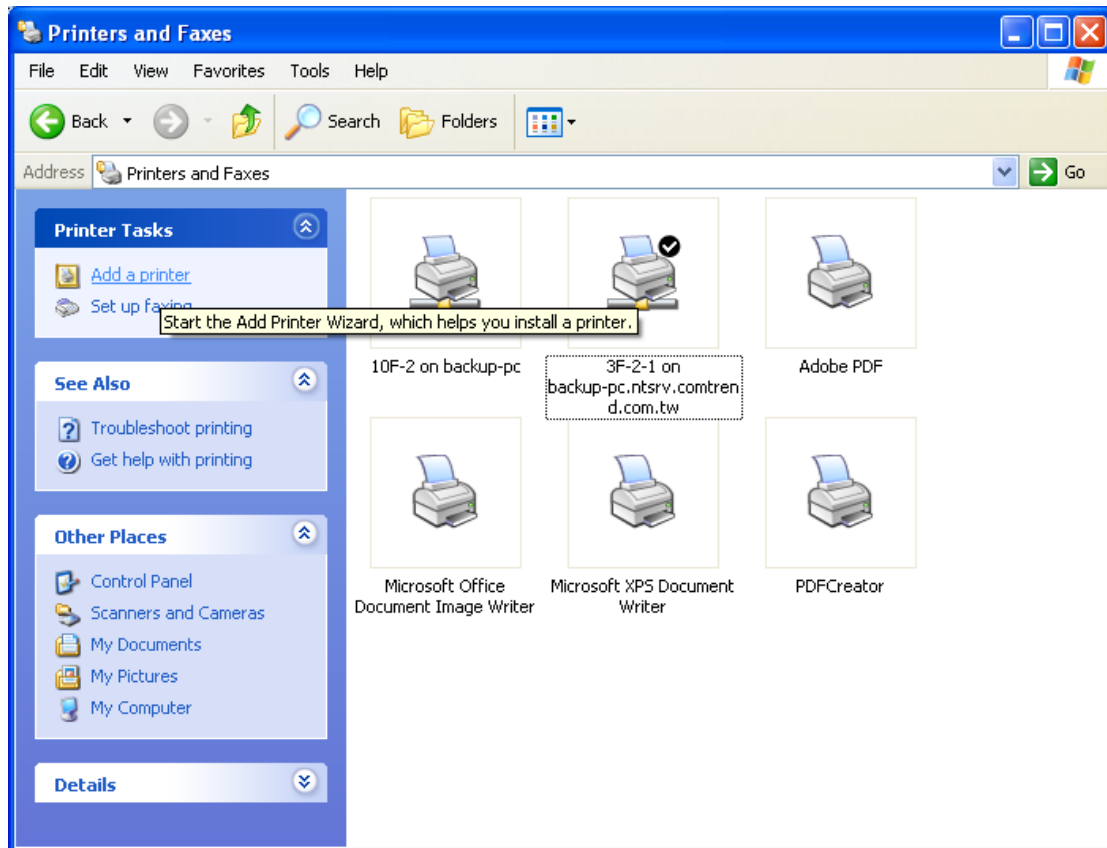
Manufacturer	Product	Serial Number
--------------	---------	---------------

Enable on-board print server.

Printer name

Make and model

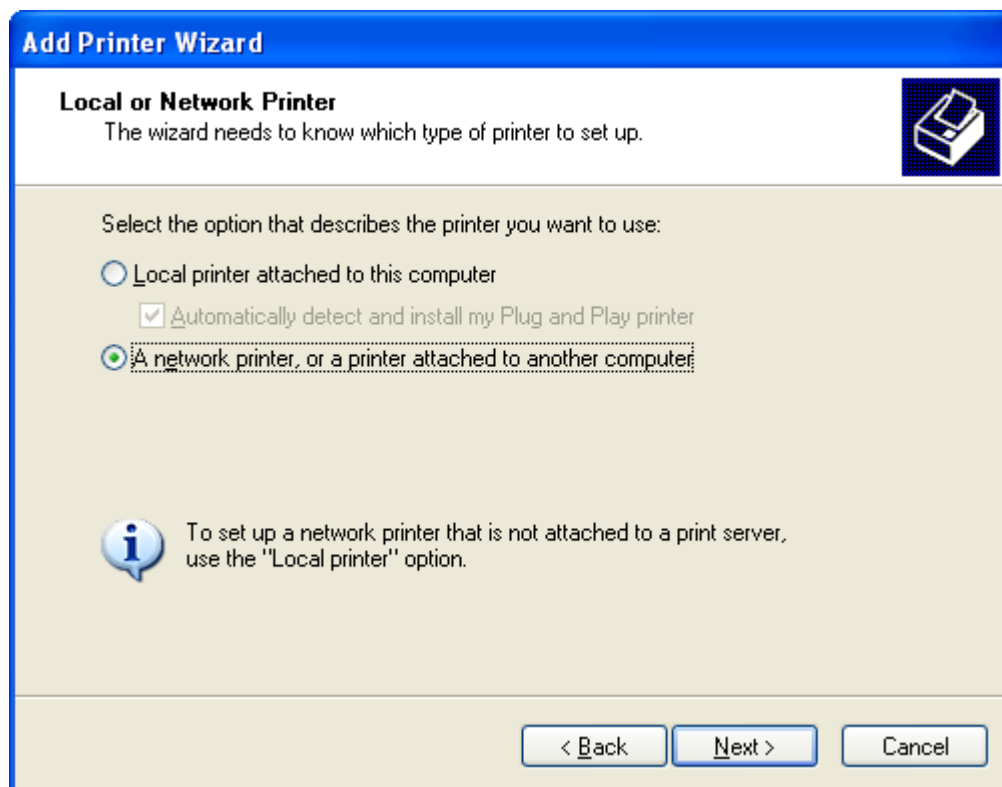
STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



STEP 3: Click **Next** to continue when you see the dialog box below.

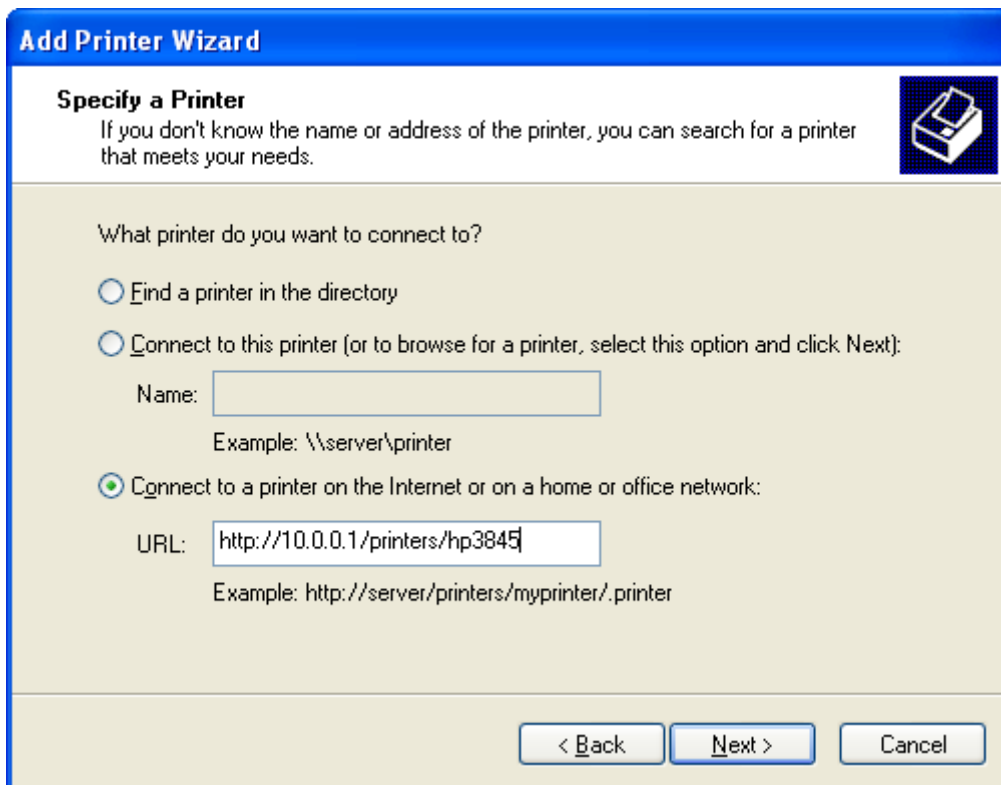


STEP 4: Select **Network Printer** and click **Next**.

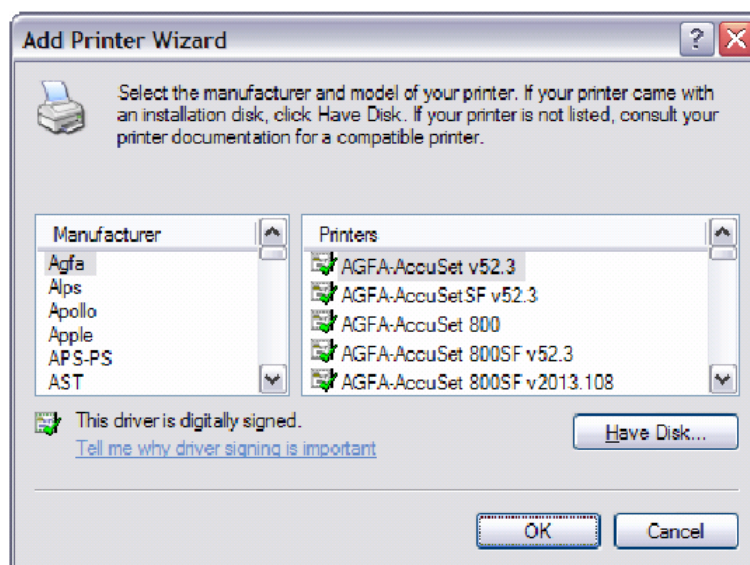


STEP 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. <http://192.168.1.1:631/printers/hp3845>) and click **Next**.

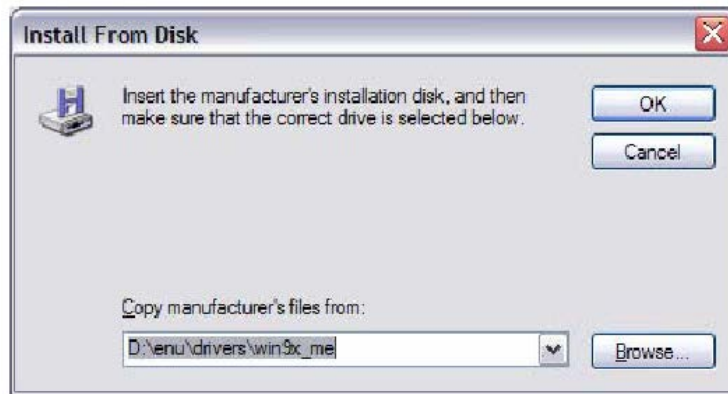
NOTE: The printer name must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.



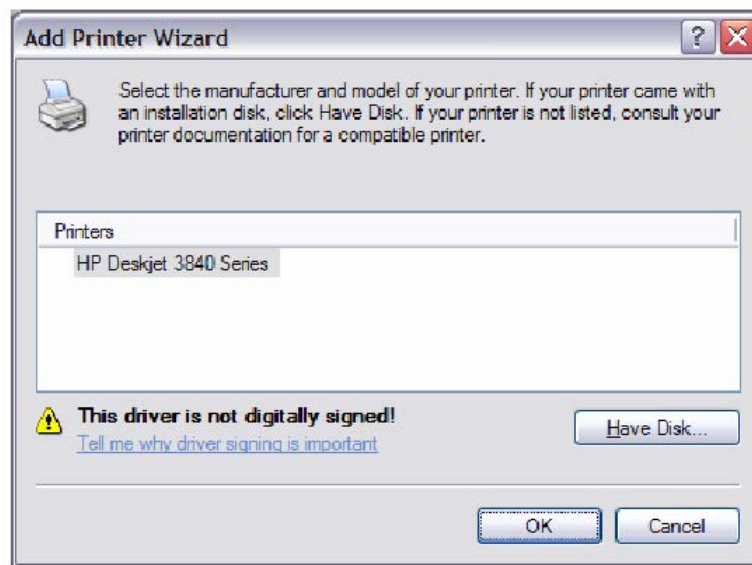
STEP 6: Click **Have Disk** and insert the printer driver CD.



STEP 7: Select driver file directory on CD-ROM and click **OK**.



STEP 8: Once the printer name appears, click **OK**.



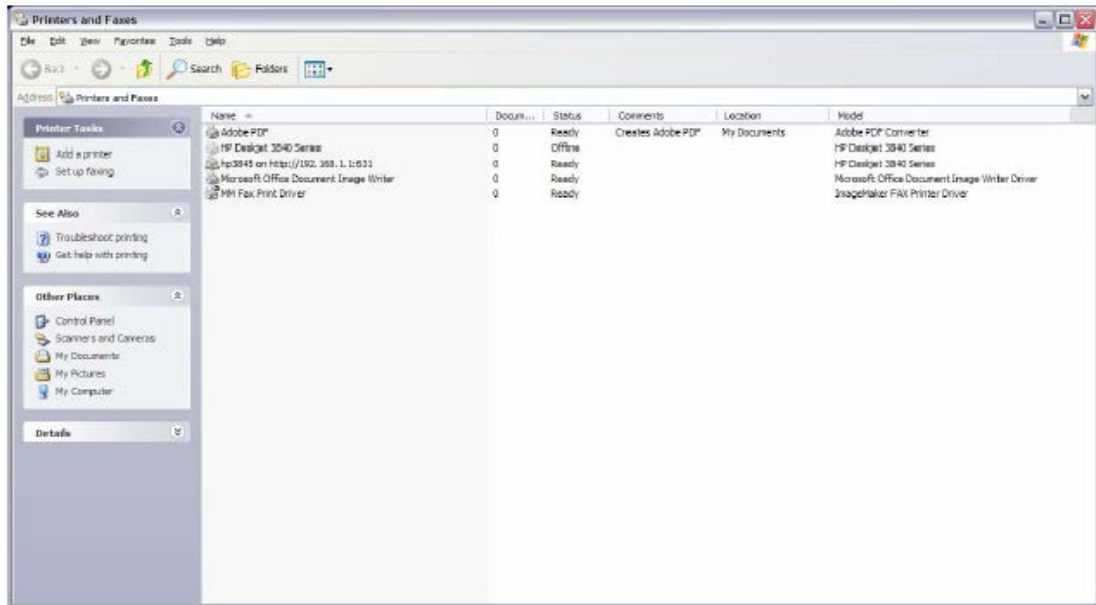
STEP 9: Choose **Yes** or **No** for default printer setting and click **Next**.



STEP 10: Click Finish.



STEP 11: Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.



Appendix G - 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.

G1 ~ Layer 2 Interfaces

Every layer2 interface operates in one of three modes: Default, VLAN Mux or MSC. A short introduction to each of these three modes is included below for reference. It is important to understand the differences between these connection modes, as they determine the number and types of connections that may be configured.

VLAN MUX MODE

Multi-Service Connection (VLAN MUX) mode supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported, while Bridging is unavailable for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces (see [G3 ~ More About VLAN MUX Mode](#)).

G1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE: The VR-3031u supports up to 16 ATM interfaces.

STEP 1: Go to Advanced Setup → Layer2 Interface → ATM Interface.

DSL ATM Interface Configuration												
Choose Add, or Remove to configure DSL ATM interfaces.												
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	<input type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="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)

Heading	Description
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
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 MSC Mode – Multiple 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 Latency
 Path0 (Fast)
 Path1 (Interleaved)

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 Latency, 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												
Choose Add, or Remove to configure DSL ATM interfaces.												
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	<input type="checkbox"/>
atm1	5	555	Path0	UBR				EoA	VlanMuxMode	Support	8/WRR/1	<input type="checkbox"/>

To add a WAN connection go to [section G2 ~ WAN Connections](#).

G1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The VR-3031u supports up to four PTM interfaces.

STEP 4: Go to Advanced Setup → Layer2 Interface → PTM Interface.

DSL PTM Interface Configuration					
Choose Add, or Remove to configure DSL PTM interfaces.					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="checkbox"/>

This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
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. MSC Mode – Multiple Services over one interface.
QoS	Quality of Service (QoS) status.
Remove	Select interfaces to remove.

STEP 5: 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 DSL Latency

Path0 (Fast)
 Path1 (Interleaved)

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)

There are many settings that can be configured here including: DSL Latency, PTM Priority, Connection Mode and Quality of Service.

STEP 6: 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					
Choose Add, or Remove to configure DSL PTM interfaces.					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="checkbox"/>

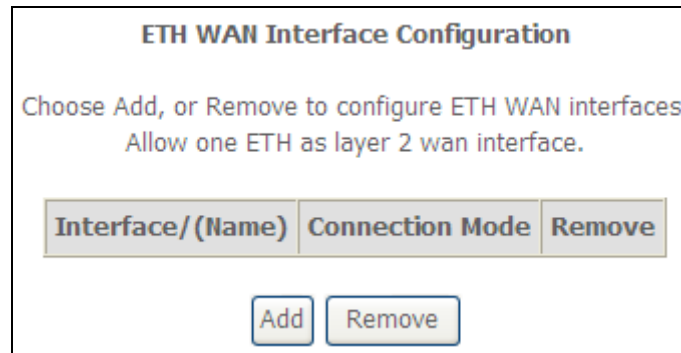
To add a WAN connection go to [section G2 ~ WAN Connections](#).

G1.3 Ethernet WAN Interface

Some models of the VR-3031u support a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet WAN interface.

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

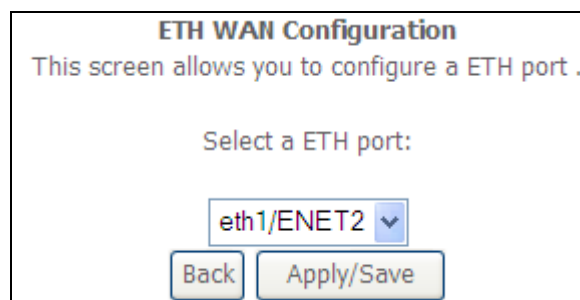
STEP 1: Go to Advanced Setup → Layer2 Interface → ETH Interface.



This table is provided here for ease of reference.

Heading	Description
Interface/(Name)	ETH WAN Interface
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection MSC Mode – Multiple Service over one Connection
Remove	Select the checkbox and click Remove to remove the connection.

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



STEP 3: **STEP 4:** Click **Apply/Save** to confirm your choice.

The figure below shows an Ethernet WAN interface configured in VlanMuxMode.

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth1/ENET2	VlanMuxMode	<input type="checkbox"/>

To add a WAN connection go to [section G2 ~ WAN Connections](#).

G2 ~ WAN Connections

In Default Mode, the VR-3031u supports one WAN connection for each interface, up to a maximum of 8 connections. VLAN Mux and MSC support up to 16 connections.

To setup a WAN connection follow these instructions.

STEP 1: Go to the Advanced Setup → WAN Service screen.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Connect/Disconnect	Remove	Edit
ppp0.1	pppoe_ATM_0	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit
ppp1.1	pppoe_PT_M_0	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

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

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

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]:

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

- (1) For [PPP over ETHERNET \(PPPoE\)](#), go to page 147.
- (2) For [IP over ETHERNET \(IPoE\)](#), go to page 153.
- (3) For [Bridging](#), go to page 159.
- (4) For [PPP over ATM \(PPPoA\)](#), go to page 161.
- (5) For [IP over ATM \(IPoA\)](#), go to page 166.

The subsections that follow continue the WAN service setup procedure.

G2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox at the bottom of this screen.

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:

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**

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second)

Number of retries:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Enable NAT

Enable Firewall

Use Static IPv4 Address

MTU:

Enable PPP Manual Mode

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

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.

KEEP ALIVE INTERVAL

This option configures the interval between each PPP LCP request and the amount of time to wait for the PPP server to reply to the LCP request. If the time expired on all requests, the current PPP session would be dropped.

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-3031u 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](#).

MTU

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 MANUAL MODE

Use this button to manually connect/disconnect PPP sessions.

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.

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 ppp1.1	ppp2.2

->
<-

Back Next

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

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

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

Available WAN Interfaces

ppp0.1 ppp1.1	<input type="button" value="->"/> <input type="button" value="<-"/>	ppp2.2
------------------	--	--------

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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

WAN Setup - Summary

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

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

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

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

G2.2 IP over ETHERNET (IPoE)

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:

Back

Next

NOTE: If IPv6 networking is enabled, an additional set of instructions, radio buttons, and text entry boxes will appear at the bottom of the screen. These configuration options are quite similar to those for IPv4 networks.

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

No Multicast VLAN Filter

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.

NO MULTICAST VLAN FILTER

Tick the checkbox to Enable/Disable multicast VLAN filter.

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
ppp0.1 ppp1.1	atm0.2

->
<-

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

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

DNS Server Configuration

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

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

ppp0.1
ppp1.1



atm0.2

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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

WAN Setup - Summary

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

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

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

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

G2.3 Bridging

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:	Disabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. 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-3031u will be inaccessible for remote management or technical support from the WAN.

G2.4 PPP over ATM (PPPoA)

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: ▼

Configure Keep-alive (PPP echo-request) Interval and the Number of retries

Interval:(second)

Number of retries:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Enable NAT
- Enable Firewall
- Use Static IPv4 Address

MTU:

- Enable PPP Manual Mode
- Enable PPP Debug Mode

Multicast Proxy

- Enable IGMP Multicast Proxy
- No Multicast VLAN Filter

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.)

KEEP ALIVE INTERVAL

This option configures the interval between each PPP LCP request and the amount of time to wait for the PPP server to reply to the LCP request. If the time expired on all requests, the current PPP session would be dropped.

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-3031u 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](#).

ENABLE PPP MANUAL MODE

Use this button to manually connect/disconnect PPP sessions.

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

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.

NO MULTICAST VLAN FILTER

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

pppoa0

Available Routed WAN Interfaces

> <

Back Next

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

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

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

pppoa0

Available WAN Interfaces

> <

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Back Next

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

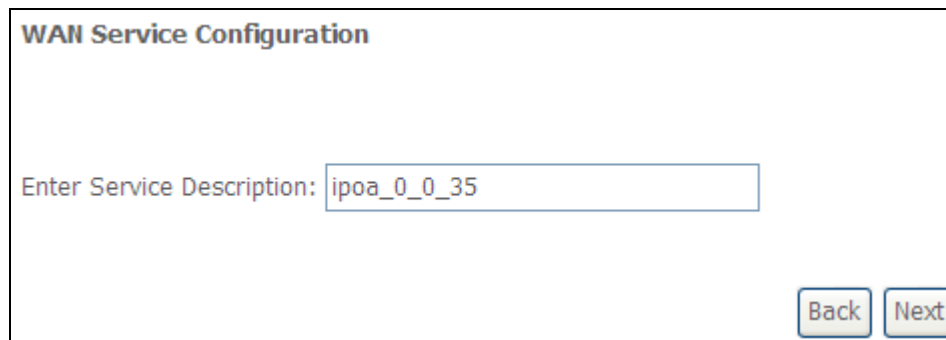
Make sure that the settings below match the settings provided by your ISP.

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 **Reboot**.

G2.5 IP over ATM (IPoA)

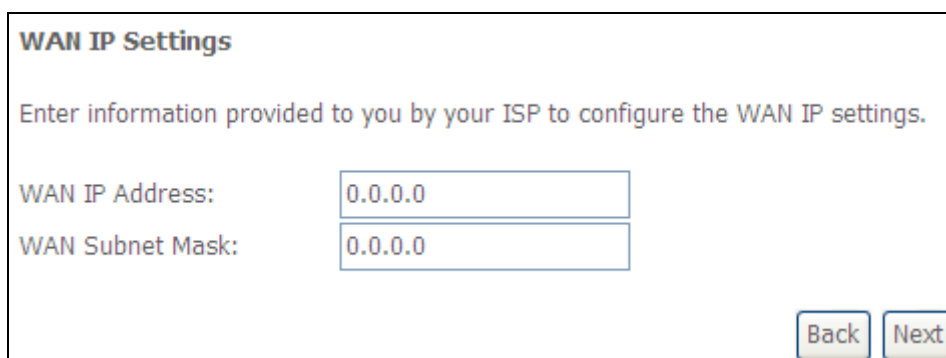


WAN Service Configuration

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

No Multicast VLAN Filter

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.

NO MULTICAST VLAN FILTER

Tick the checkbox to Enable/Disable multicast VLAN filter.

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

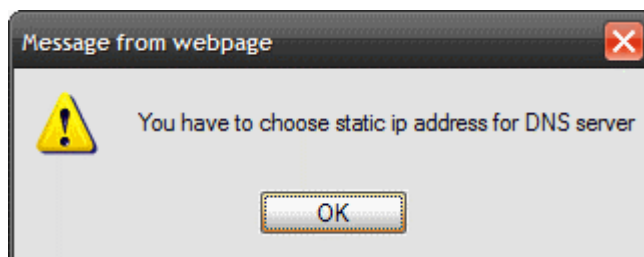
Routing -- Default Gateway

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.

<p>Selected Default Gateway Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;">ipoa0</div>	<input type="button" value="->"/> <input type="button" value="<-"/>	<p>Available Routed WAN Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"></div>
--	--	---

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

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



STEP 5: Choose an interface to be the default gateway.

DNS Server Configuration

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

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

Select DNS Server Interface from available WAN interfaces:

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"></div>	<input type="button" value="->"/> <input type="button" value="<-"/>	<p>Available WAN Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"></div>
---	--	---

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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

WAN Setup - Summary

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

Connection Type:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	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 **Reboot**.

G3 ~ More About VLAN MUX Mode

The procedure for WAN connection setup in multiple service [VLAN Mux](#) mode is as follows:

STEP 1: Create a Layer2 interface in VLAN MUX connection mode.

STEP 2: Add WAN connections to the interface (Bridge, PPPoE or IPoE).

STEP 3: Use [Interface Grouping](#) to connect LAN and WAN interfaces.

These three steps are repeated below with screenshots added for reference.

STEP 1: Create a Layer2 interface in VLAN MUX connection mode.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

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	<input type="checkbox"/>

STEP 2: Add WAN connections to the interface (Bridge, PPPoE or IPoE).

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Connect/Disconnect	Remove	Edit
ppp0.1	pppoe_0_0_35.6	PPPoE	0	6	Disabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

NOTES: If QoS is configured on the first VLAN MUX connection, it will be configured by default for all subsequent connections.

If a MSC connection is removed every other VLAN MUX connection should be removed to avoid potential configuration problems.

STEP 3: Use [Interface Grouping](#) to connect LAN and WAN interfaces.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			ENET4	
MSC1	<input type="checkbox"/>	atm0_2	ENET1	
			ENET2	
			ENET3	
MSC2	<input type="checkbox"/>	atm0_3	wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	
MSC3	<input type="checkbox"/>	ppp0_1	ETHWAN	

See the instructions in [Interface Grouping](#) for help with this final step.