COMTREND CORPORATION

CT-5374

Multi-DSL WLAN Router

User Manual

Version A3.0, March 28, 2011

Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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

⚠ WARNING

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

FCC Compliance

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

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

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Copyright

NOTE:	This document is subject to change without notice.

Protect Our Environment

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

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

Table of Contents

Chapter 1 Introduction

The CT-5374 Multi-DSL WLAN Router provides wired and wireless access for high-bandwidth applications in the home or office. It includes four fast Ethernet ports and supports ADSL2/2+ and VDSL2 connections with DSLAM switching. ADSL2+ connections support multiple simultaneous Internet connections while VDSL2 connections are suitable for triple play (Video + Voice + Data) applications.

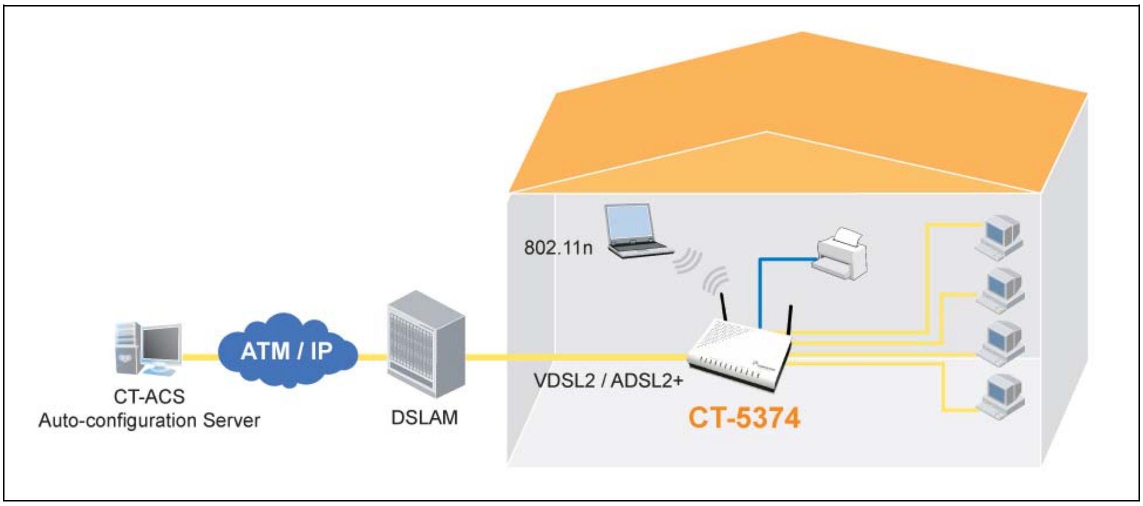
An integrated 802.11n WLAN Access Point (AP) provides faster wireless connections with increased range, when compared with 802.11b and 802.11g, without sacrificing backwards compatibility with these older wireless standards. WPS (Wi-Fi Protected Setup) and Wi-Fi On/Off buttons are positioned on the front panel for easy wireless network setup and control.

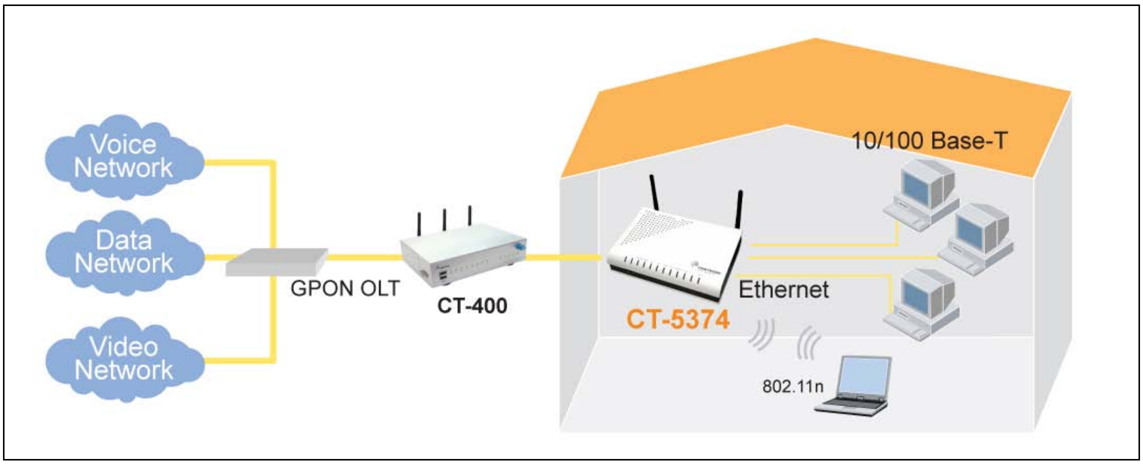
1.1 Features

- Integrated 802.11n AP (802.11b/g backward-compatible)
- Up to VDSL2 17a profile support
- IP and Per-VC packet level QoS
- WPA/WPA2 and 802.1x
- RADIUS client
- Static routing & RIP/RIP v2
- NAT/PAT
- IGMP Proxy and fast leave
- Web-based management
- Supports remote administration
- Configuration backup and restoration
- Firmware upgrade and configuration
- Automatic ADSL2+ / VDSL2 switching based on DSLAM setting
- Auto PVC configuration
- Supports up to 16 VCs
- WMM & UPnP
- IP/MAC filtering
- Dynamic IP assignment
- Parental Control
- DHCP Server/Relay/Client
- DNS Relay/Proxy
- FTP/TFTP server
- TR-069/TR-098/TR-104/TR-111

1.2 Application

The following diagrams depict typical applications of the CT-5374.





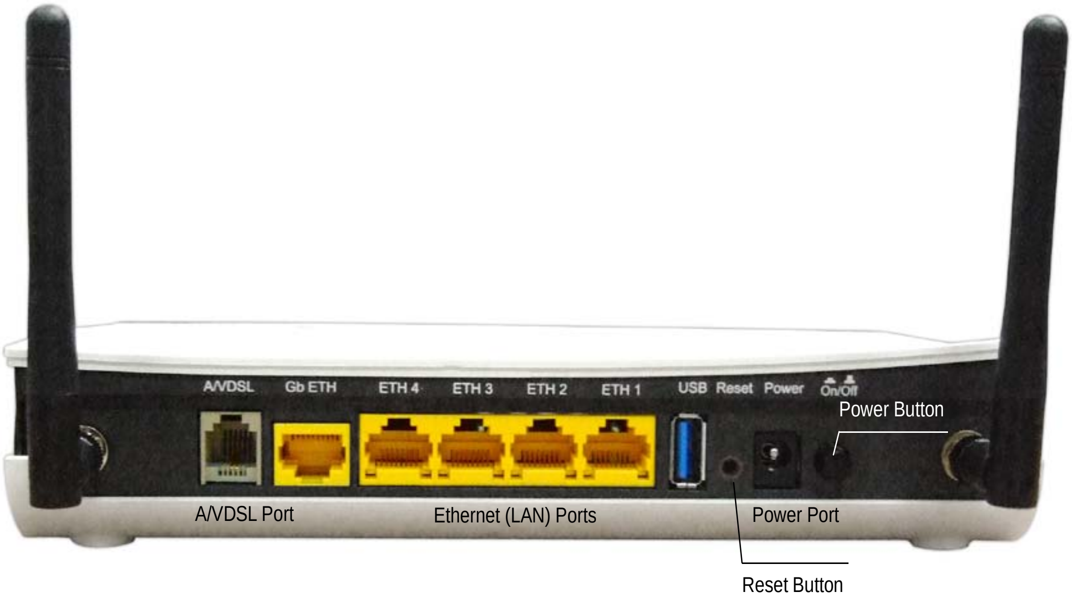
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



Power ON

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section 2.2 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 5 to 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 20 seconds, the CT-5374 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.

Connection to USB host port
With software support, users can connect USB devices such as printers and a hard disc to the router. For this software release, printer service is supported.

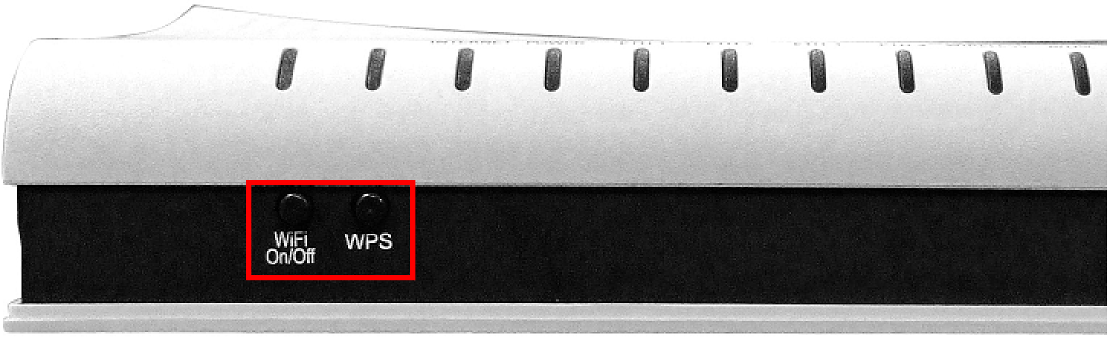
Ethernet (LAN) Ports
Use 10/100 BASE-T RJ-45 cables to connect up to four network devices. These ports are auto-sensing MDI/X; so either straight-through or crossover cable can be used.

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

DSL Port
Connect to an ADSL2/2+ or VDSL with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

FRONT PANEL

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

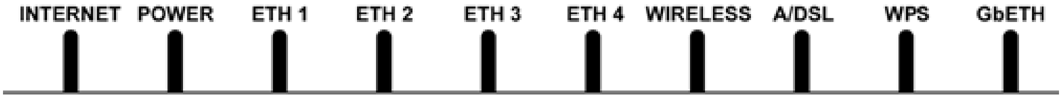


WiFi Switch
Press this button to enable/disable the wireless LAN (WLAN).

WPS Button
Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode (see 6.2.1 WPS for instructions).

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
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.)
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 1X-4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
WIRELESS	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.
A/VDSL	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.

WPS	Green	On	WPS enabled.
		Off	WPS disenabled.
		Blink	The router is searching for WPS clients.
GbETH	Green (for 10/100 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.
	Amber (for 10/100/1000 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- User access (username: **user**, password: **user**)
- Remote (WAN) access (username: **support**, password: **support**)
- Administrator access: **enabled**
- User access: **disabled**
- Remote (WAN) access: **disabled**
- 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 five 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 CT-5374 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

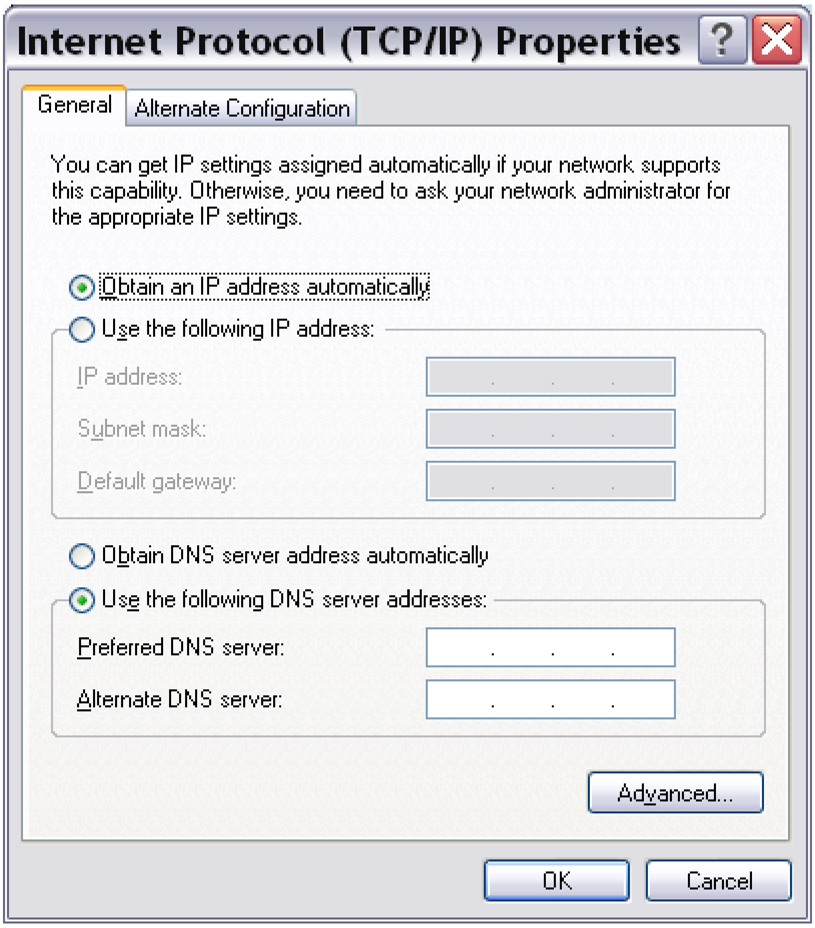
To obtain an IP address from the DCHP server, follow the steps provided below.

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

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

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

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



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

STATIC IP MODE

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

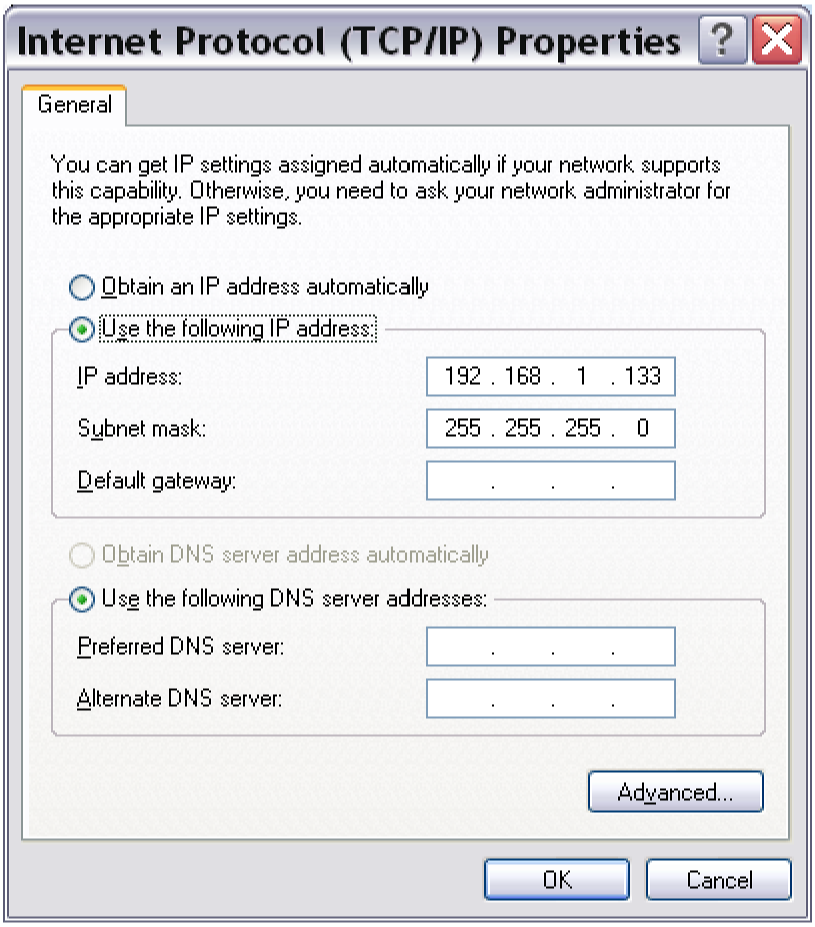
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

3.3 Login Procedure

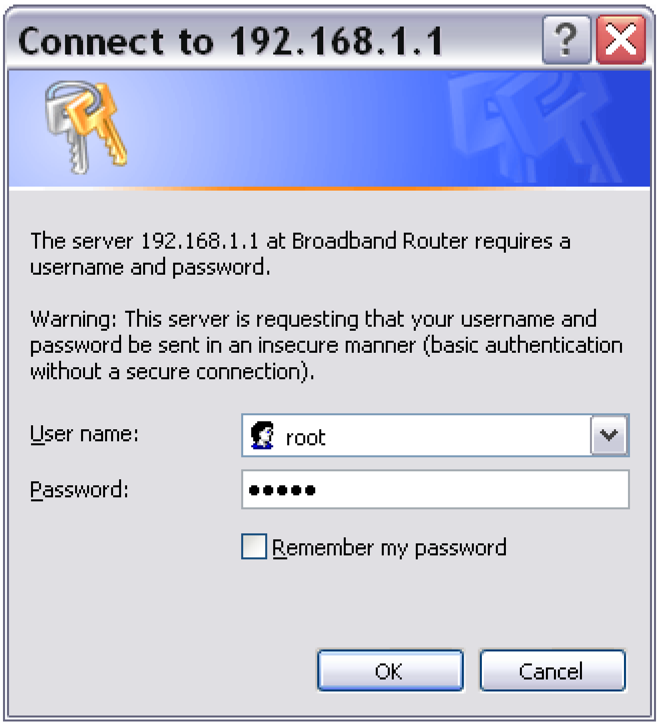
Perform the following steps to login to the web user interface.

NOTE: The default settings can be found in 3.1 Default Settings.

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

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Chapter 4 Device Information screen and login with remote username and password.

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



Connect to 192.168.1.1

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

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

User name: root

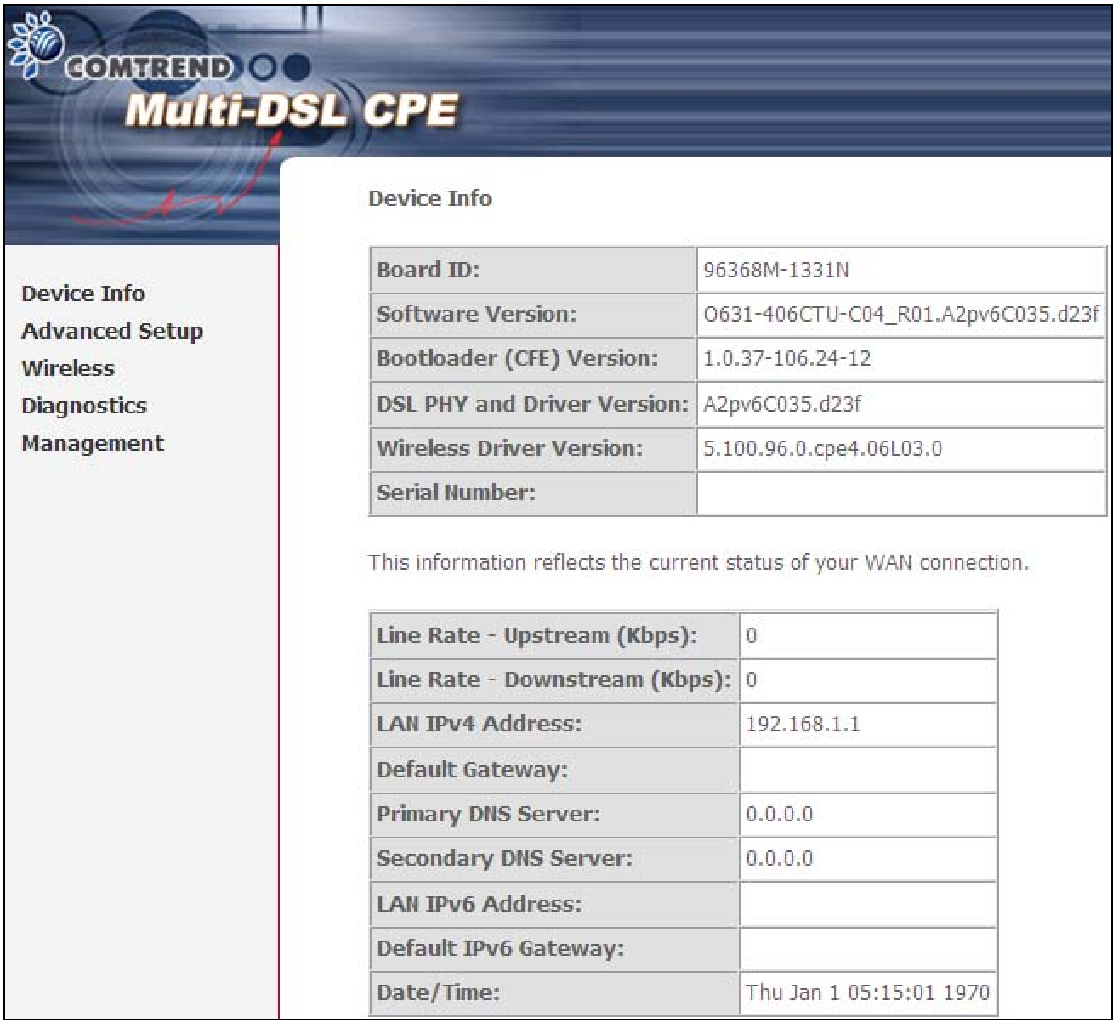
Password: •••••

□ Remember my password

Click **OK** to continue.

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

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



Device Info

Board ID:	96368M-1331N
Software Version:	O631-406CTU-C04_R01.A2pv6C035.d23f
Bootloader (CFE) Version:	1.0.37-106.24-12
DSL PHY and Driver Version:	A2pv6C035.d23f
Wireless Driver Version:	5.100.96.0.cpe4.06L03.0
Serial Number:	

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
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 05:15:01 1970

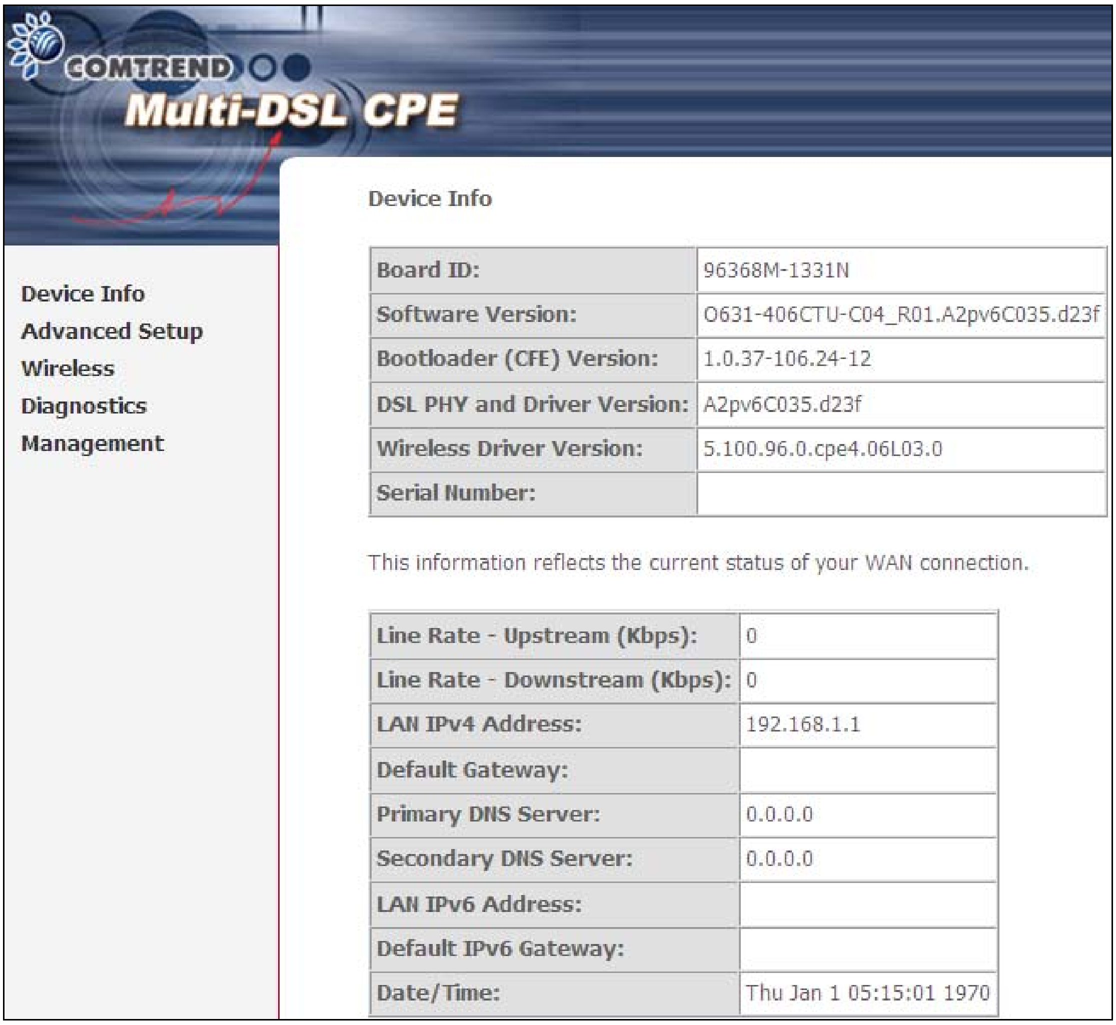
Chapter 4 Device Information

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:	96368M-1331N
Software Version:	O631-406CTU-C04_R01.A2pv6C035.d23f
Bootloader (CFE) Version:	1.0.37-106.24-12
DSL PHY and Driver Version:	A2pv6C035.d23f
Wireless Driver Version:	5.100.96.0.cpe4.06L03.0
Serial Number:	

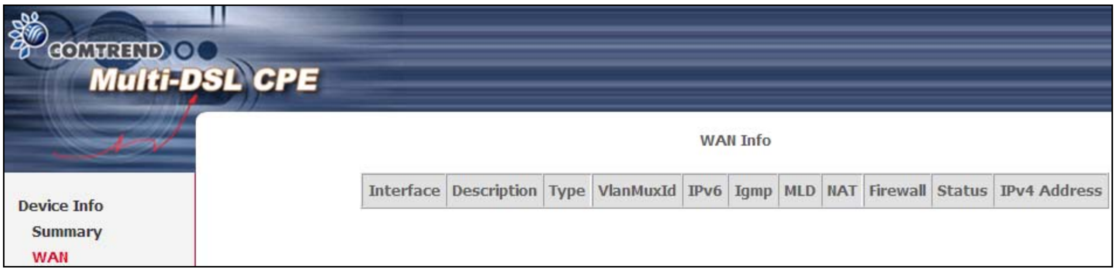
This information reflects the current status of your WAN connection.

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
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 05:15:01 1970

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

4.1 WAN

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



WAN Info

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

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

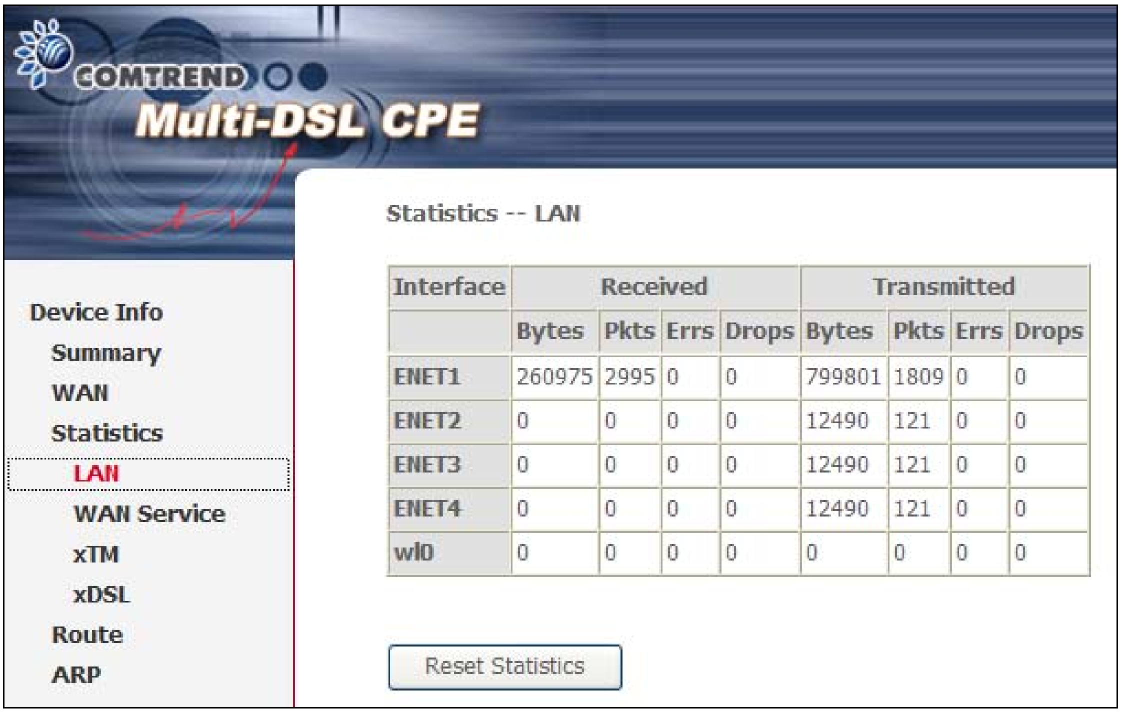
4.2 Statistics

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.



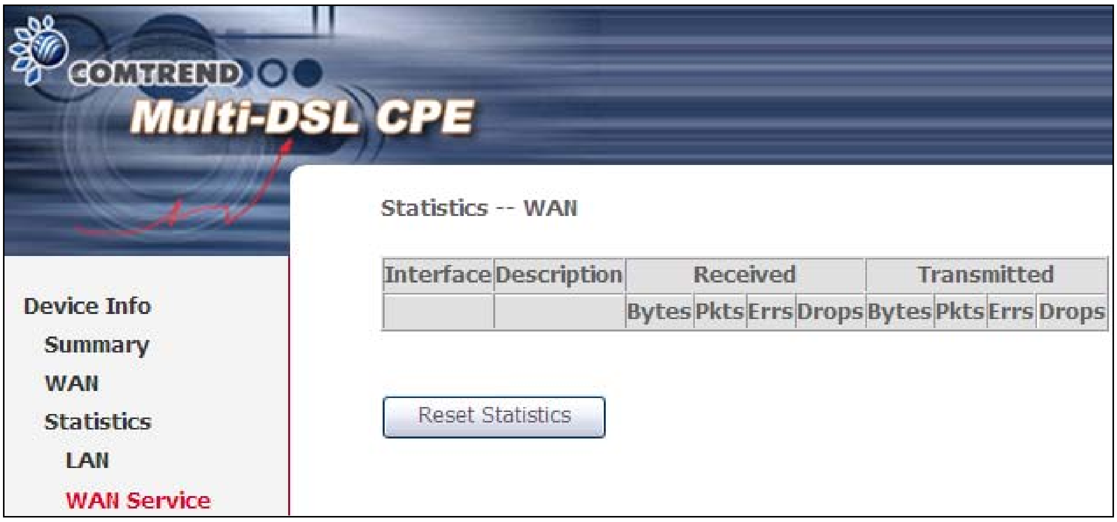
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ENET1	260975	2995	0	0	799801	1809	0	0
ENET2	0	0	0	0	12490	121	0	0
ENET3	0	0	0	0	12490	121	0	0
ENET4	0	0	0	0	12490	121	0	0
wl0	0	0	0	0	0	0	0	0

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

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.



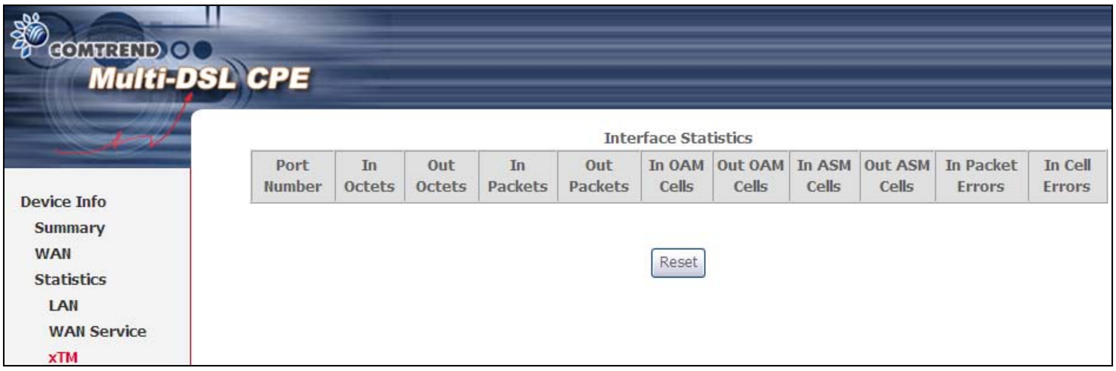
Statistics -- WAN

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

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

4.2.3 xTM Statistics

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



Interface Statistics

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

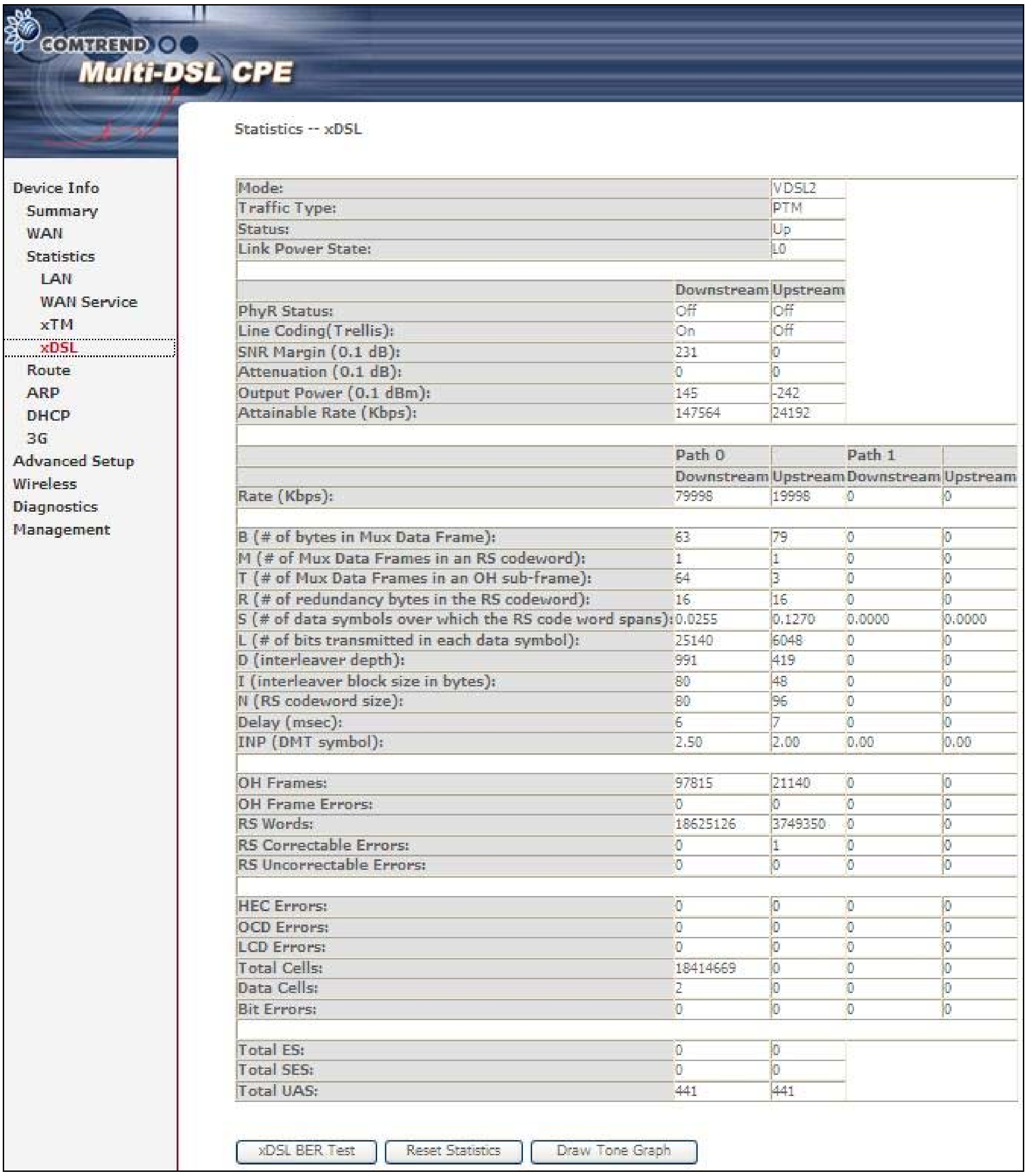
ATM Interface Statistics

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

4.2.4 xDSL Statistics

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

VDSL



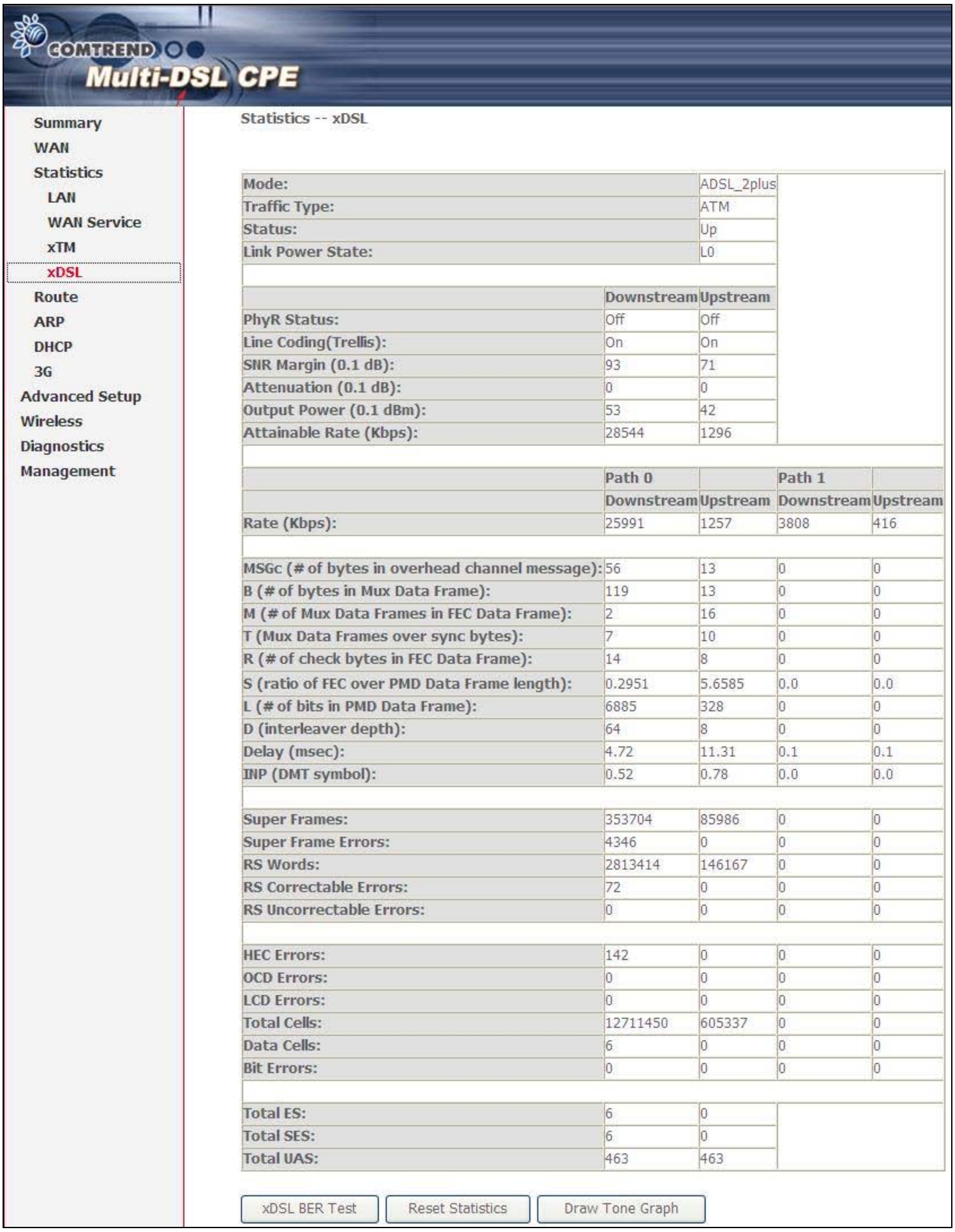
Statistics -- xDSL

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):	231	0
Attenuation (0.1 dB):	0	0
Output Power (0.1 dBm):	145	-242
Attainable Rate (Kbps):	147564	24192

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	79998	19998	0	0
B (# of bytes in Mux Data Frame):	63	79	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	64	3	0	0
R (# of redundancy bytes in the RS codeword):	16	16	0	0
S (# of data symbols over which the RS code word spans):	0.0255	0.1270	0.0000	0.0000
L (# of bits transmitted in each data symbol):	25140	6048	0	0
D (interleaver depth):	991	419	0	0
I (interleaver block size in bytes):	80	48	0	0
N (RS codeword size):	80	96	0	0
Delay (msec):	6	7	0	0
INP (DMT symbol):	2.50	2.00	0.00	0.00
OH Frames:	97815	21140	0	0
OH Frame Errors:	0	0	0	0
RS Words:	18625126	3749350	0	0
RS Correctable Errors:	0	1	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:	18414669	0	0	0
Data Cells:	2	0	0	0
Bit Errors:	0	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	441	441		

ADSL



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):	93	71		
Attenuation (0.1 dB):	0	0		
Output Power (0.1 dBm):	53	42		
Attainable Rate (Kbps):	28544	1296		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	25991	1257	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):	0.2951	5.6585	0.0	0.0
L (# of bits in PMD Data Frame):	6885	328	0	0
D (interleaver depth):	64	8	0	0
Delay (msec):	4.72	11.31	0.1	0.1
INP (DMT symbol):	0.52	0.78	0.0	0.0
Super Frames:	353704	85986	0	0
Super Frame Errors:	4346	0	0	0
RS Words:	2813414	146167	0	0
RS Correctable Errors:	72	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	142	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	12711450	605337	0	0
Data Cells:	6	0	0	0
Bit Errors:	0	0	0	0
Total ES:	6	0		
Total SES:	6	0		
Total UAS:	463	463		

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

Field	**Description**
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2
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)

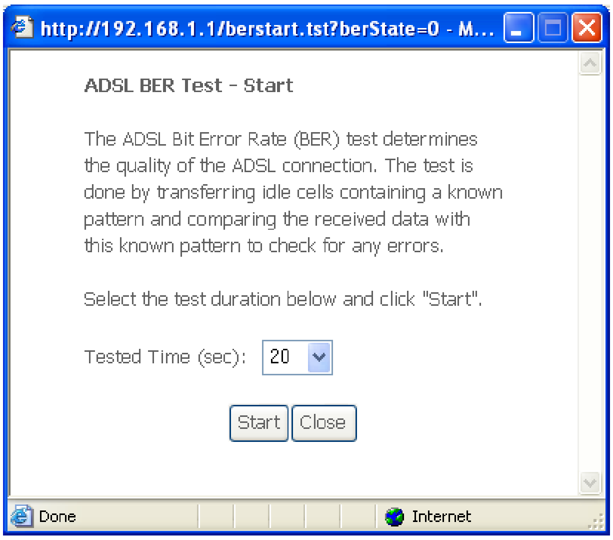
OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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

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

xDSL BER TEST

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



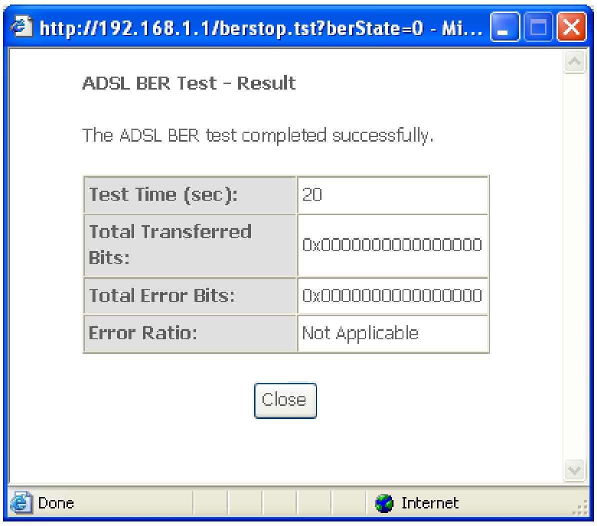
ADSL BER Test - Start

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

Select the test duration below and click "Start".

Tested Time (sec): 20

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



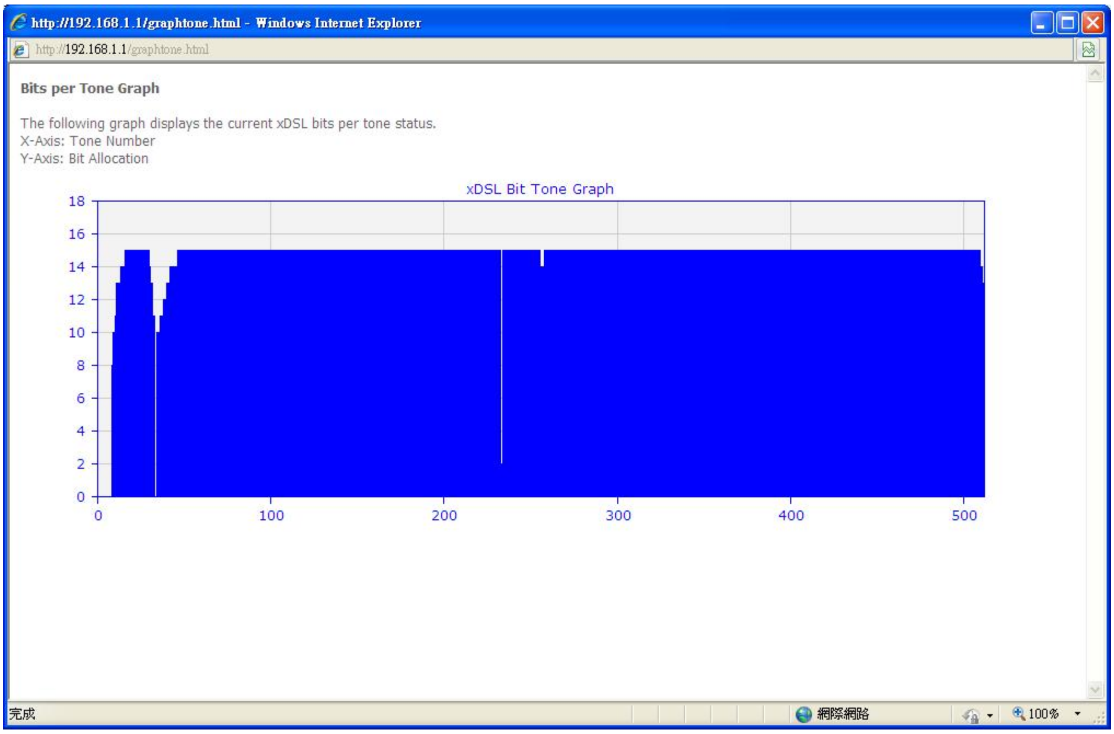
ADSL BER Test - Result

The ADSL BER test completed successfully.

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

xDSL TONE GRAPH

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

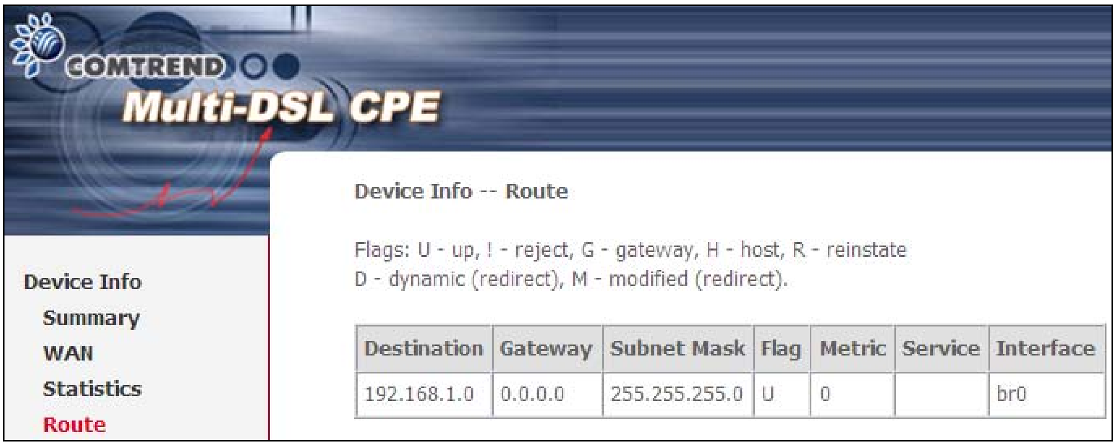

http://192.168.1.1/graphtone.html - Windows Internet Explorer
http://192.168.1.1/graphtone.html
xDSL Bit Tone Graph
18
16
14
12
10
8
6
4
2
0
0
100
200
300
400
500
完成
網際網路
100%

Bits per Tone Graph

The following graph displays the current xDSL bits per tone status.
X-Axis: Tone Number
Y-Axis: Bit Allocation

4.3 Route

Choose **Route** to display the routes that the CT-5374 has found.



Device Info -- Route

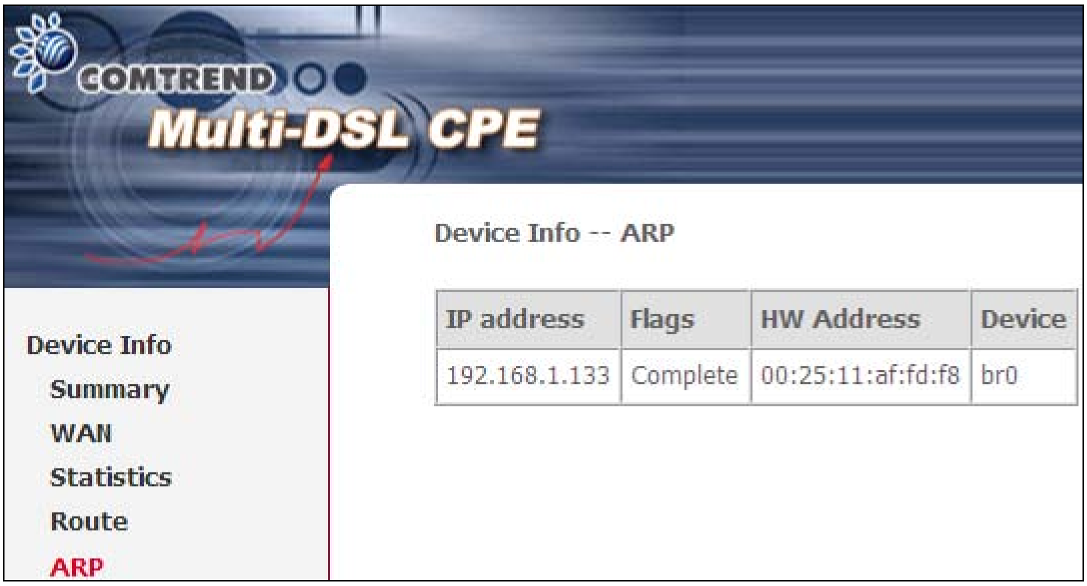
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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.



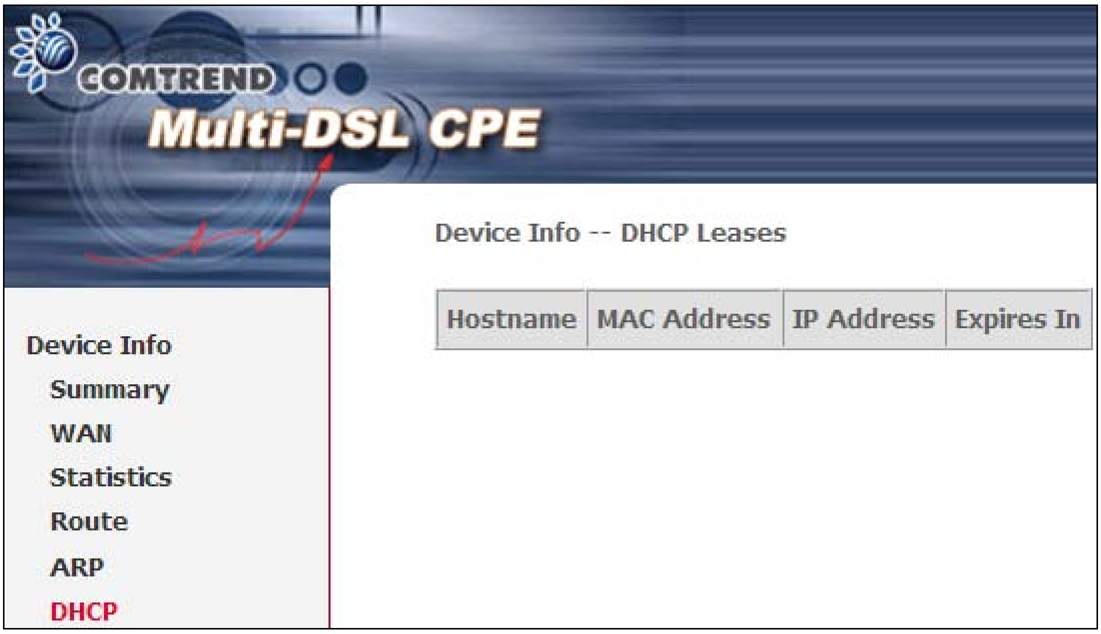
Device Info -- ARP

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

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

4.5 DHCP

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



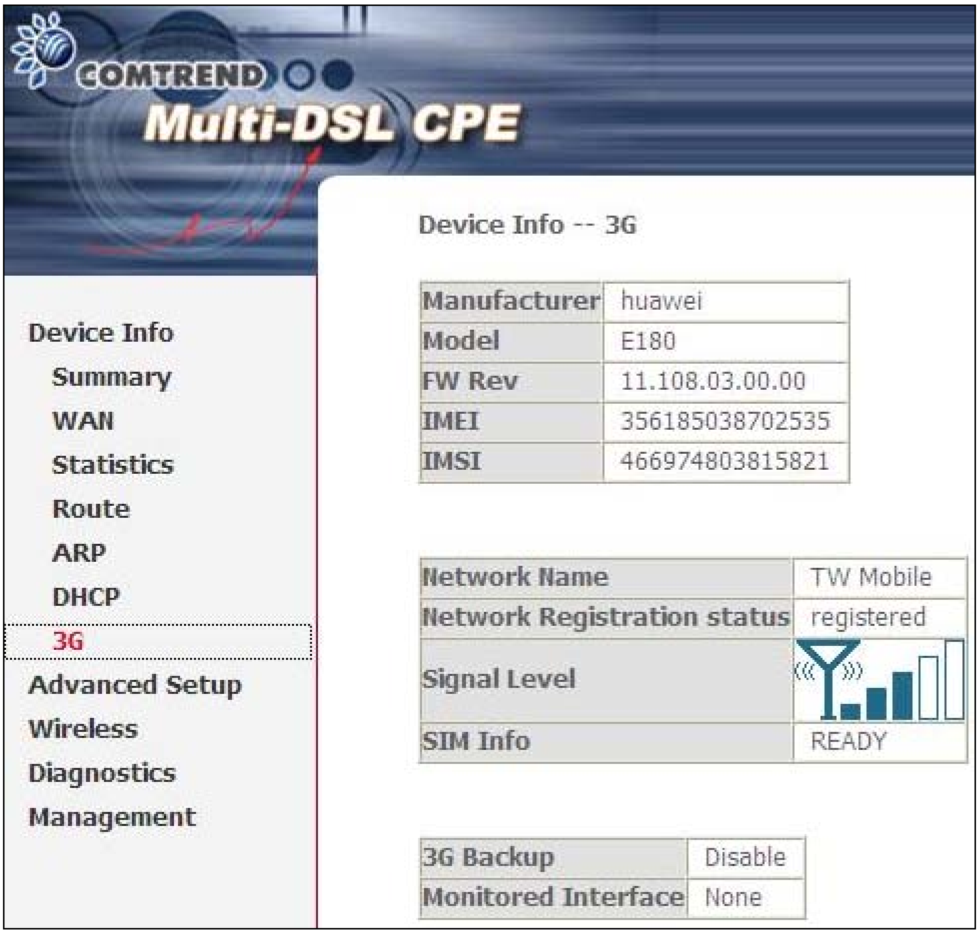
Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

Field	**Description**
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 3G

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



Device Info -- 3G

Manufacturer	huawei
Model	E180
FW Rev	11.108.03.00.00
IMEI	356185038702535
IMSI	466974803815821

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

3G Backup	Disable
Monitored Interface	None

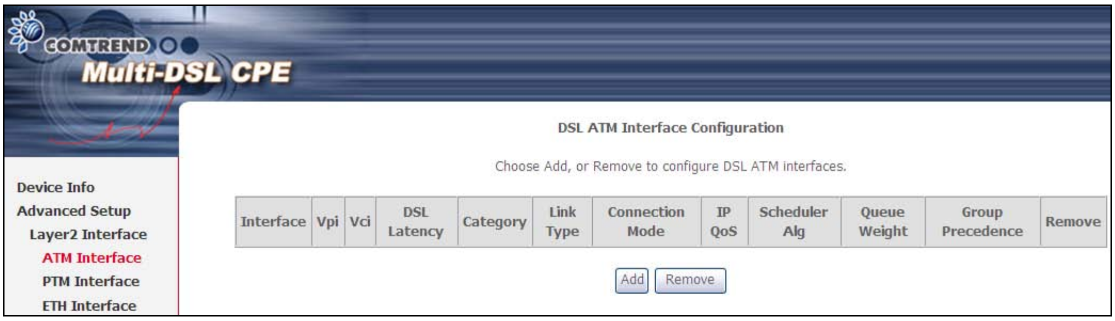
Chapter 5 Advanced Setup

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.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

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

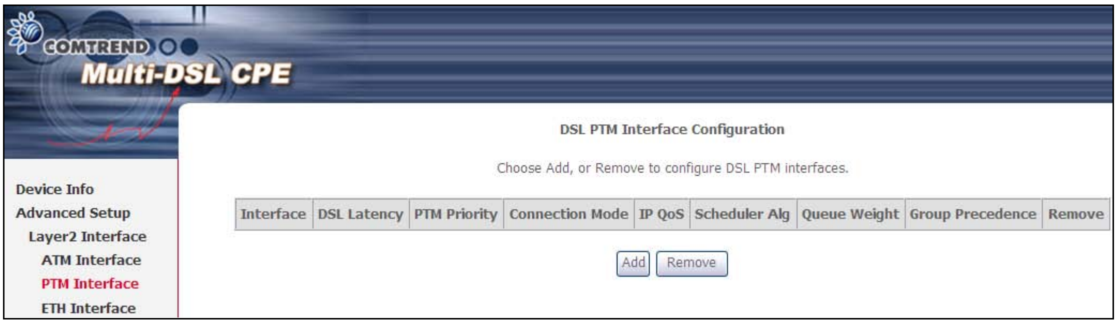
Field	Description
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
IP QoS	Quality of Service (QoS) status
Scheduler Alg	The algorithm used to schedule the dequeue behavior.
Queue Weight	The weight of the specified queue.
Group Precedence	The Precedence of the specified group.
Remove	Select items for removal

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.



DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

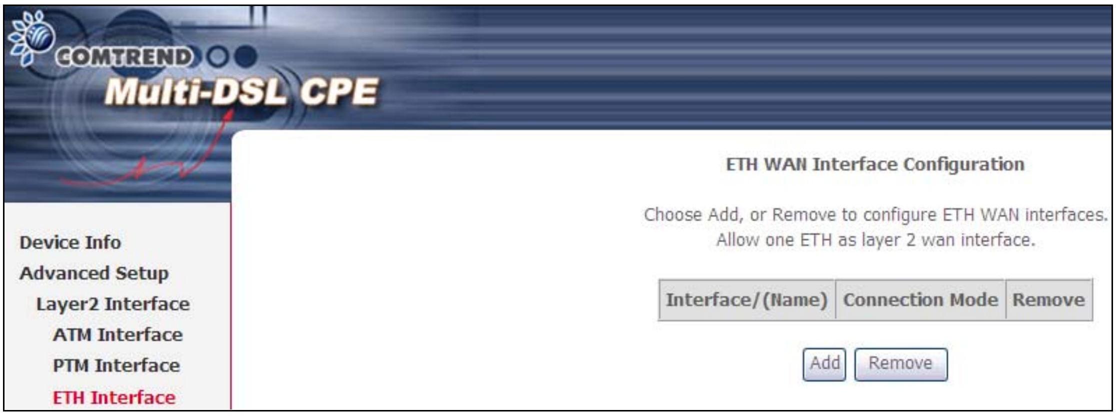
Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

Click **Add** to create a new connection (see Appendix G - Connection Setup). 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.



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

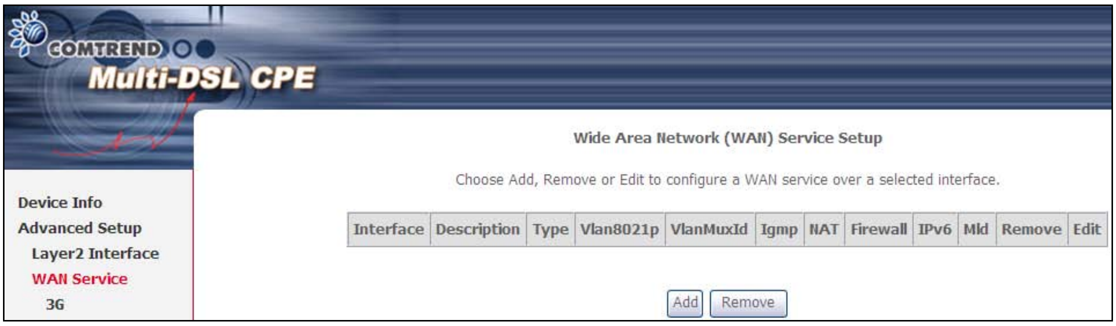
Click **Add** to create a new connection (see Appendix G - Connection Setup).

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 Service

This screen allows for the configuration of WAN interfaces.



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	IPv6	Mld	Remove	Edit

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

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

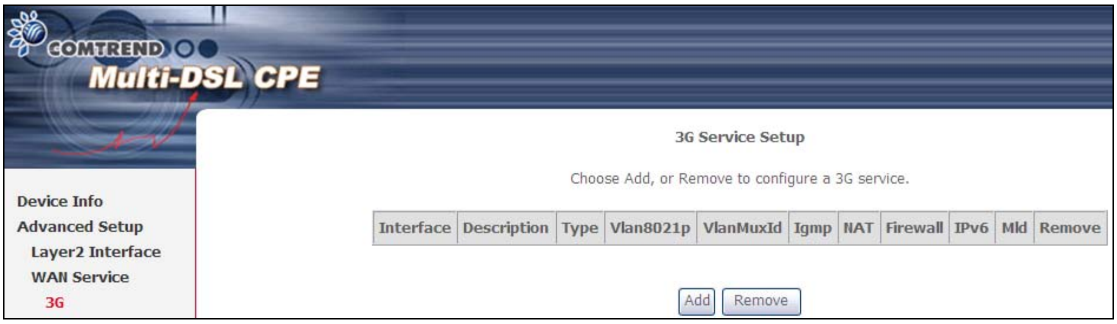
To remove a connection, select its Remove column radio button and click **Remove.**

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

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.



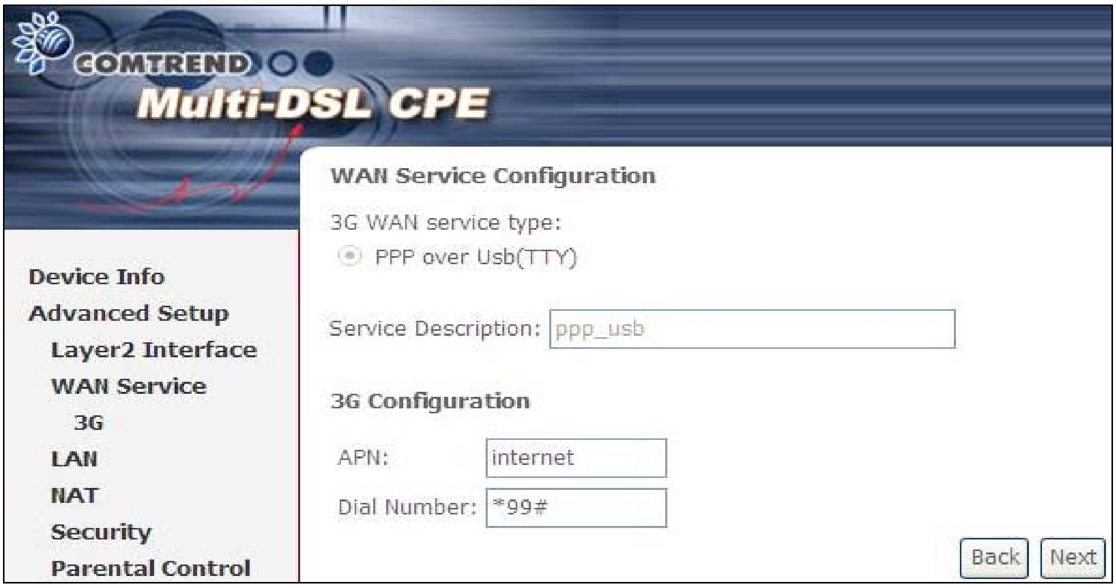
3G Service Setup

Choose Add, or Remove to configure a 3G service.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove

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

Click the **Add** button to create a new connection.
To remove a connection, select its Remove column radio button and click **Remove.**



WAN Service Configuration

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

Service Description: ppp_usb

3G Configuration

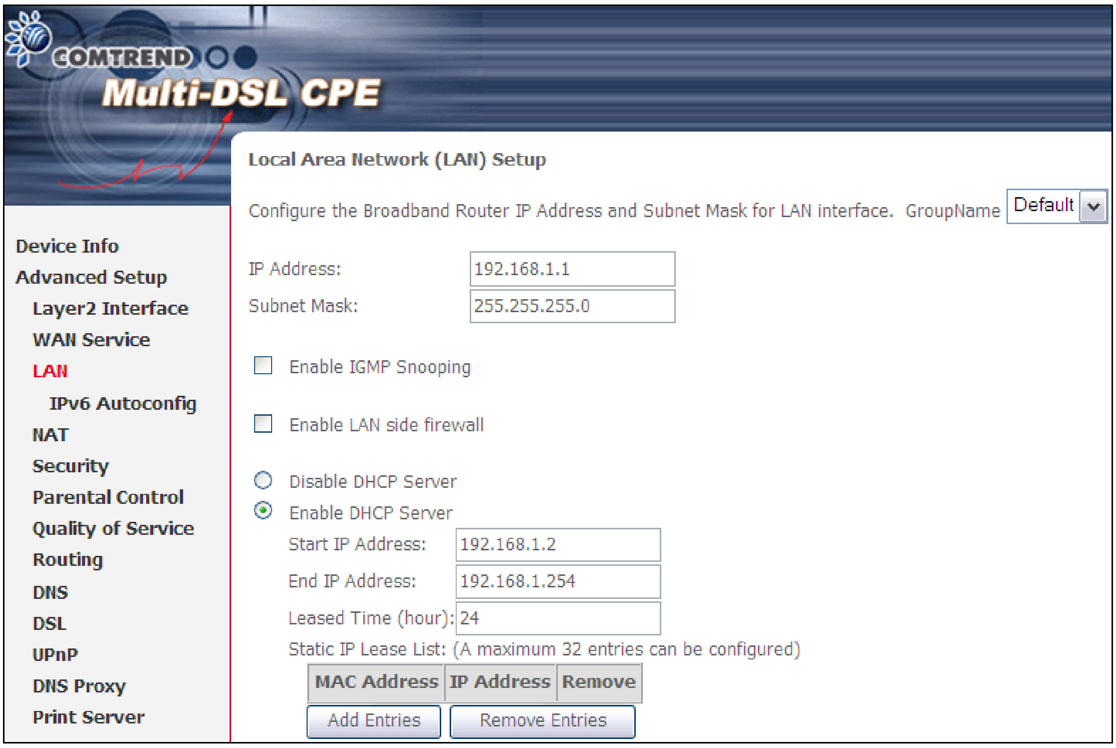
APN: internet

Dial Number: *99#

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

5.3 LAN

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



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

□ Enable IGMP Snooping

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

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

MAC Address	IP Address	Remove

Add Entries | Remove Entries

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

Enable IGMP Snooping: Enable by ticking the checkbox ☑.

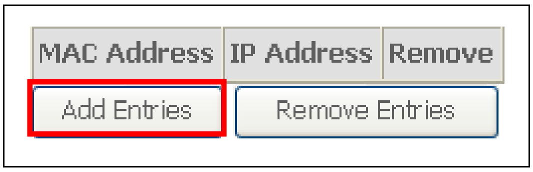
Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

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

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

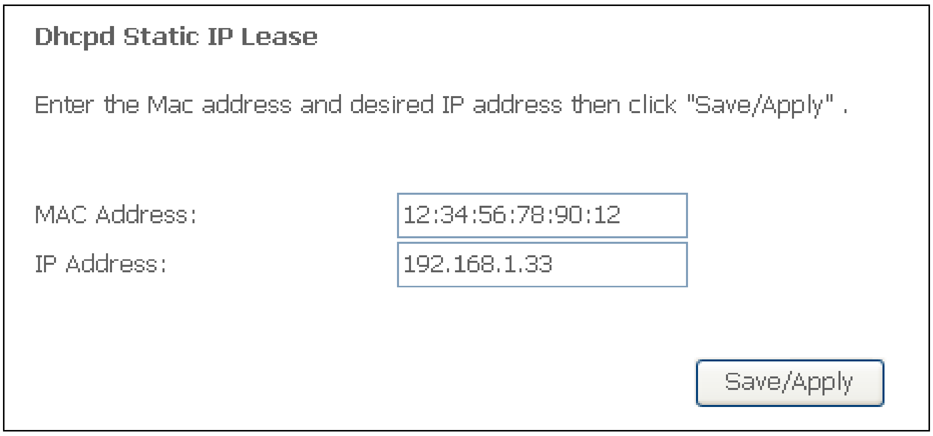
DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

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



MAC Address	IP Address	Remove

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



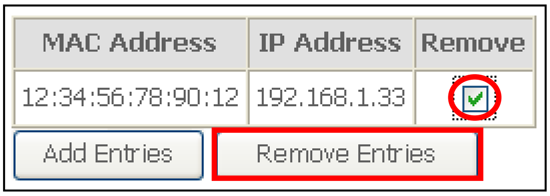
Dhcpd Static IP Lease

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

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

IP Address: 192.168.1.33

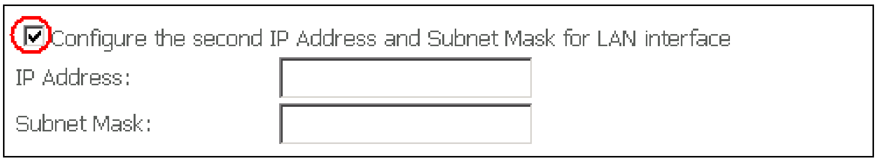
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



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

2ND LAN INTERFACE

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



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

IP Address:

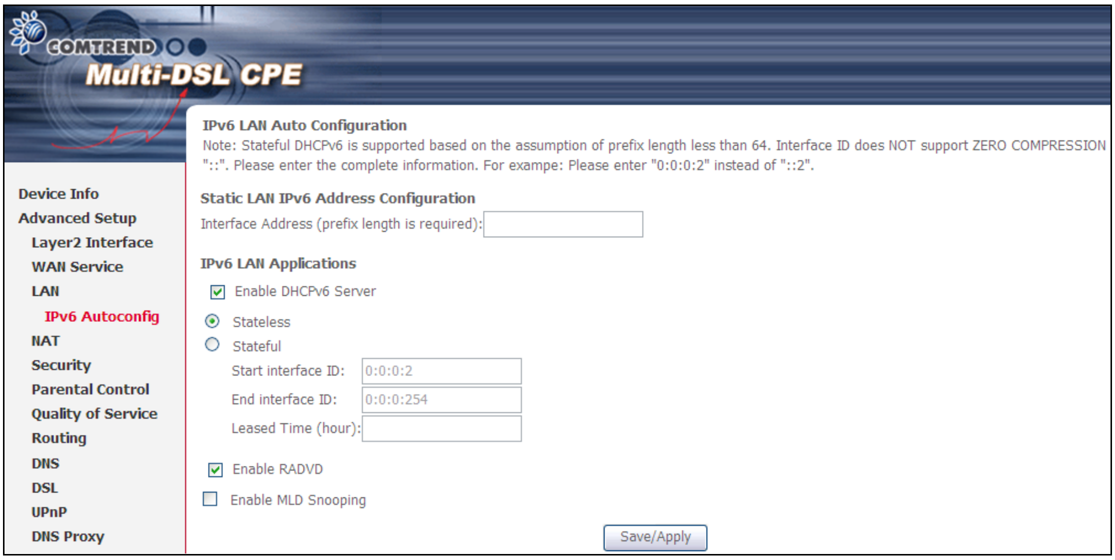
Subnet Mask:

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

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

5.4 IPv6 LAN Auto Configuration

Configure the IPv6 LAN Auto Configuration options (see below) and then click **Save / Apply**.



IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☑ Enable DHCPv6 Server

● Stateless

○ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour):

☑ Enable RADVD

□ Enable MLD Snooping

Static LAN IPv6 Address Configuration

Input the static LAN IPv6 address.

DHCPv6 Server: To enable DHCP for IPv6, select the **Enable DHCPv6 server** checkbox ☑. This setting enables the router to assign IP settings to every IPv6-capable LAN device (IPv6 clients).

RADVD: Select the checkbox ☑ to enable the **R**outer **ADV**ertisement **D**aemon. This provides information that IPv6 clients can use for autoconfiguration according to the Neighbour Discovery for IPv6 protocol (RFC2461).

Enable MLD Snooping: Enable by ticking the checkbox ☑.

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

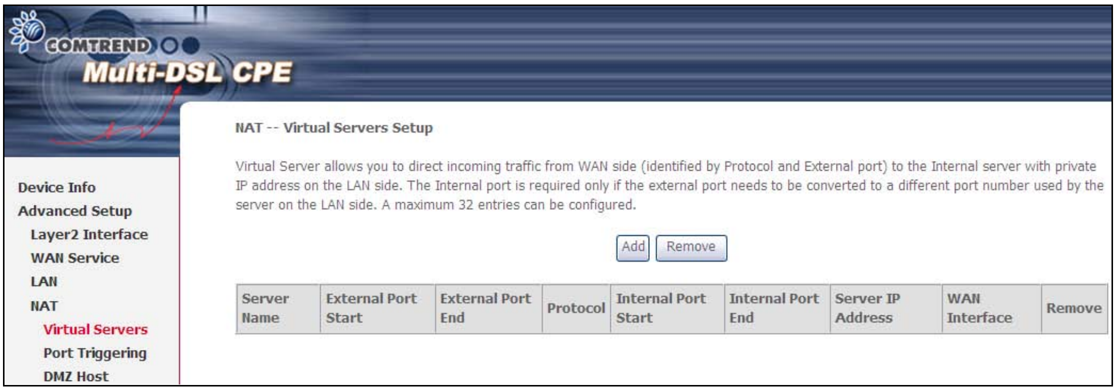
Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

5.5 NAT

To display this option, NAT must be enabled in at least one PVC shown on the Chapter 5 Advanced Setup - . *NAT is not an available option in Bridge mode*.

5.5.1 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.

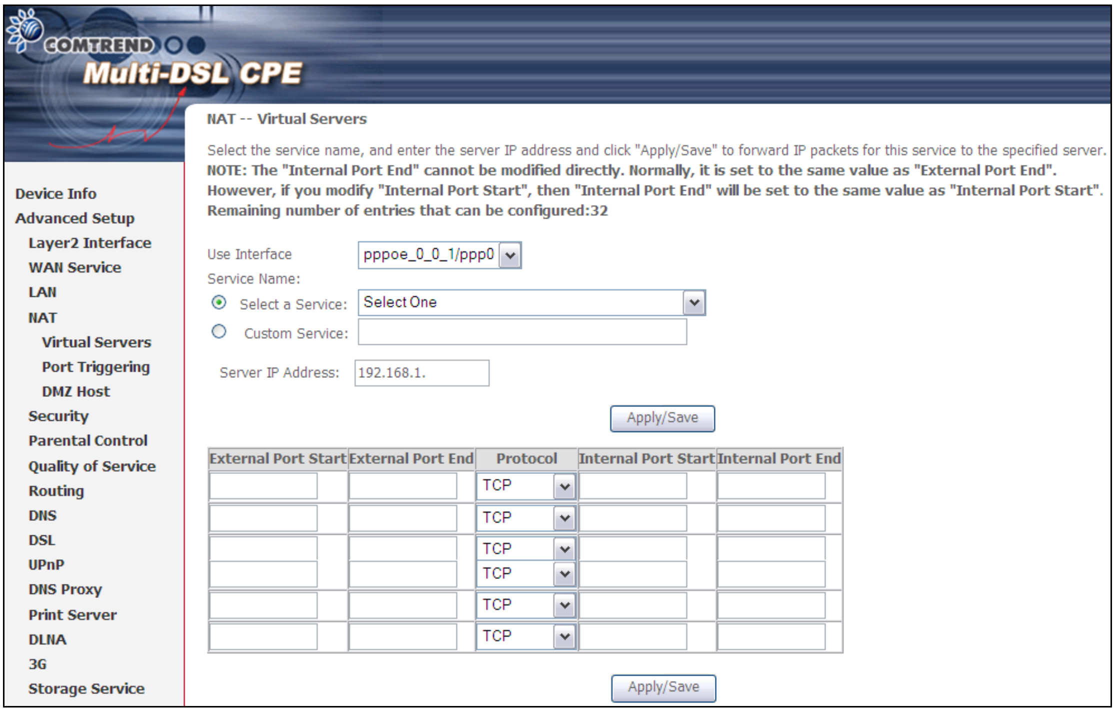


NAT -- Virtual Servers Setup

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	Remove

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured:32

Use Interface pppoe_0_0_1/ppp0

Service Name:

● Select a Service: Select One

○ Custom Service:

Server IP Address: 192.168.1.

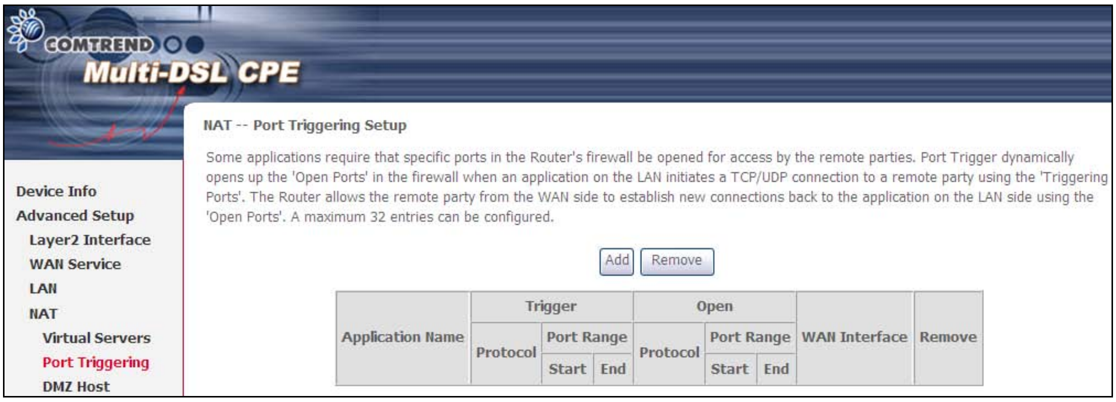
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Consult the table below for field and header descriptions.

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

5.5.2 Port Triggering

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

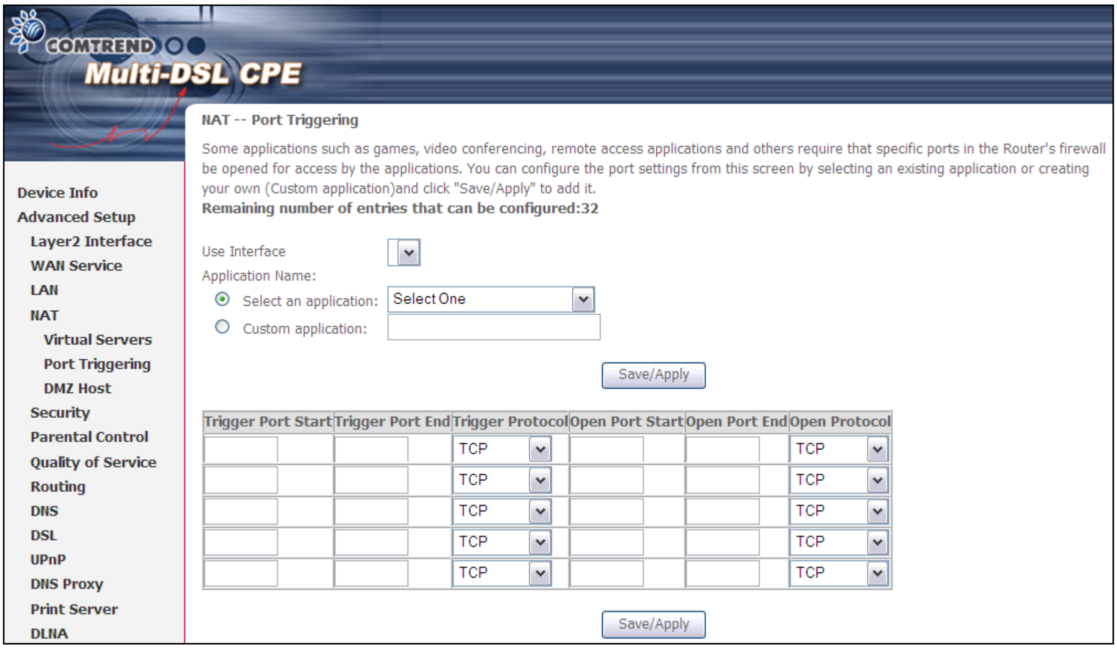


NAT -- Port Triggering Setup

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

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

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



NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Use Interface

Application Name:

● Select an application: Select One

○ Custom application:

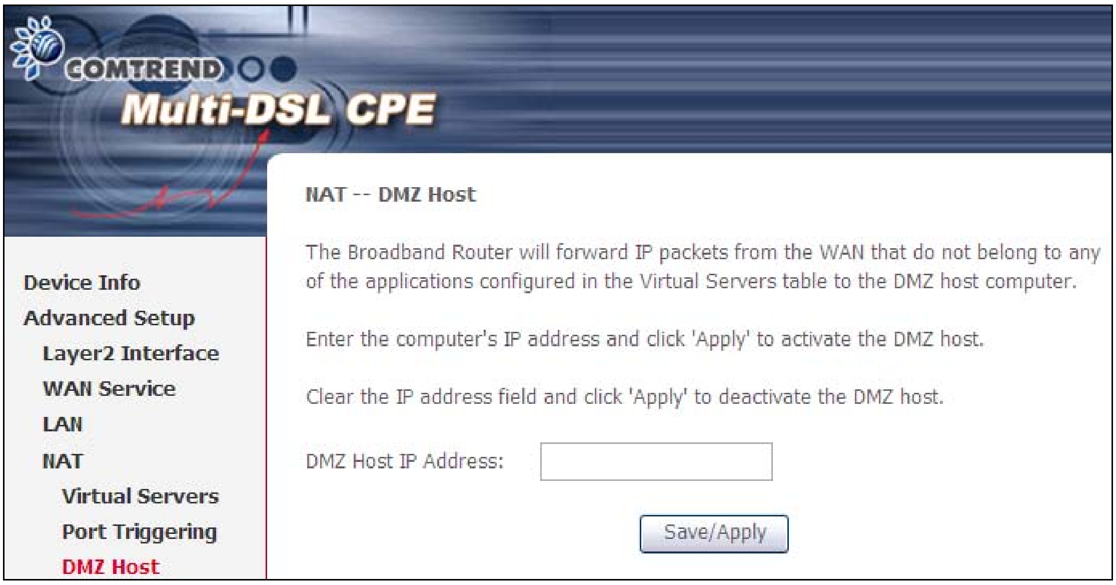
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

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.

5.5.3 DMZ Host

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



NAT -- DMZ Host

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

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

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

DMZ Host IP Address:

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**.

5.6 Security

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

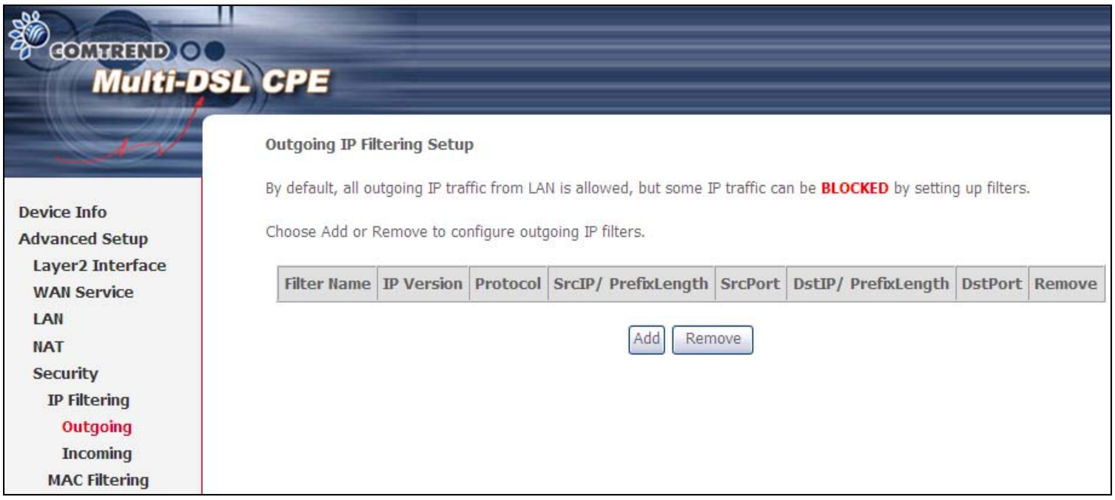
5.6.1 IP Filtering

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, 5.6.2 MAC Filtering performs a similar function.

OUTGOING IP FILTER

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



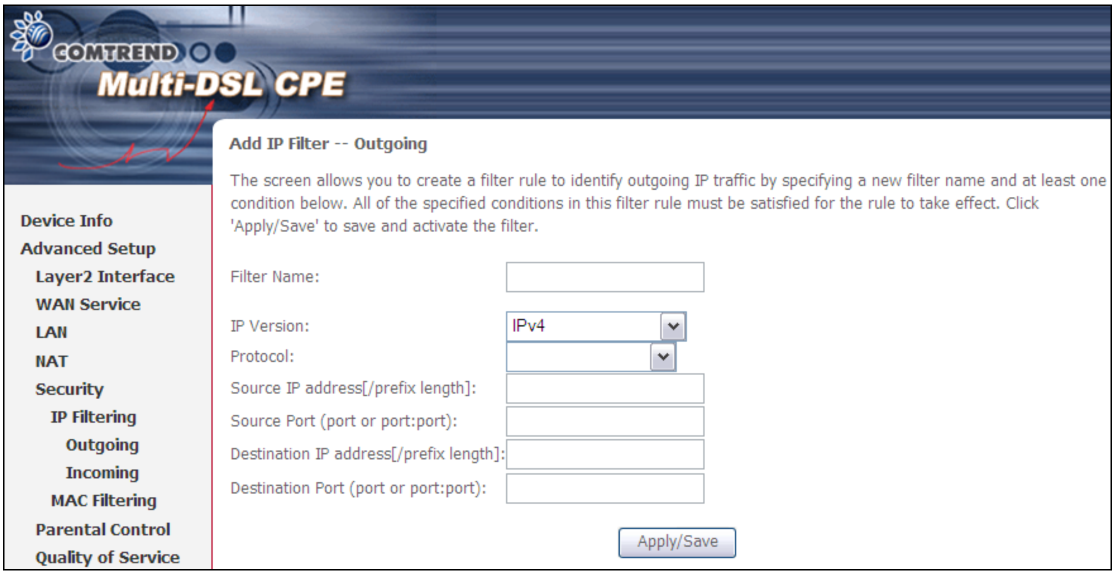
Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

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

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



Add IP Filter -- Outgoing

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

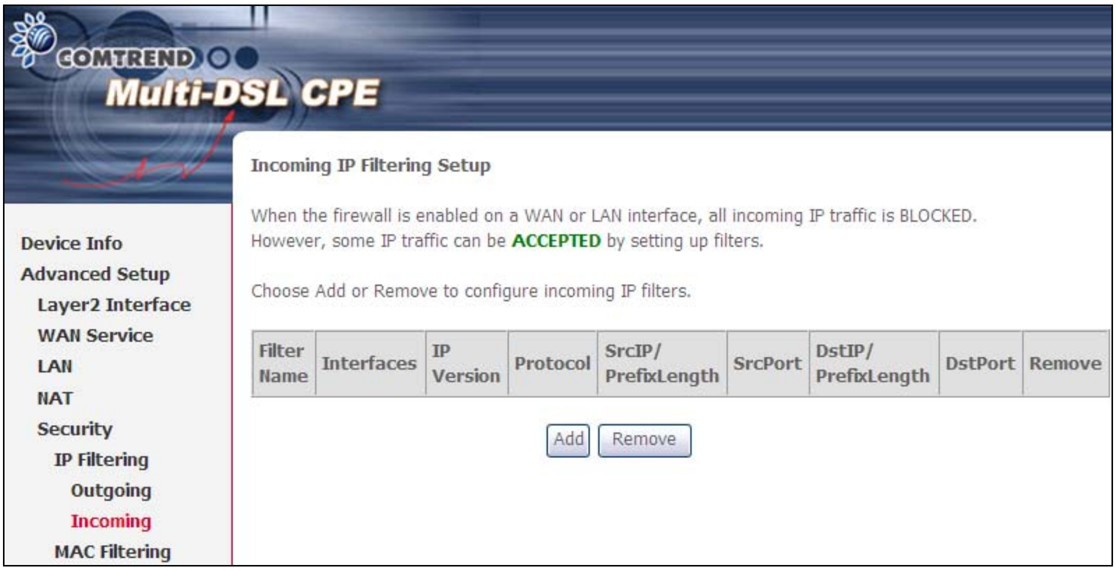
Filter Name:	
IP Version:	IPv4
Protocol:	
Source IP address[/prefix length]:	
Source Port (port or port:port):	
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

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



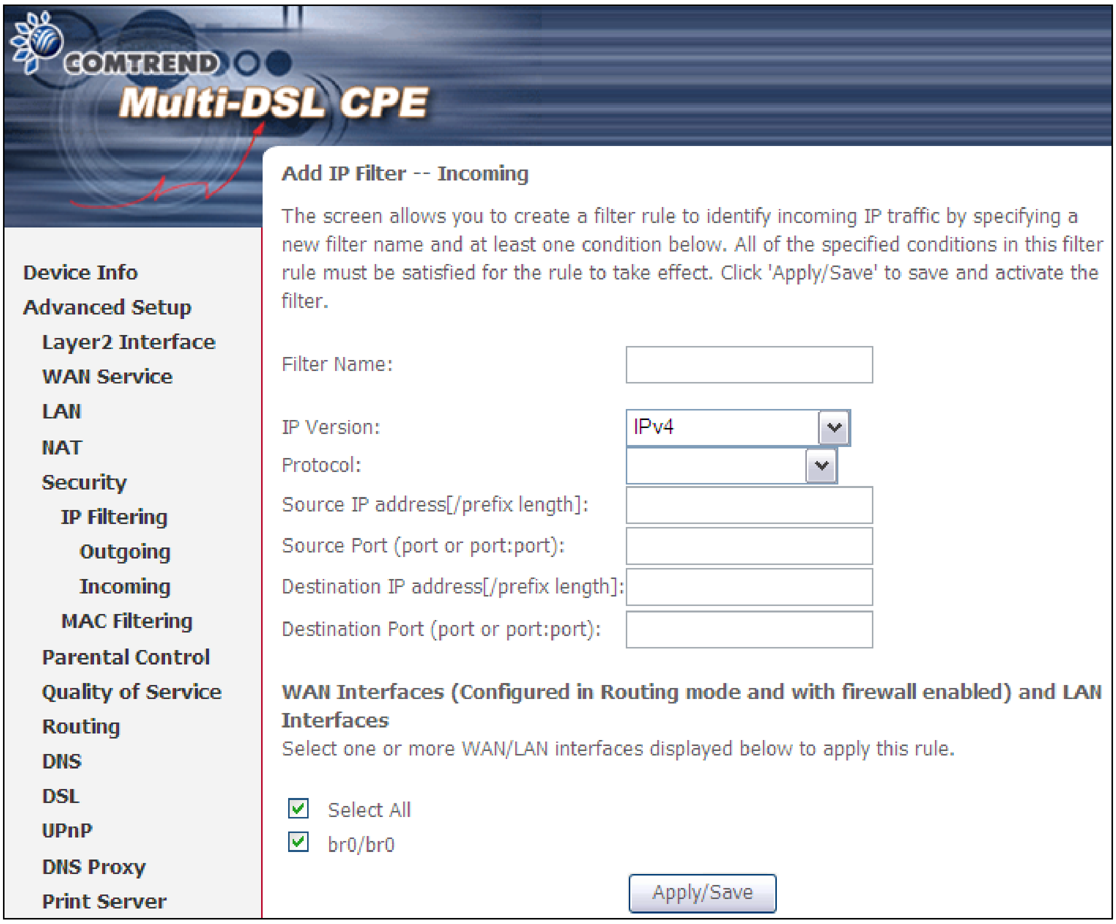
Incoming IP Filtering Setup

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

Choose Add or Remove to configure incoming IP filters.

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

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



Add IP Filter -- Incoming

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

Filter Name:

IP Version: IPv4

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All

☑ br0/br0

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
IP Version	IPv4 selected by default.
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.

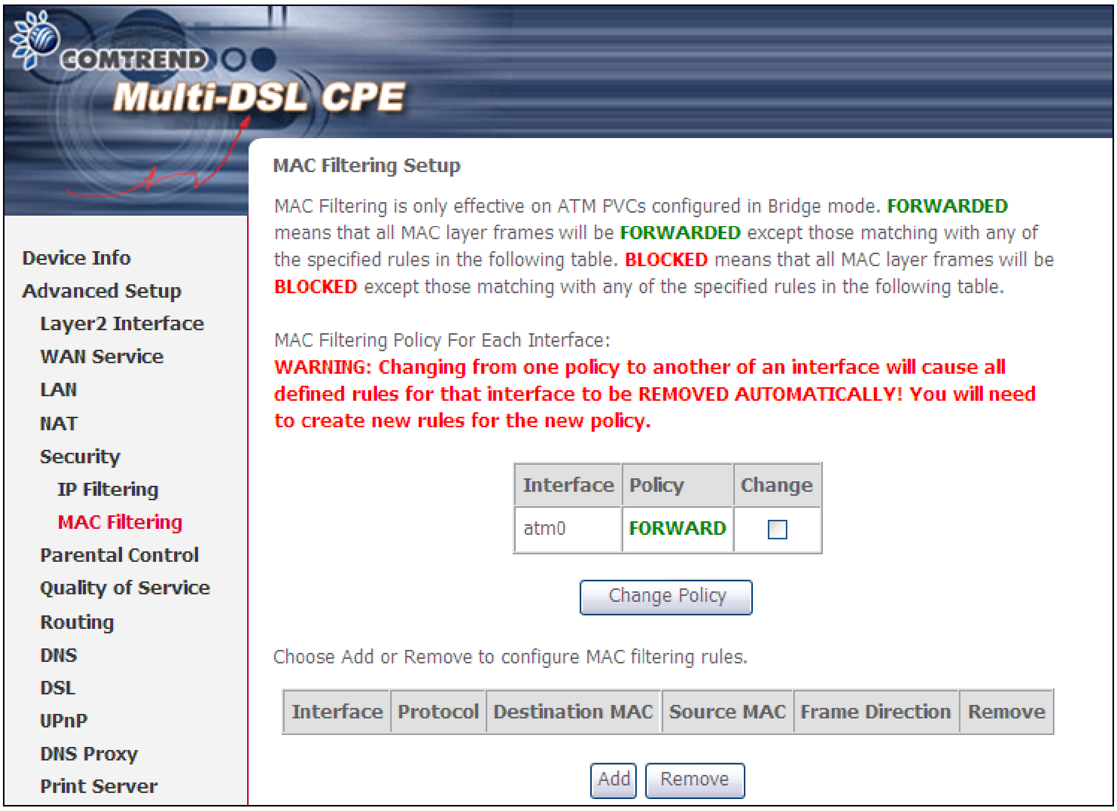
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

5.6.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use 5.6.1 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 CT-5374 can be set according to the following procedure.

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



MAC Filtering Setup

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

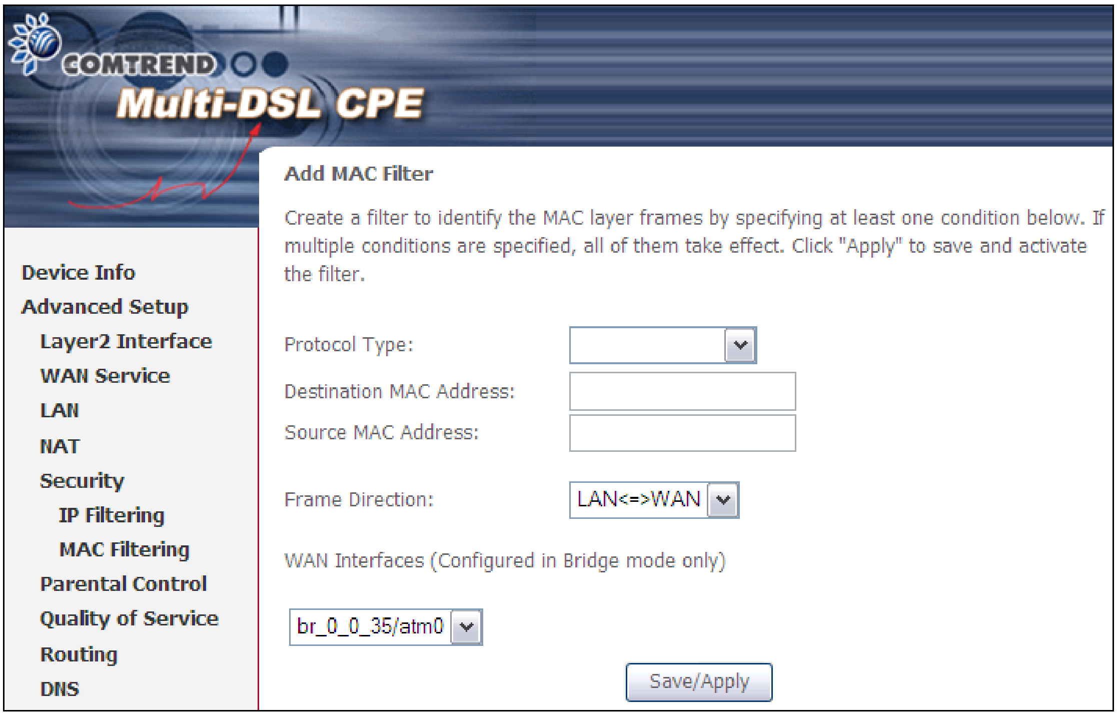
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm0	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

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



Add MAC Filter

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_35/atm0

Consult the table below for detailed field descriptions.

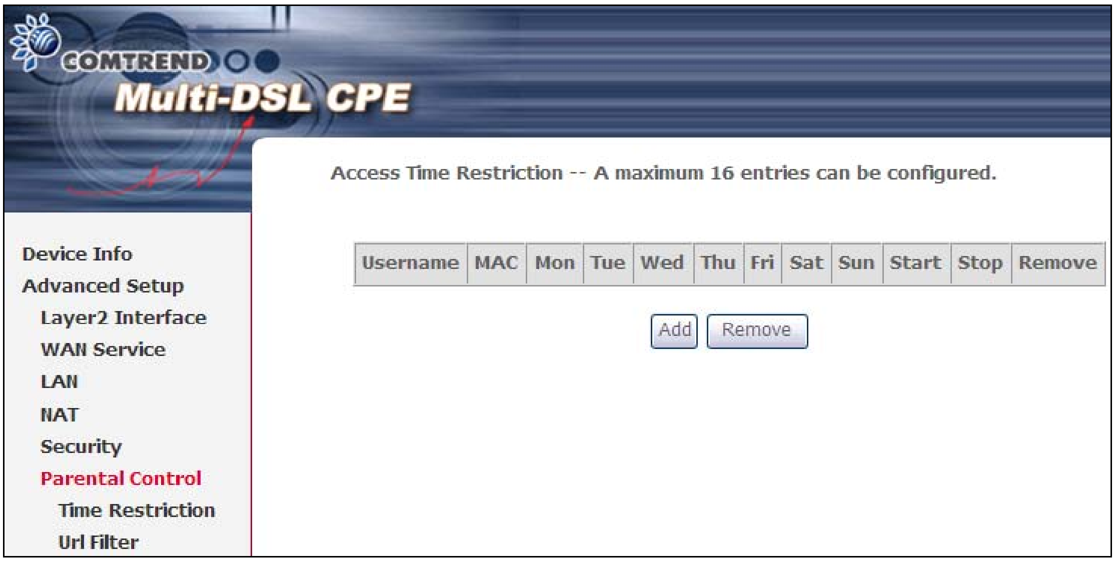
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

5.7 Parental Control

This selection provides WAN access control functionality.

5.7.1 Time Restriction

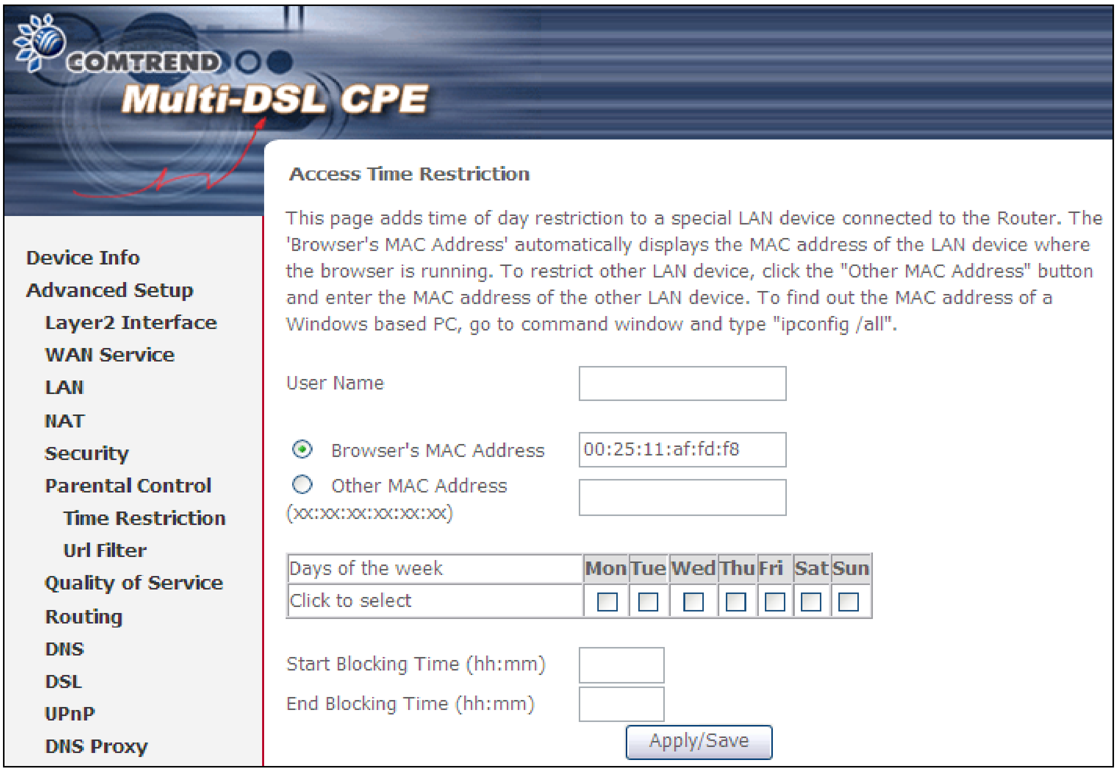
This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in 8.5 Internet Time, so that the scheduled times match your local time.



Access Time Restriction -- A maximum 16 entries can be configured.

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

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



Access Time Restriction

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

User Name

● Browser's MAC Address 00:25:11:af:fd:f8

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

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

Start Blocking Time (hh:mm)

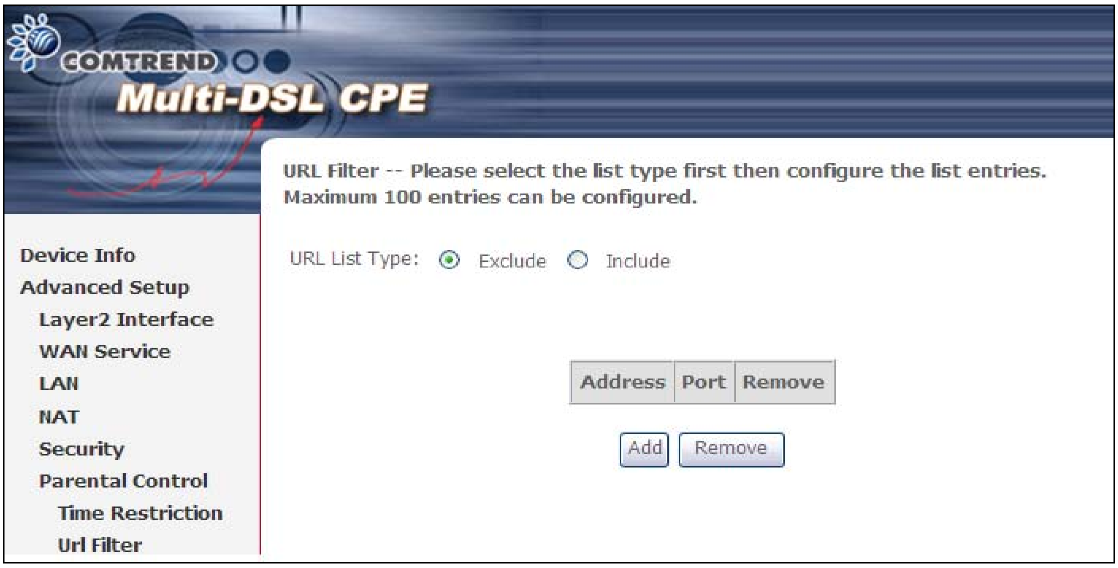
End Blocking Time (hh:mm)

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

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

5.7.2 URL Filter

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

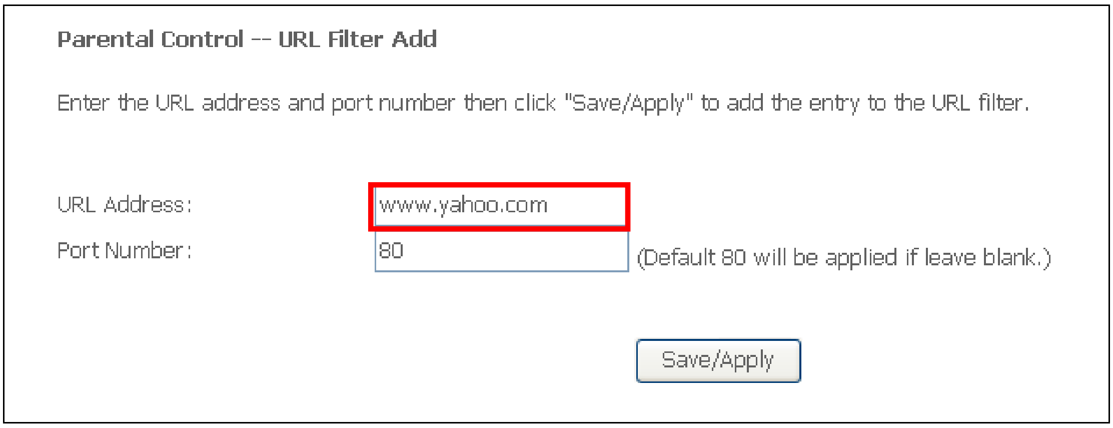


URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ● Exclude ○ Include

Address	Port	Remove

Select URL List Type, and Click **Add** to display the following screen.



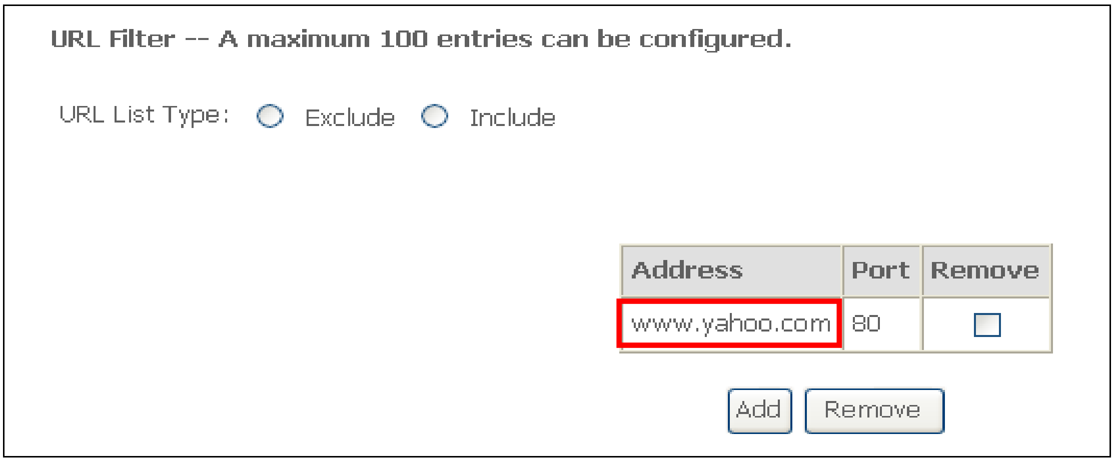
Parental Control -- URL Filter Add

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

URL Address: www.yahoo.com

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

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



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

URL List Type: ○ Exclude ○ Include

Address	Port	Remove
www.yahoo.com	80	□

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

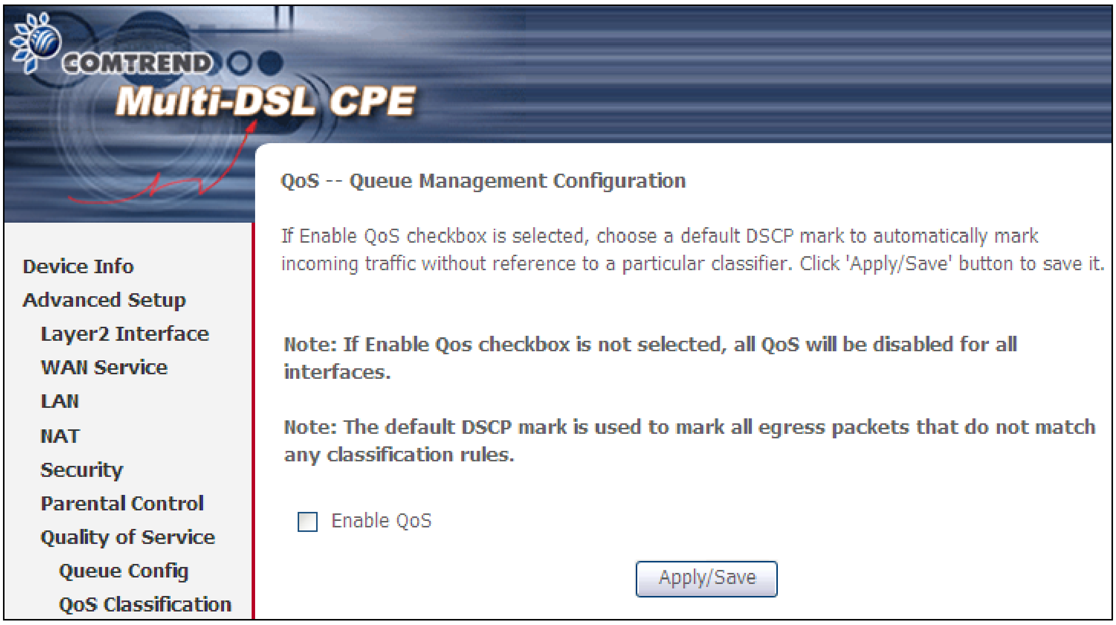
5.8 Quality of Service (QoS)

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

5.8.1 Queue Management Configuration

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

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



QoS -- Queue Management Configuration

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

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

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

□ Enable QoS

Apply/Save

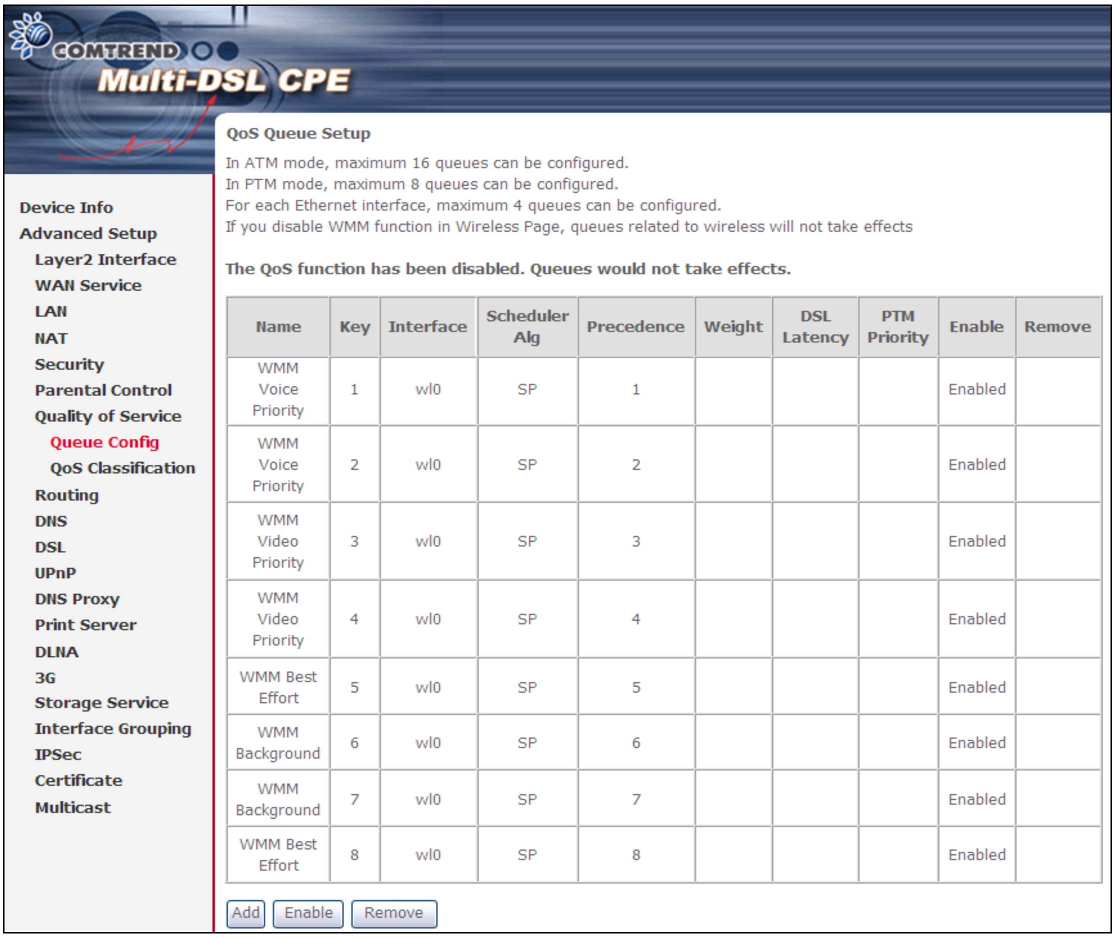
QoS and **DSCP Mark** are defined as follows:

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

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

5.8.2 Queue Configuration

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.



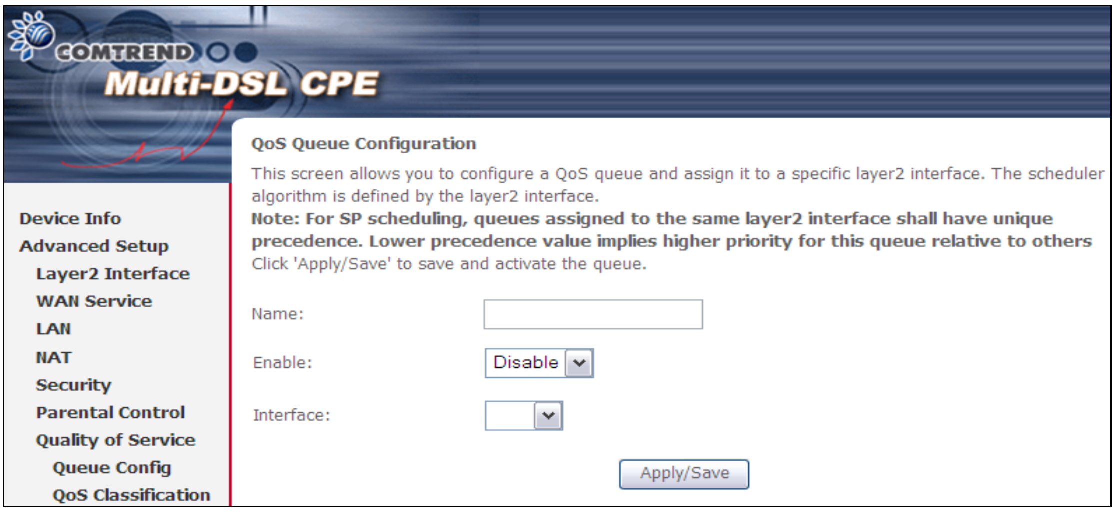
QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function 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	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	

Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.



QoS Queue Configuration

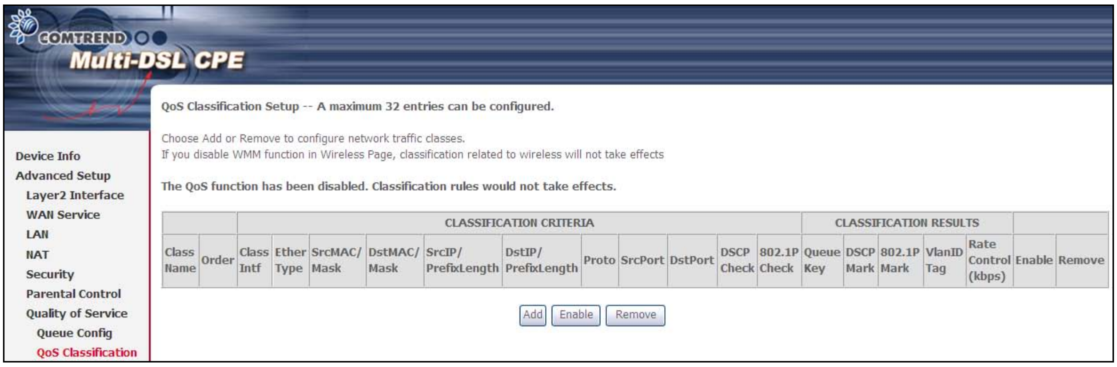
This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.
Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others
Click 'Apply/Save' to save and activate the queue.

Name:	
Enable:	Disable
Interface:	

Name: Identifier for this Queue entry.
Enable: Enable/Disable the Queue entry.
Interface: Assign the entry to a specific network interface (QoS enabled).

5.8.3 QoS Classification

The network traffic classes are listed in the following table.



QoS Classification Setup -- A maximum 32 entries can be configured.

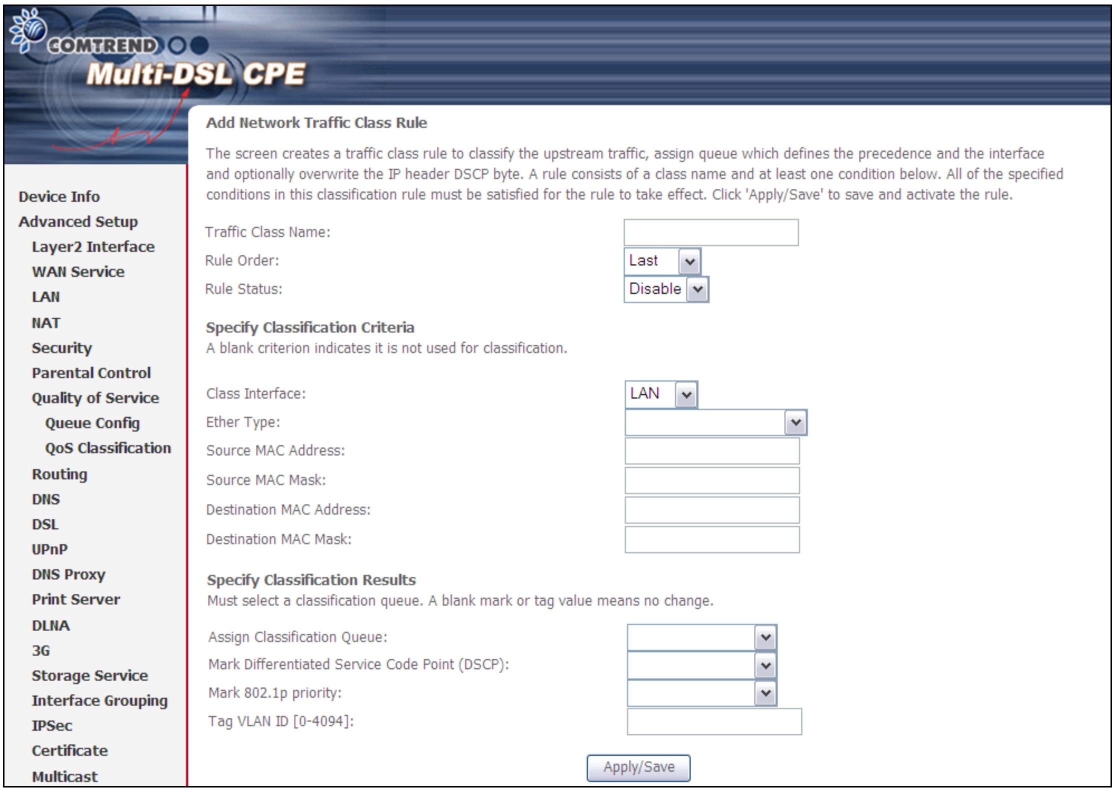
Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS							
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove

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

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



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:	
Rule Order:	Last
Rule Status:	Disable

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

Class Interface:	LAN
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID [0-4094]:	

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.

Field	Description
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece P&Queue Q" where P and Q are the Precedence and Queue Key values for the corresponding Interface as listed on the Queue Config screen.
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.
Tag VLAN ID	Enter a 802.1Q VLAN ID tag [2-4094]

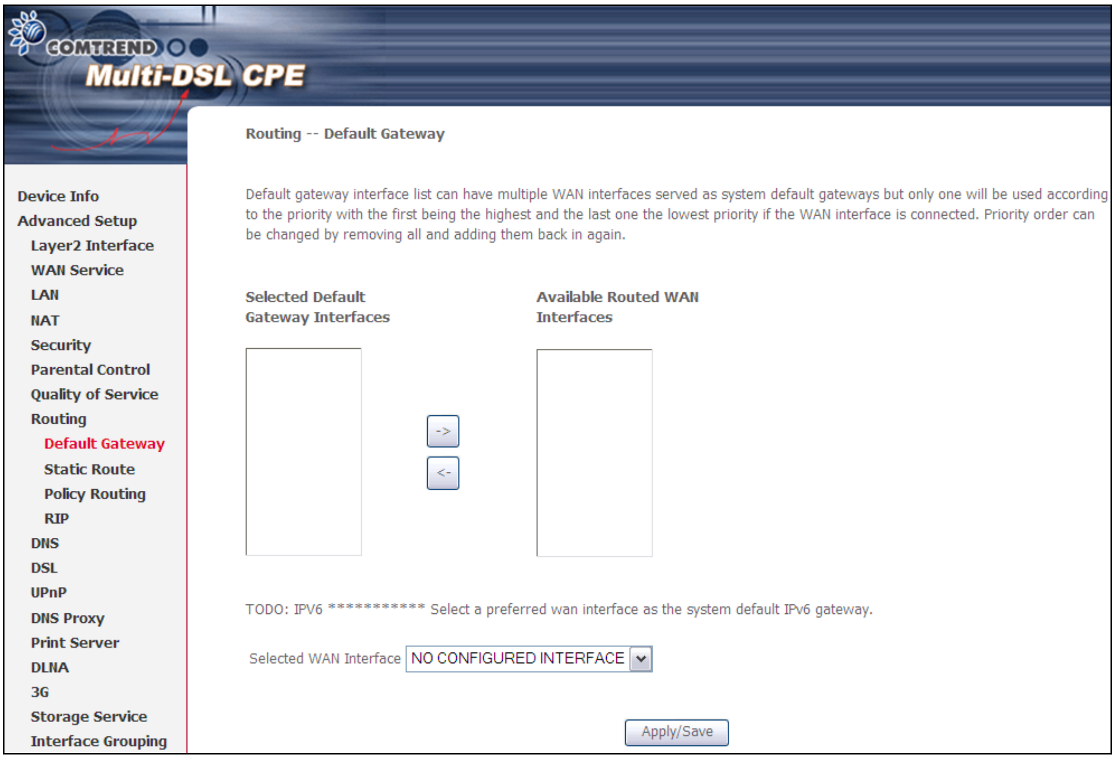
5.9 Routing

This 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.

5.9.1 Default Gateway

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



Routing -- Default Gateway

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

Selected Default Gateway Interfaces

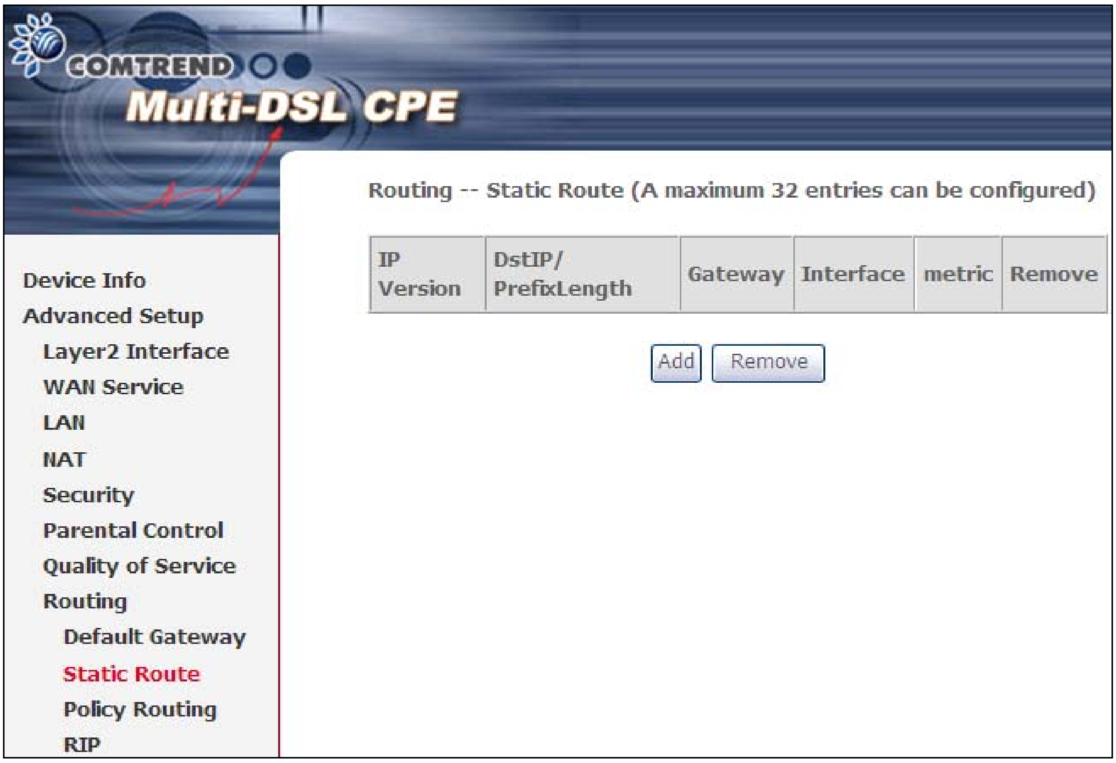
Available Routed WAN Interfaces

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

Selected WAN Interface NO CONFIGURED INTERFACE

5.9.2 Static Route

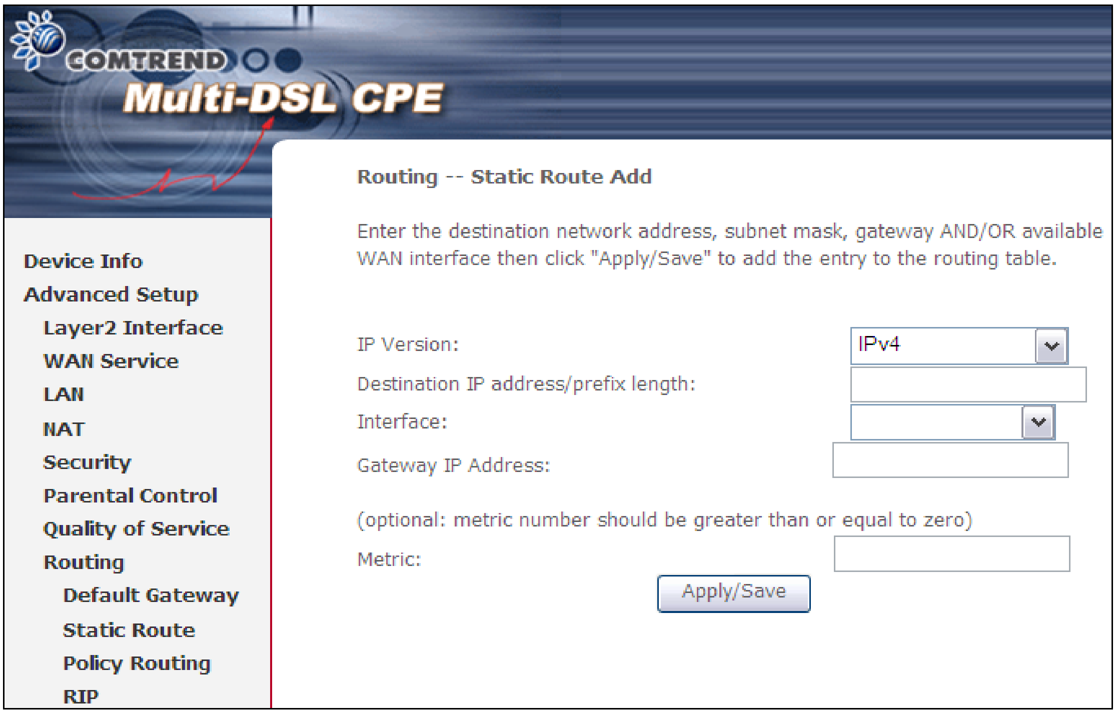
This option allows for the configuration of static routes by destination IP.
Click **Add** to create a static route or click **Remove** to delete a static route.



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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

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



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

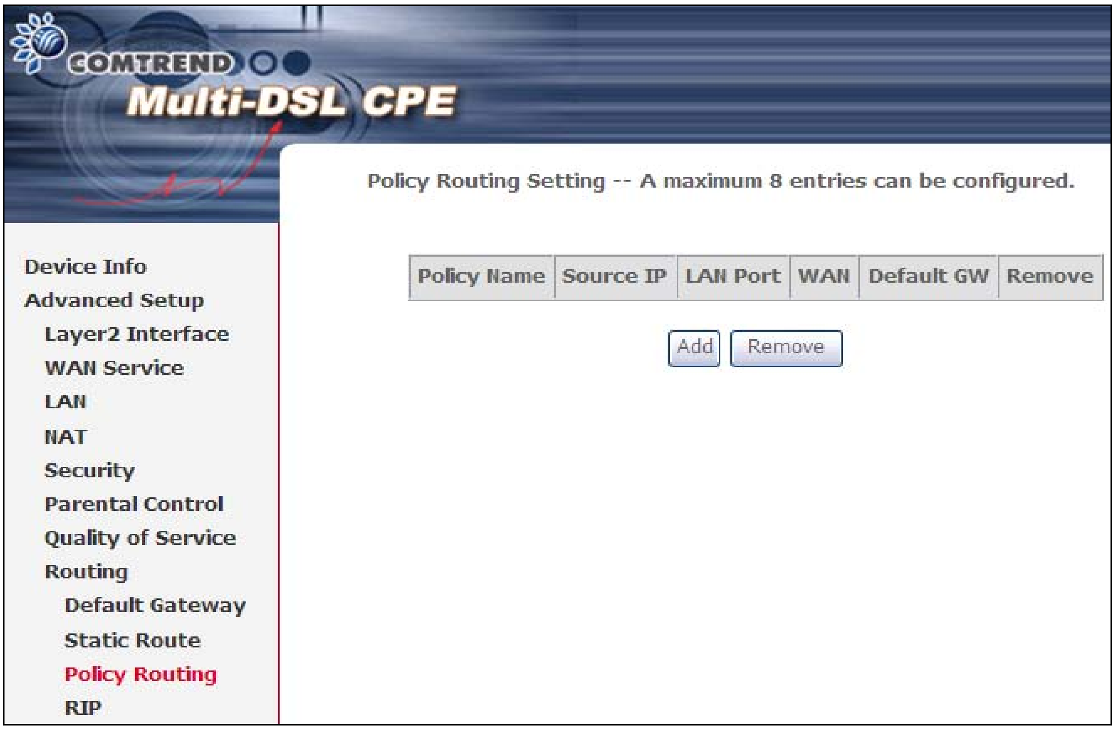
(optional: metric number should be greater than or equal to zero)

Metric:

Input the Destination IP Address, select the interface type, Input the Gateway IP, (and the Metric number if required). Then, click **Apply/Save** to add an entry to the routing table.

5.9.3 Policy Routing

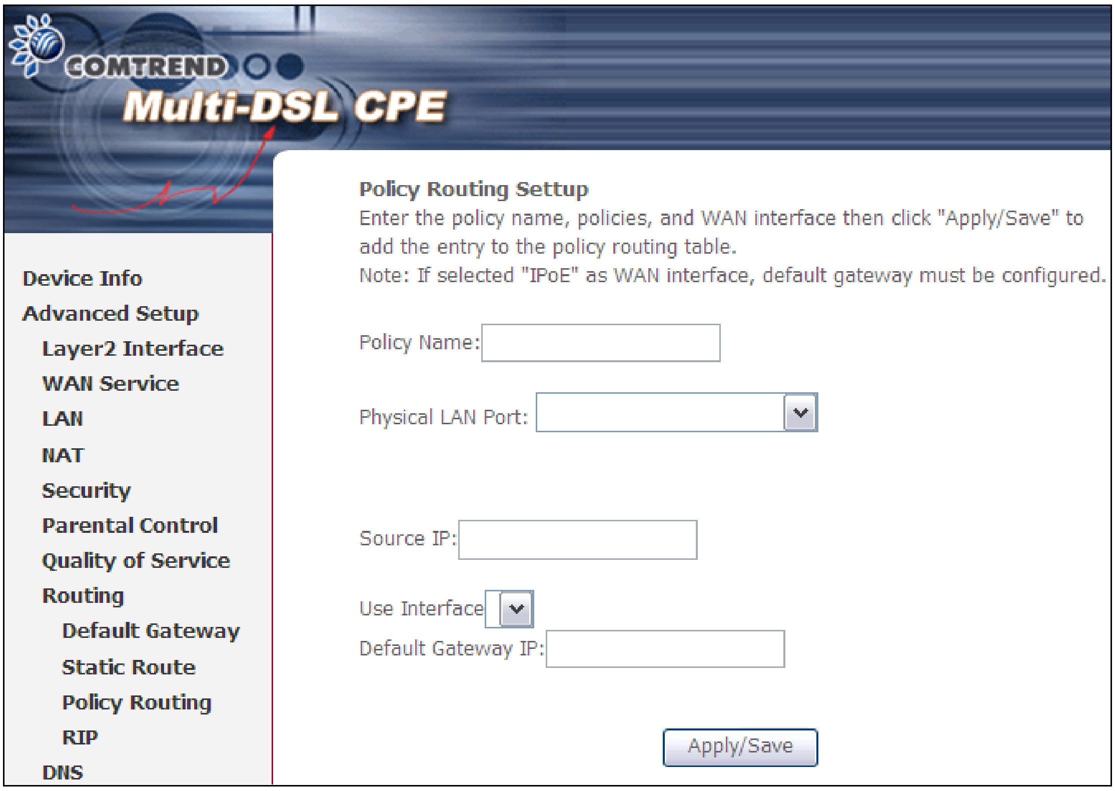
This page allows users configure the outgoing WAN interface (depending on source IP or LAN port).



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

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Click **Add** to create an entry or click **Remove** to delete an entry.



Policy Routing Settup

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:

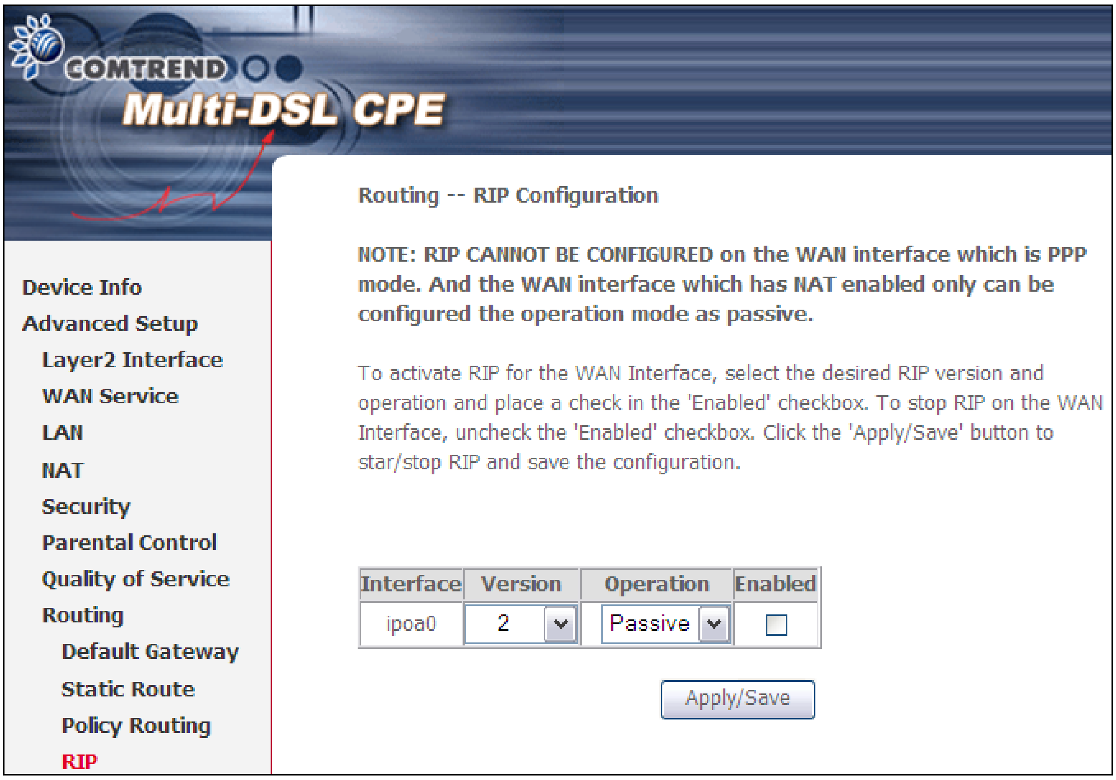
Use Interface

Default Gateway IP:

Input a Policy Name and select the Physical LAN Port. Then, input the Source IP, select which Interface to use and input the Default Gateway IP. Click **Apply/Save** to add the entry to the policy routing table.

5.9.4 RIP

To activate RIP, select the **Enabled** radio button for Global RIP Mode. To configure an individual interface (PVC), select the desired RIP Version and Operation, and then select the **Enabled** checkbox ☑ for that interface (PVC). Click **Save / Apply** to save the configuration and start/stop RIP (based on the Global RIP mode selected).



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.

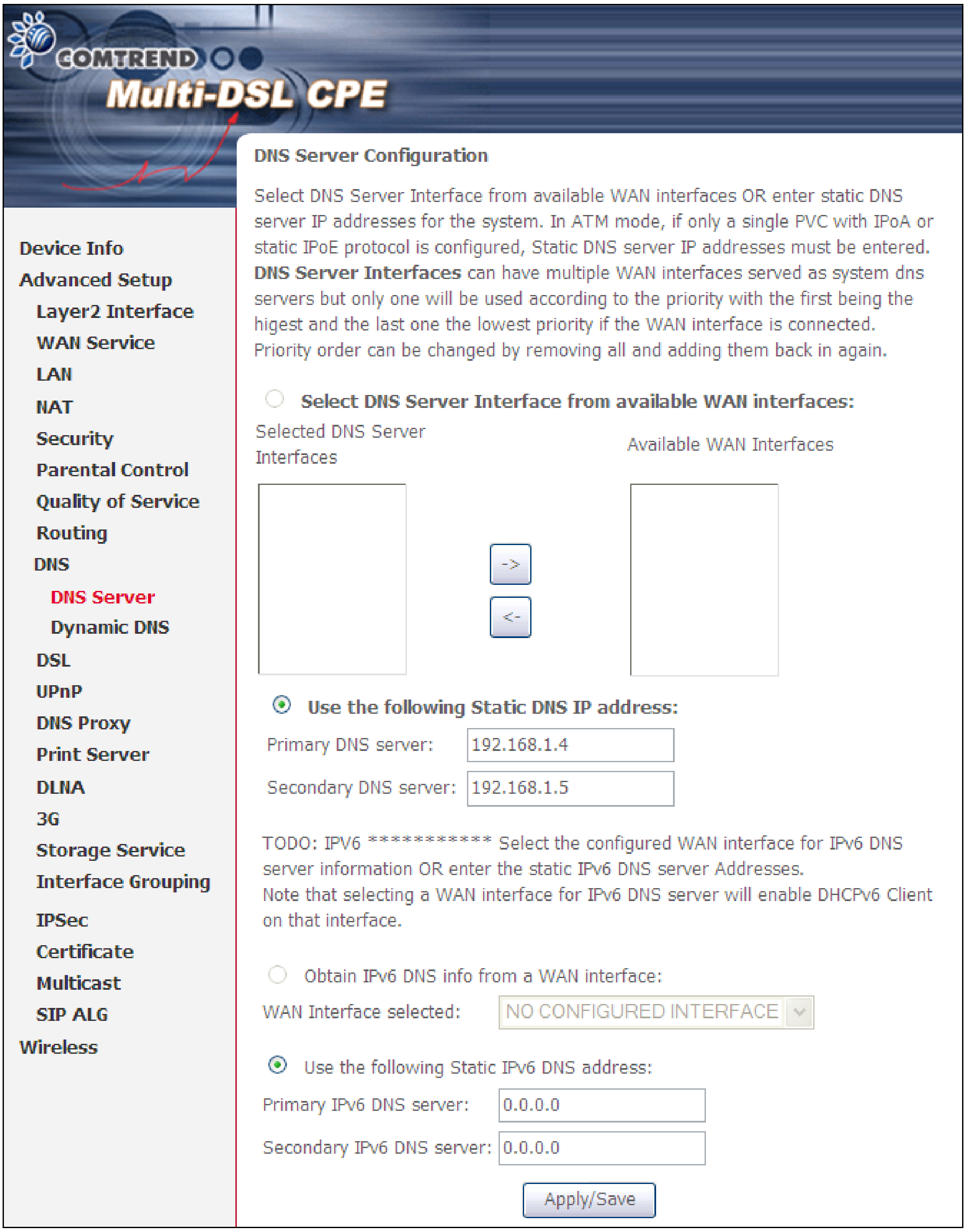
To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
ipoa0	2	Passive	□

5.10 DNS

5.10.1 DNS Server

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



DNS Server Configuration

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

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

Selected DNS Server Interfaces

Available WAN Interfaces

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

Primary DNS server: 192.168.1.4

Secondary DNS server: 192.168.1.5

TODO: IPV6 *********** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

○ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: NO CONFIGURED INTERFACE

● Use the following Static IPv6 DNS address:

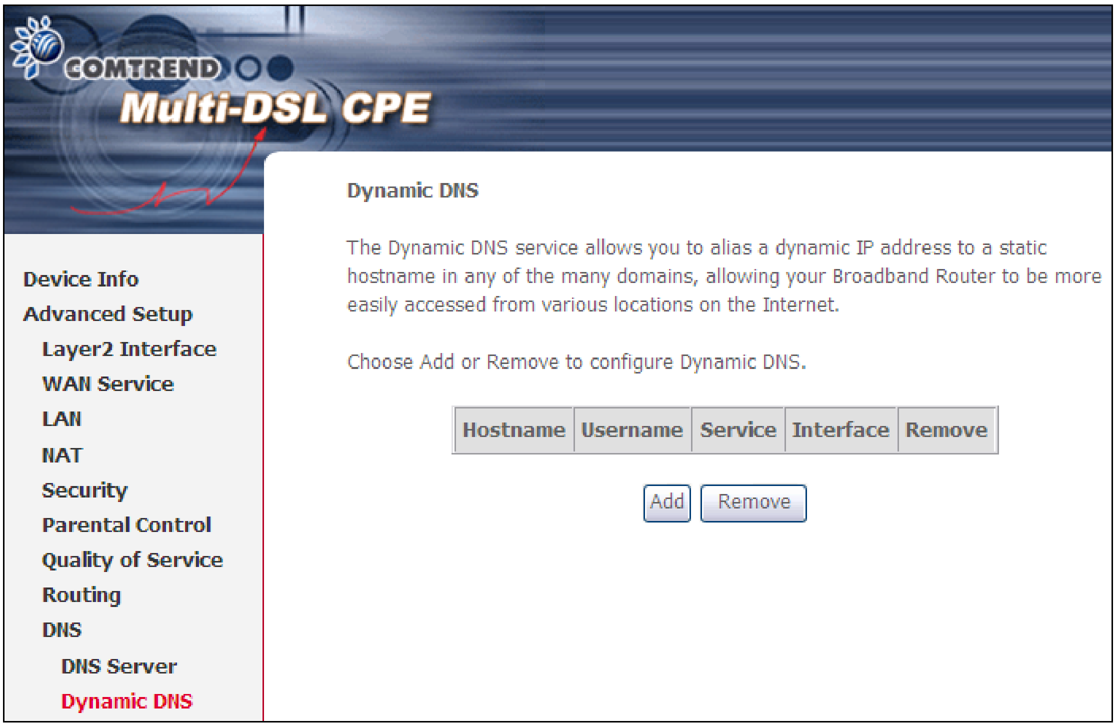
Primary IPv6 DNS server: 0.0.0.0

Secondary IPv6 DNS server: 0.0.0.0

Click Apply/Save to save the new configuration.

5.10.2 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-3026e to be more easily accessed from various locations on the Internet.



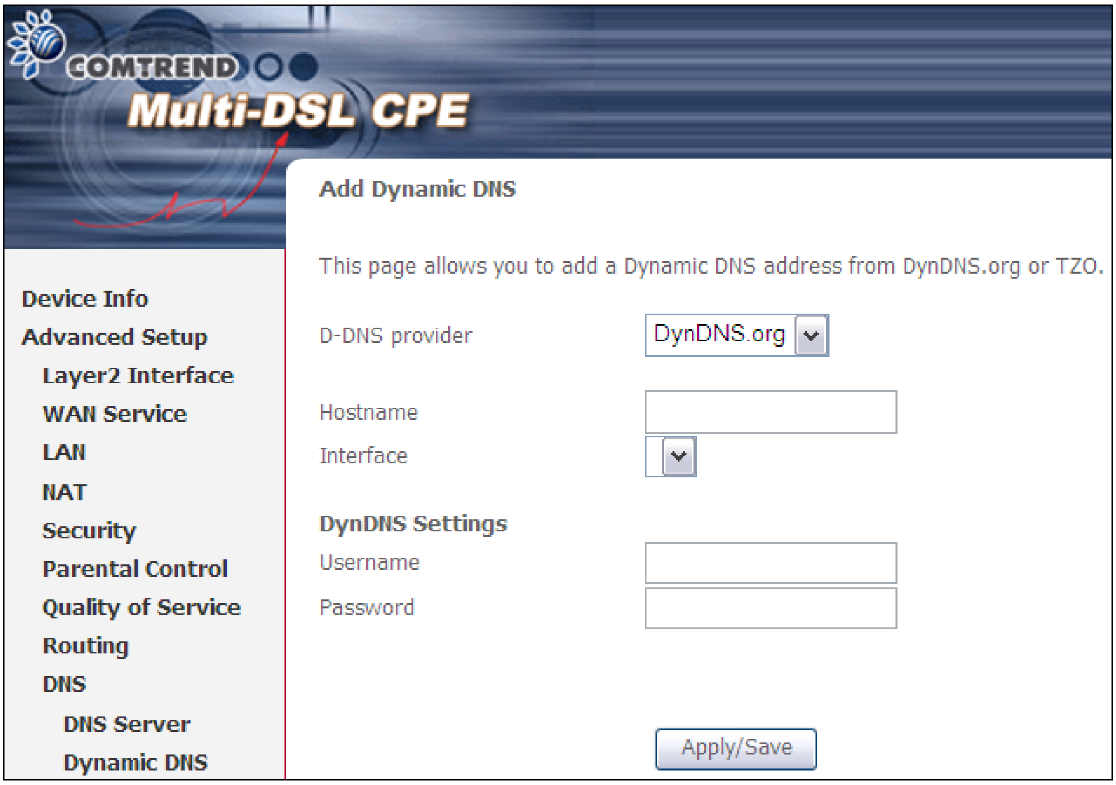
Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

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



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface:

DynDNS Settings

Username:

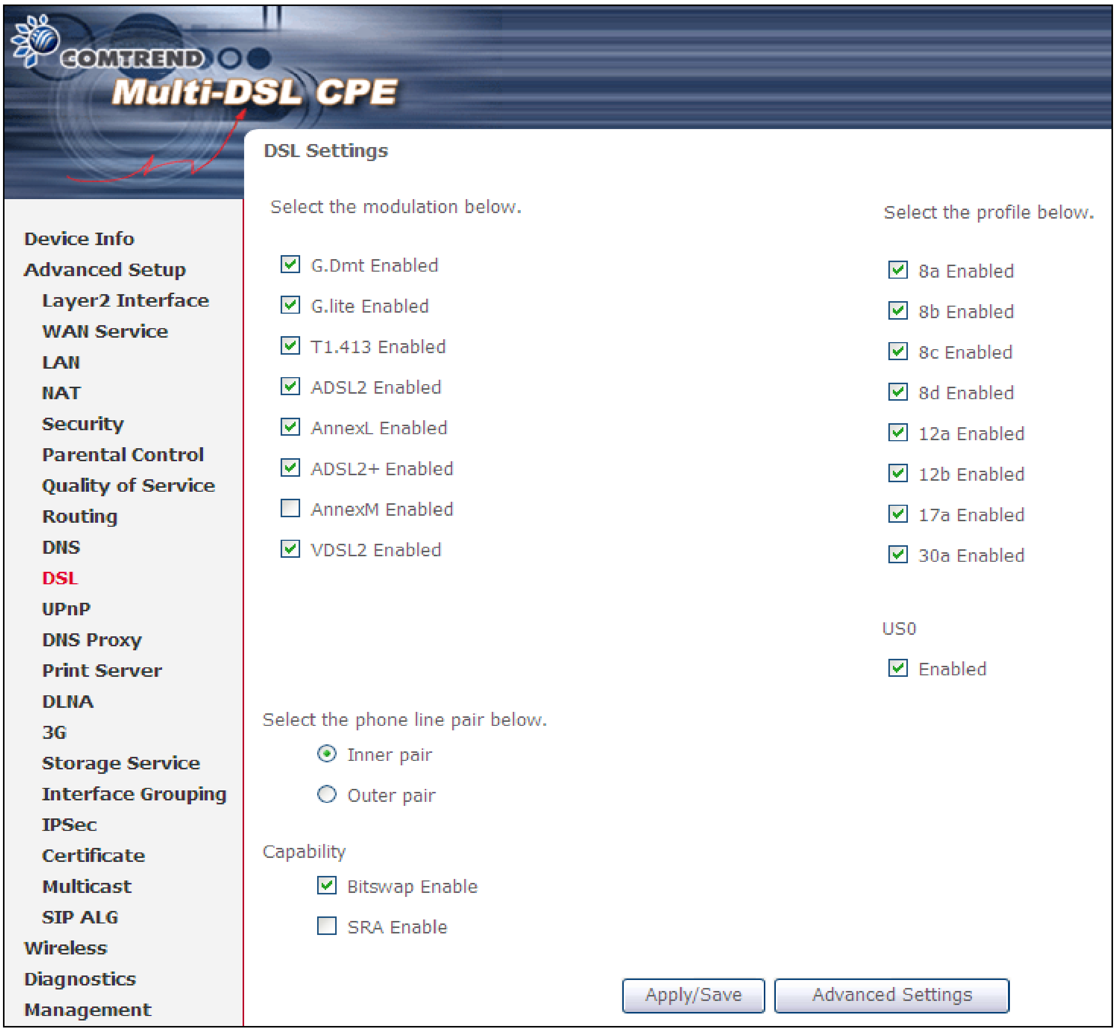
Password:

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

5.11 DSL

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



DSL Settings

Select the modulation below.

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

Select the profile below.

☑ 8a Enabled
☑ 8b Enabled
☑ 8c Enabled
☑ 8d Enabled
☑ 12a Enabled
☑ 12b Enabled
☑ 17a Enabled
☑ 30a Enabled

US0

☑ Enabled

Select the phone line pair below.

● Inner pair
○ Outer pair

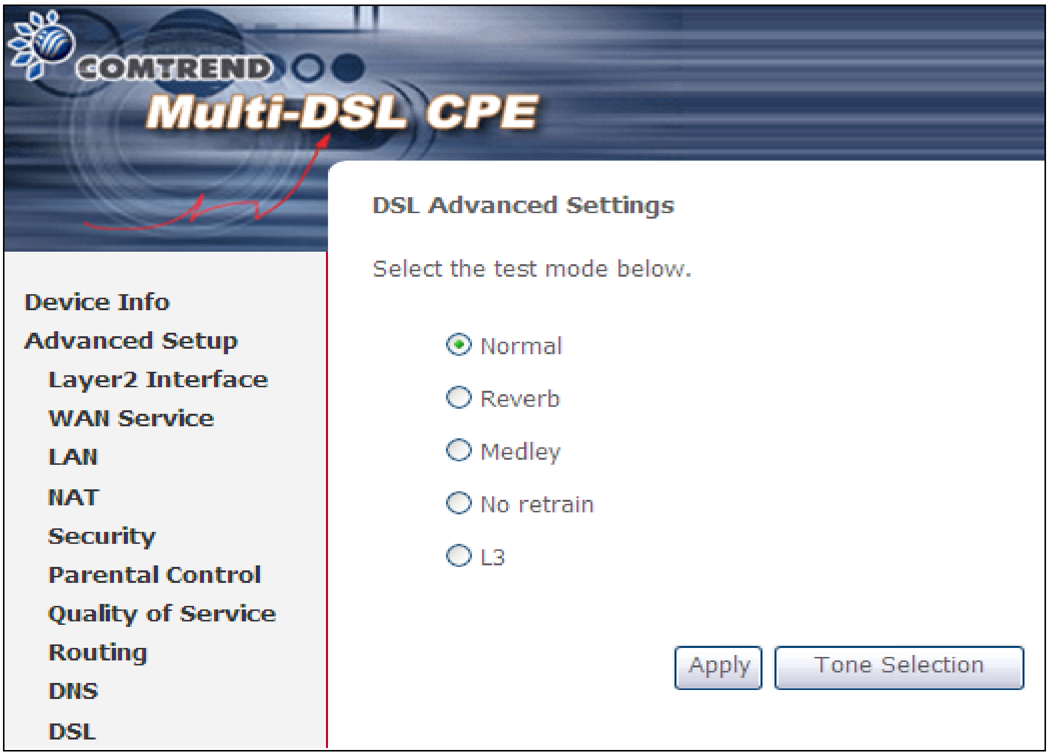
Capability

☑ Bitswap Enable
□ SRA Enable

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)
Profile Selection	8a-d, 12a-b, 17a, 30a, 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.



DSL Advanced Settings

Select the test mode below.

● Normal

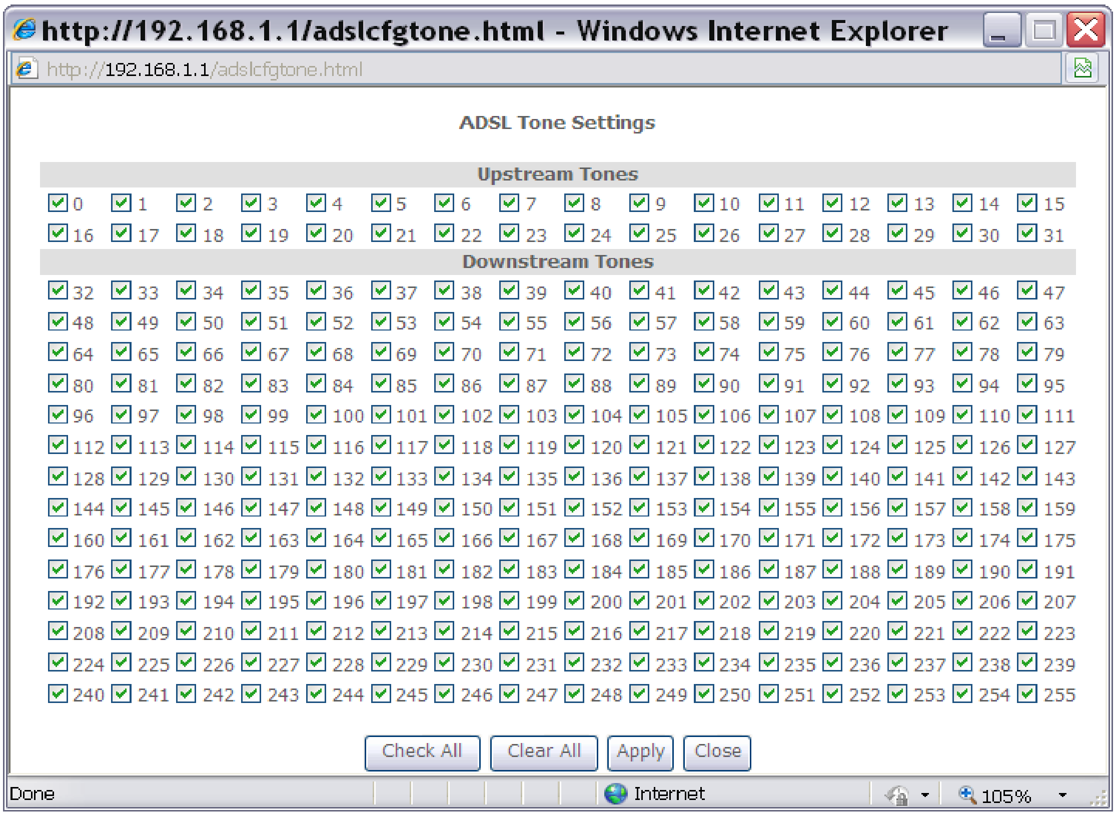
○ Reverb

○ Medley

○ No retrain

○ L3

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


http://192.168.1.1/adslcfgtone.html - Windows Internet Explorer
http://192.168.1.1/adslcfgtone.html

ADSL Tone Settings

Upstream Tones

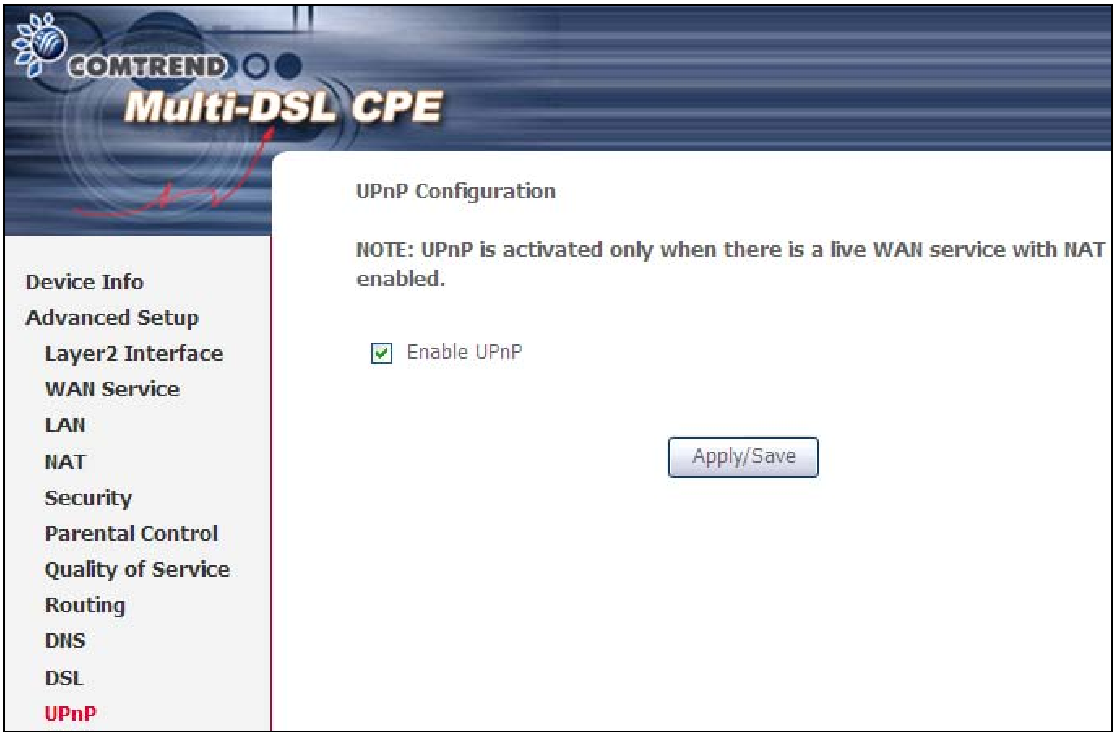
☑ 0	☑ 1	☑ 2	☑ 3	☑ 4	☑ 5	☑ 6	☑ 7	☑ 8	☑ 9	☑ 10	☑ 11	☑ 12	☑ 13	☑ 14	☑ 15
☑ 16	☑ 17	☑ 18	☑ 19	☑ 20	☑ 21	☑ 22	☑ 23	☑ 24	☑ 25	☑ 26	☑ 27	☑ 28	☑ 29	☑ 30	☑ 31

Downstream Tones

☑ 32	☑ 33	☑ 34	☑ 35	☑ 36	☑ 37	☑ 38	☑ 39	☑ 40	☑ 41	☑ 42	☑ 43	☑ 44	☑ 45	☑ 46	☑ 47
☑ 48	☑ 49	☑ 50	☑ 51	☑ 52	☑ 53	☑ 54	☑ 55	☑ 56	☑ 57	☑ 58	☑ 59	☑ 60	☑ 61	☑ 62	☑ 63
☑ 64	☑ 65	☑ 66	☑ 67	☑ 68	☑ 69	☑ 70	☑ 71	☑ 72	☑ 73	☑ 74	☑ 75	☑ 76	☑ 77	☑ 78	☑ 79
☑ 80	☑ 81	☑ 82	☑ 83	☑ 84	☑ 85	☑ 86	☑ 87	☑ 88	☑ 89	☑ 90	☑ 91	☑ 92	☑ 93	☑ 94	☑ 95
☑ 96	☑ 97	☑ 98	☑ 99	☑ 100	☑ 101	☑ 102	☑ 103	☑ 104	☑ 105	☑ 106	☑ 107	☑ 108	☑ 109	☑ 110	☑ 111
☑ 112	☑ 113	☑ 114	☑ 115	☑ 116	☑ 117	☑ 118	☑ 119	☑ 120	☑ 121	☑ 122	☑ 123	☑ 124	☑ 125	☑ 126	☑ 127
☑ 128	☑ 129	☑ 130	☑ 131	☑ 132	☑ 133	☑ 134	☑ 135	☑ 136	☑ 137	☑ 138	☑ 139	☑ 140	☑ 141	☑ 142	☑ 143
☑ 144	☑ 145	☑ 146	☑ 147	☑ 148	☑ 149	☑ 150	☑ 151	☑ 152	☑ 153	☑ 154	☑ 155	☑ 156	☑ 157	☑ 158	☑ 159
☑ 160	☑ 161	☑ 162	☑ 163	☑ 164	☑ 165	☑ 166	☑ 167	☑ 168	☑ 169	☑ 170	☑ 171	☑ 172	☑ 173	☑ 174	☑ 175
☑ 176	☑ 177	☑ 178	☑ 179	☑ 180	☑ 181	☑ 182	☑ 183	☑ 184	☑ 185	☑ 186	☑ 187	☑ 188	☑ 189	☑ 190	☑ 191
☑ 192	☑ 193	☑ 194	☑ 195	☑ 196	☑ 197	☑ 198	☑ 199	☑ 200	☑ 201	☑ 202	☑ 203	☑ 204	☑ 205	☑ 206	☑ 207
☑ 208	☑ 209	☑ 210	☑ 211	☑ 212	☑ 213	☑ 214	☑ 215	☑ 216	☑ 217	☑ 218	☑ 219	☑ 220	☑ 221	☑ 222	☑ 223
☑ 224	☑ 225	☑ 226	☑ 227	☑ 228	☑ 229	☑ 230	☑ 231	☑ 232	☑ 233	☑ 234	☑ 235	☑ 236	☑ 237	☑ 238	☑ 239
☑ 240	☑ 241	☑ 242	☑ 243	☑ 244	☑ 245	☑ 246	☑ 247	☑ 248	☑ 249	☑ 250	☑ 251	☑ 252	☑ 253	☑ 254	☑ 255

5.12 UPnP

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



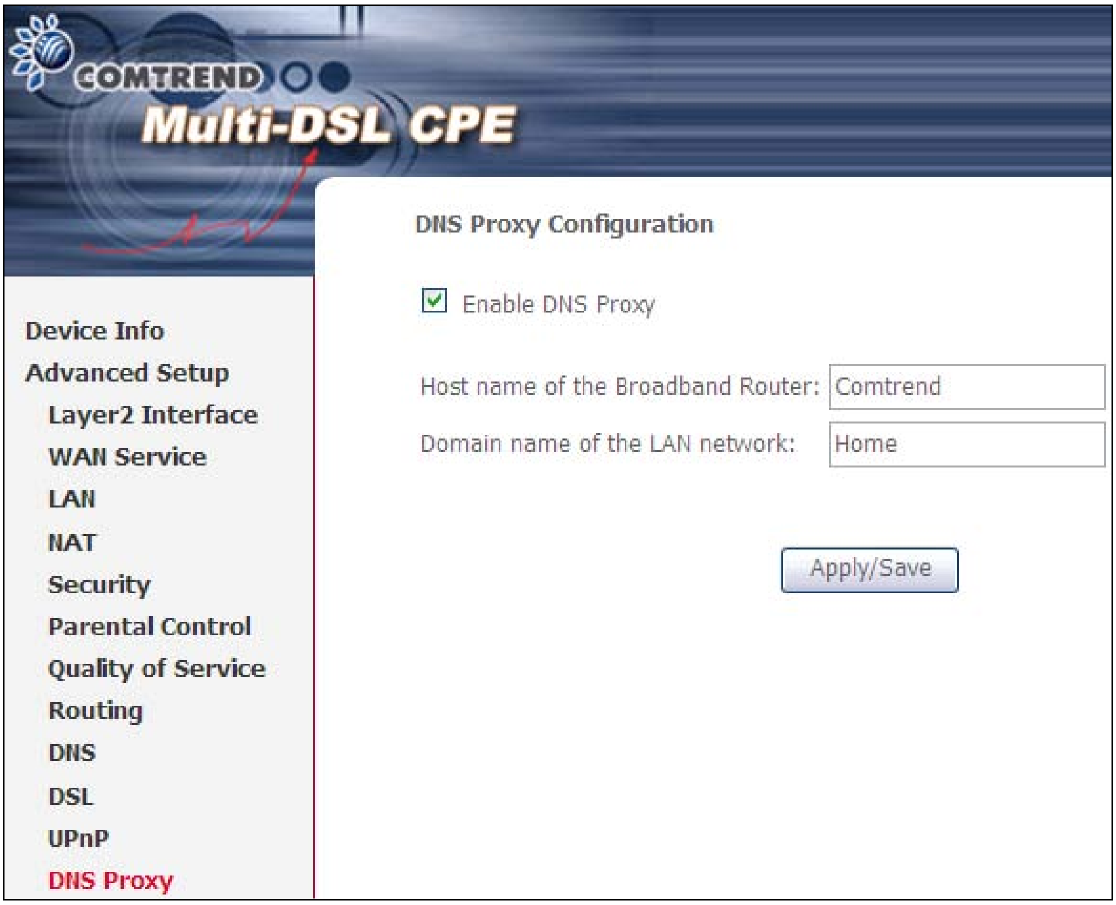
UPnP Configuration

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

☑ Enable UPnP

5.13 DNS Proxy

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



DNS Proxy Configuration

☑ Enable DNS Proxy

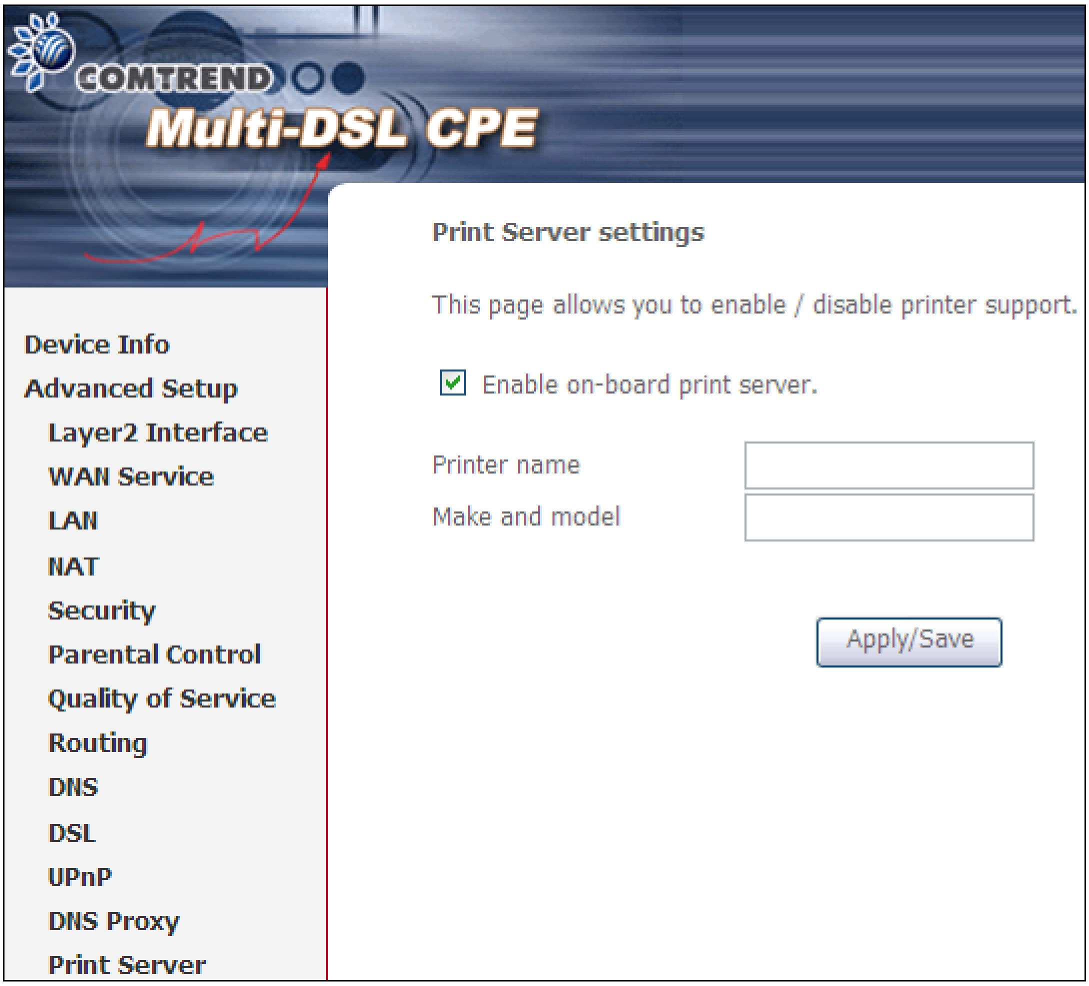
Host name of the Broadband Router: Comtrend

Domain name of the LAN network: Home

Apply/Save

5.14 Print Server

The CT-5374 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.



Print Server settings

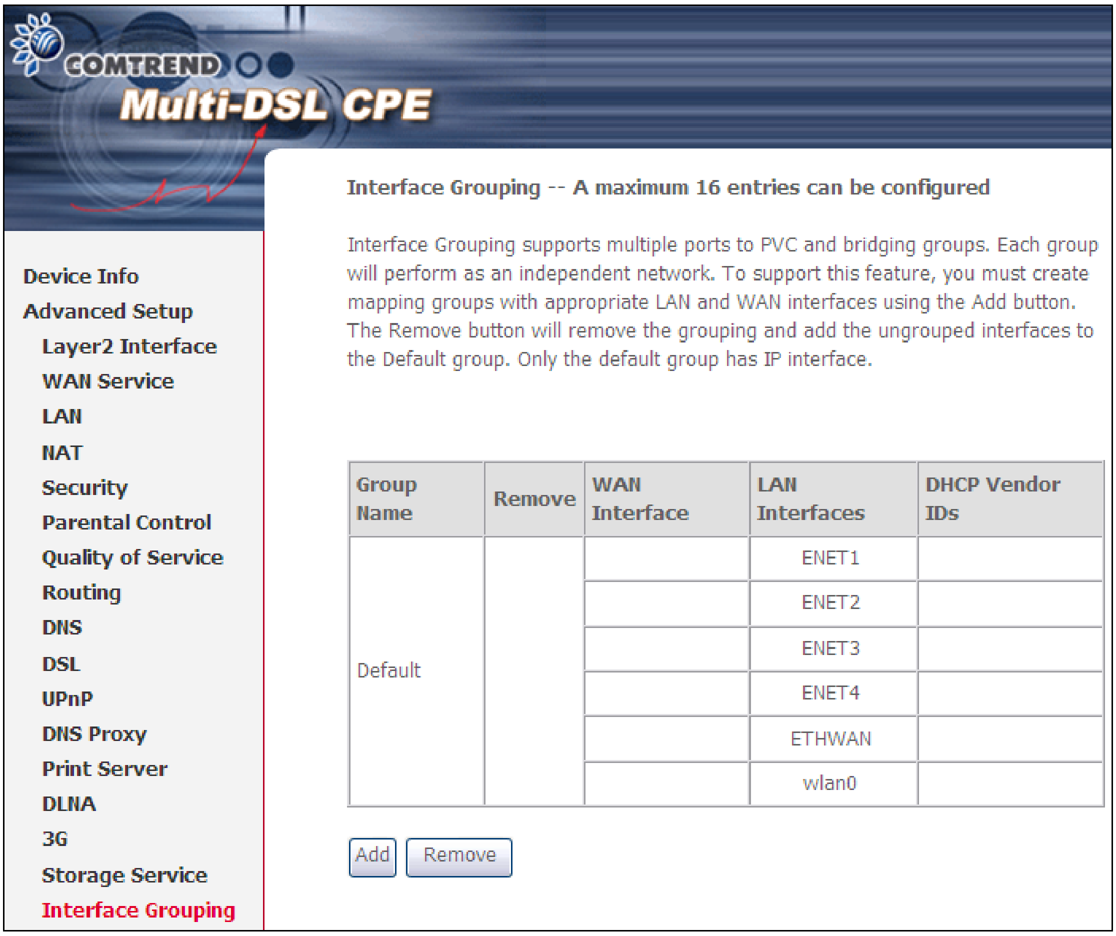
This page allows you to enable / disable printer support.

☑ Enable on-board print server.

Printer name	
Make and model	

5.15 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.

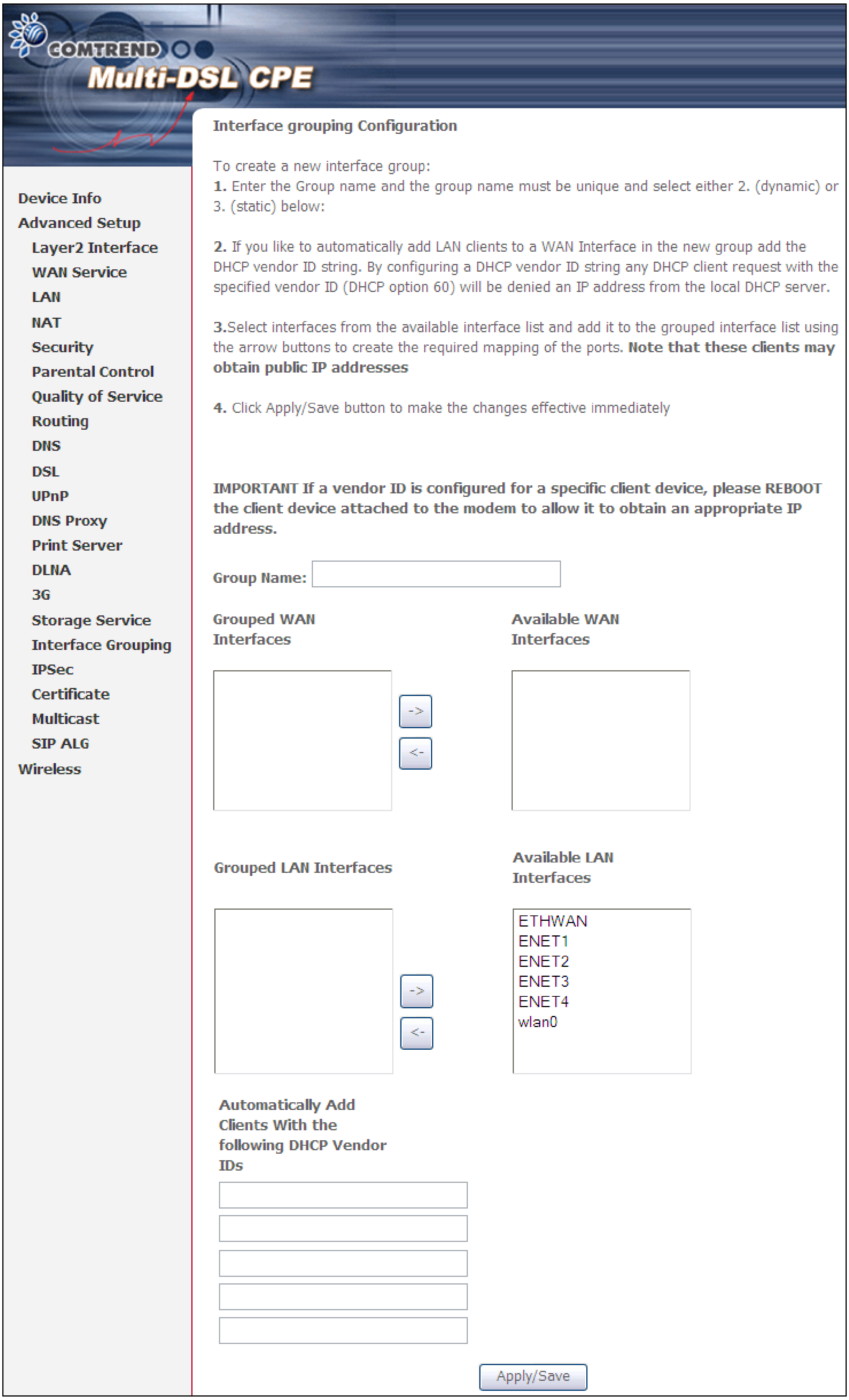


Interface Grouping -- A maximum 16 entries can be configured

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			ENET1	
			ENET2	
			ENET3	
			ENET4	
			ETHWAN	
			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 onscreen.



Interface grouping Configuration

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

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

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

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

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

Group Name:

Grouped WAN Interfaces | **Available WAN Interfaces**

Grouped LAN Interfaces | **Available LAN Interfaces**

ETHWAN
ENET1
ENET2
ENET3
ENET4
wlan0

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients With Following DHCP Vendor IDs:

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

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

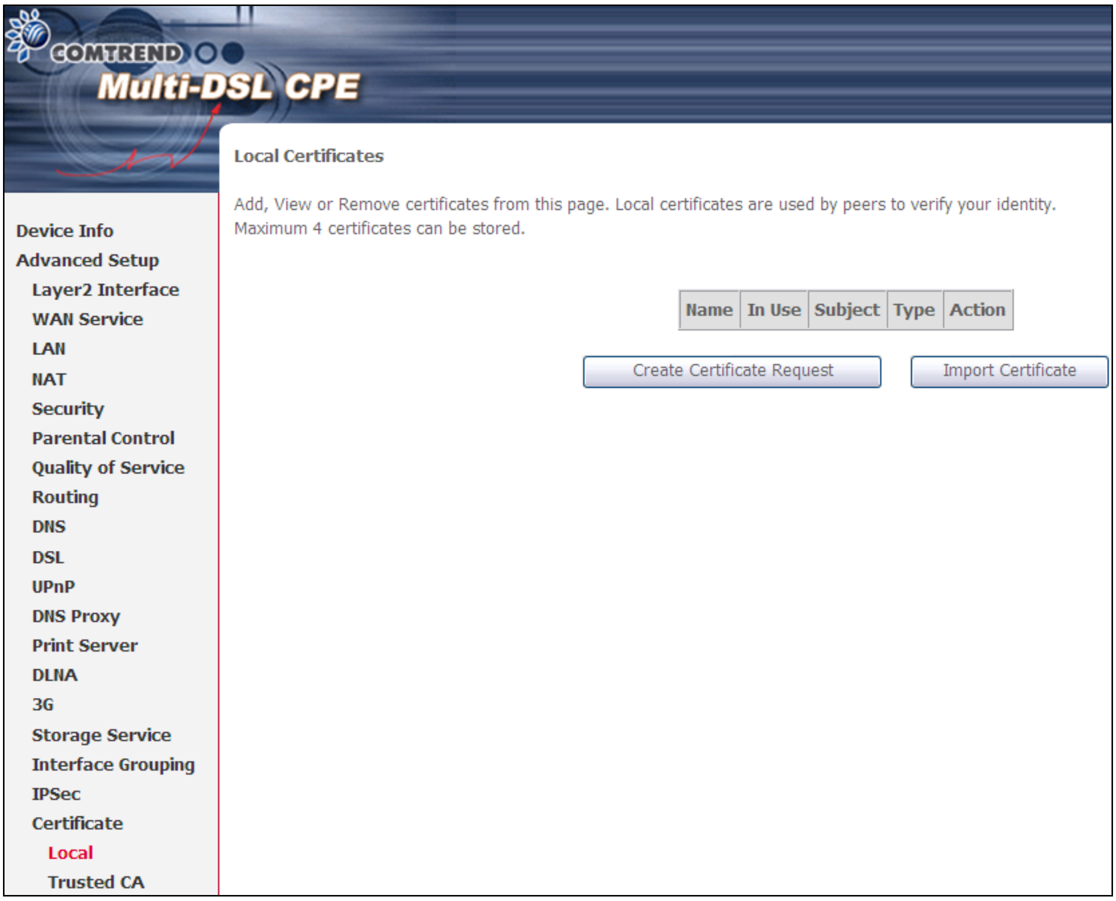
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

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

5.16 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



Local Certificates

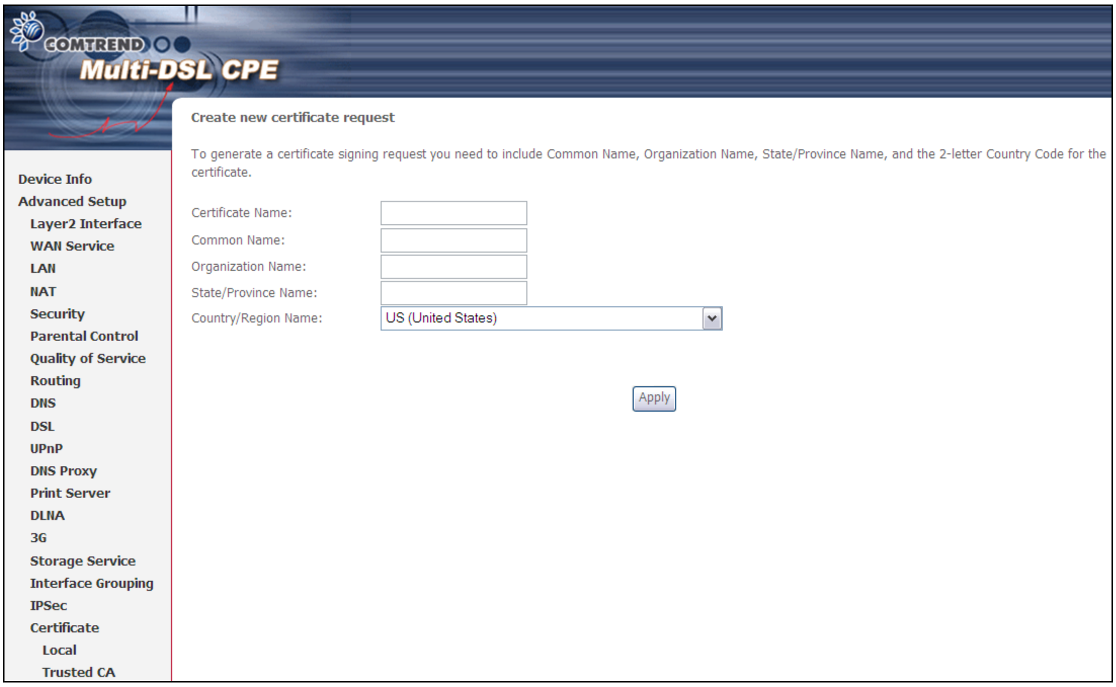
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

CREATE CERTIFICATE REQUEST

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

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



Create new certificate request

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

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

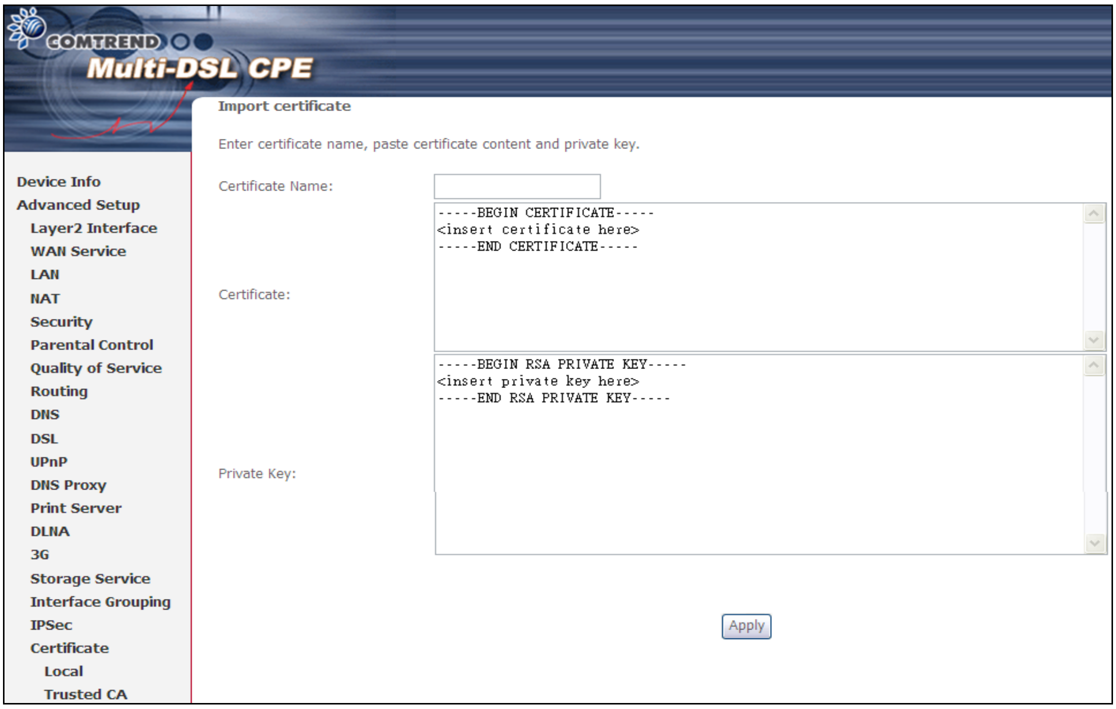
Country/Region Name: US (United States)

The following table is provided for your reference.

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

IMPORT CERTIFICATE

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



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

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

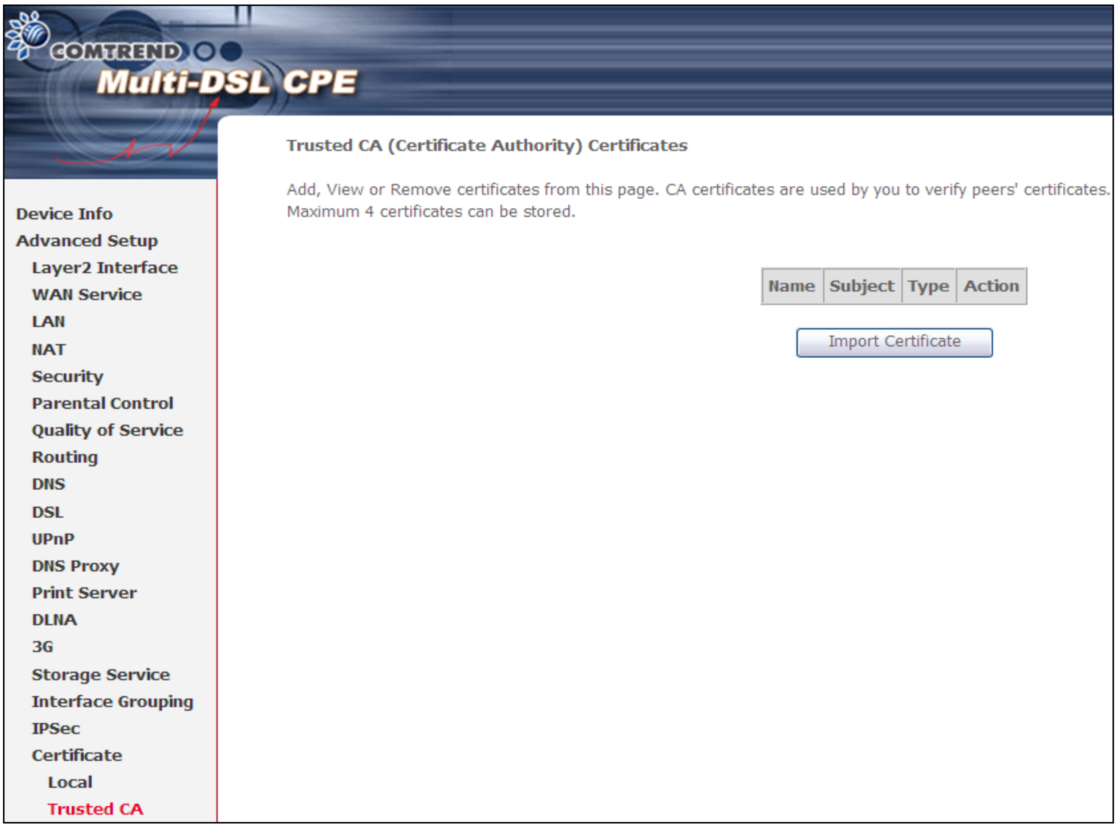
Private Key:

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

Enter a certificate name and click **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.

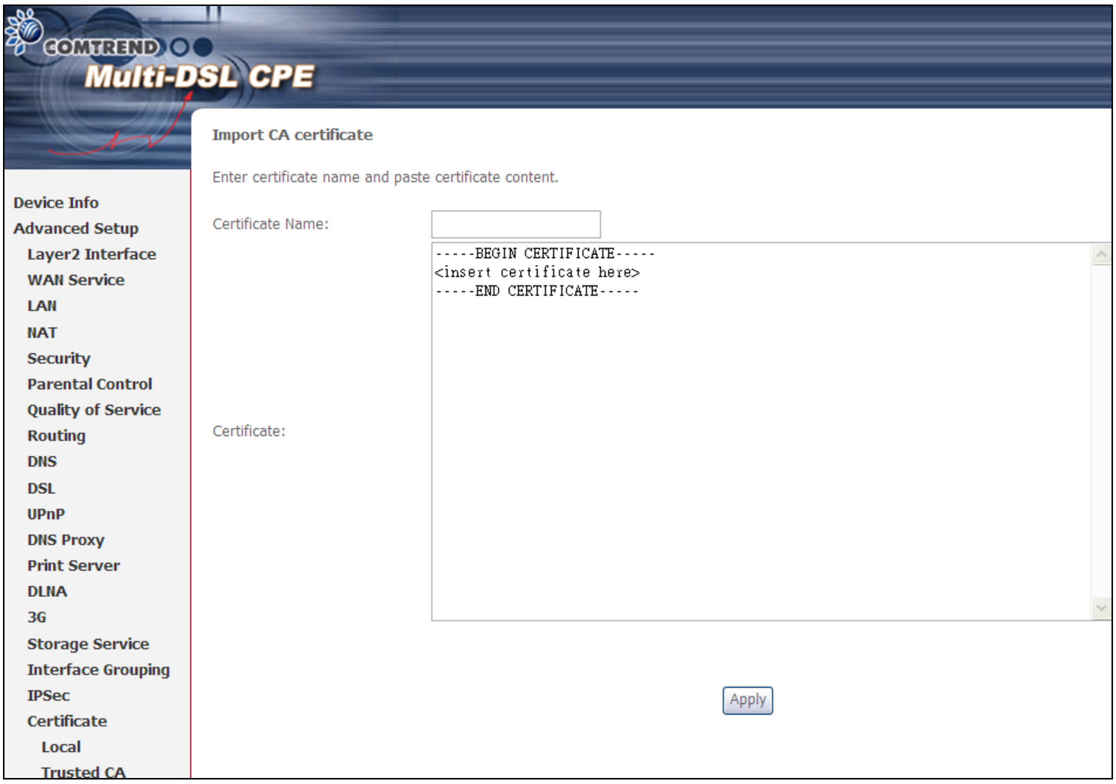


Trusted CA (Certificate Authority) Certificates

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

Name	Subject	Type	Action

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



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

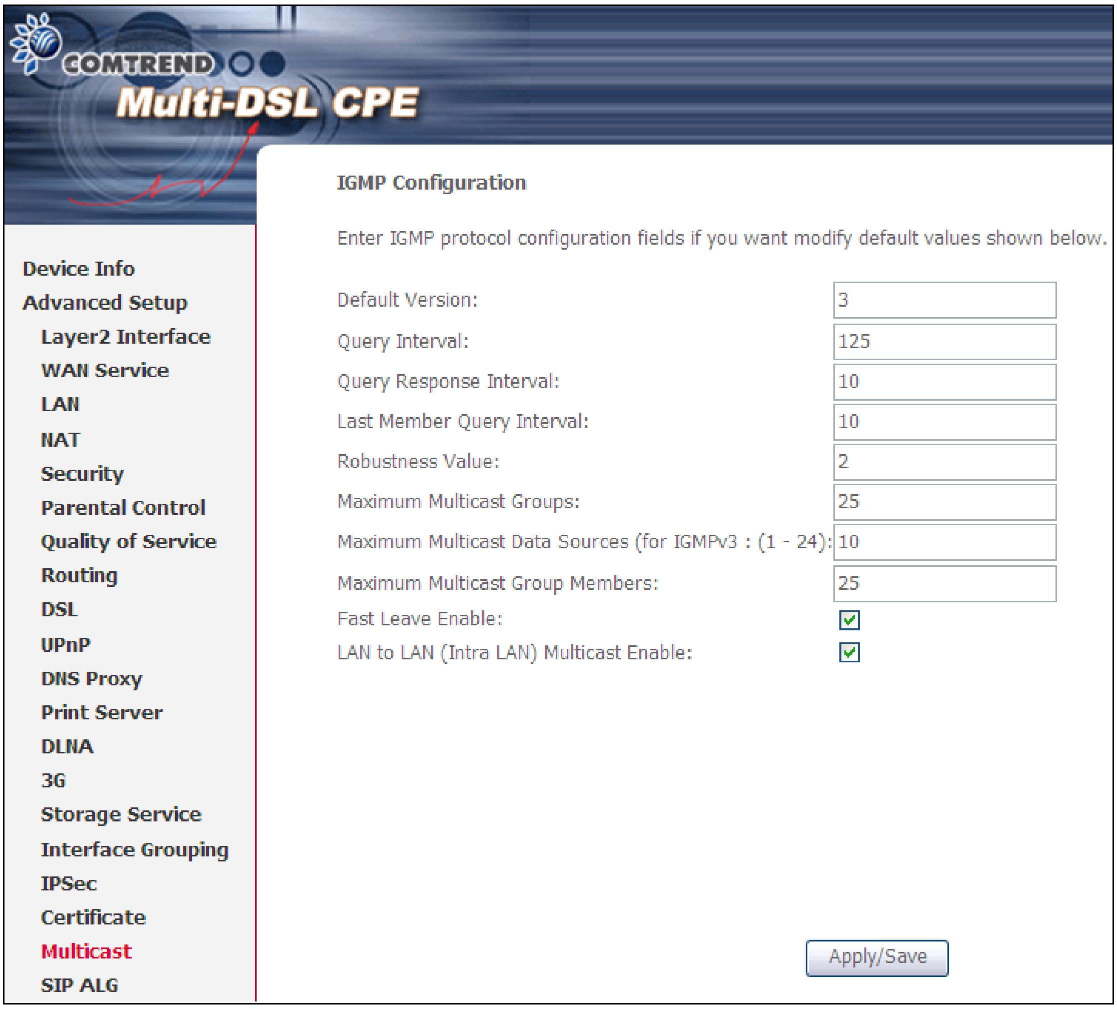
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

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

5.17 Multicast

IP multicast is a method of forwarding the same set of IP packets to a number of hosts within a network .You can use multicast in both IPv4 and IPv6 networks to provide efficient delivery of data to multiple destinations.

Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel.



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: ☑
LAN to LAN (Intra LAN) Multicast Enable: ☑

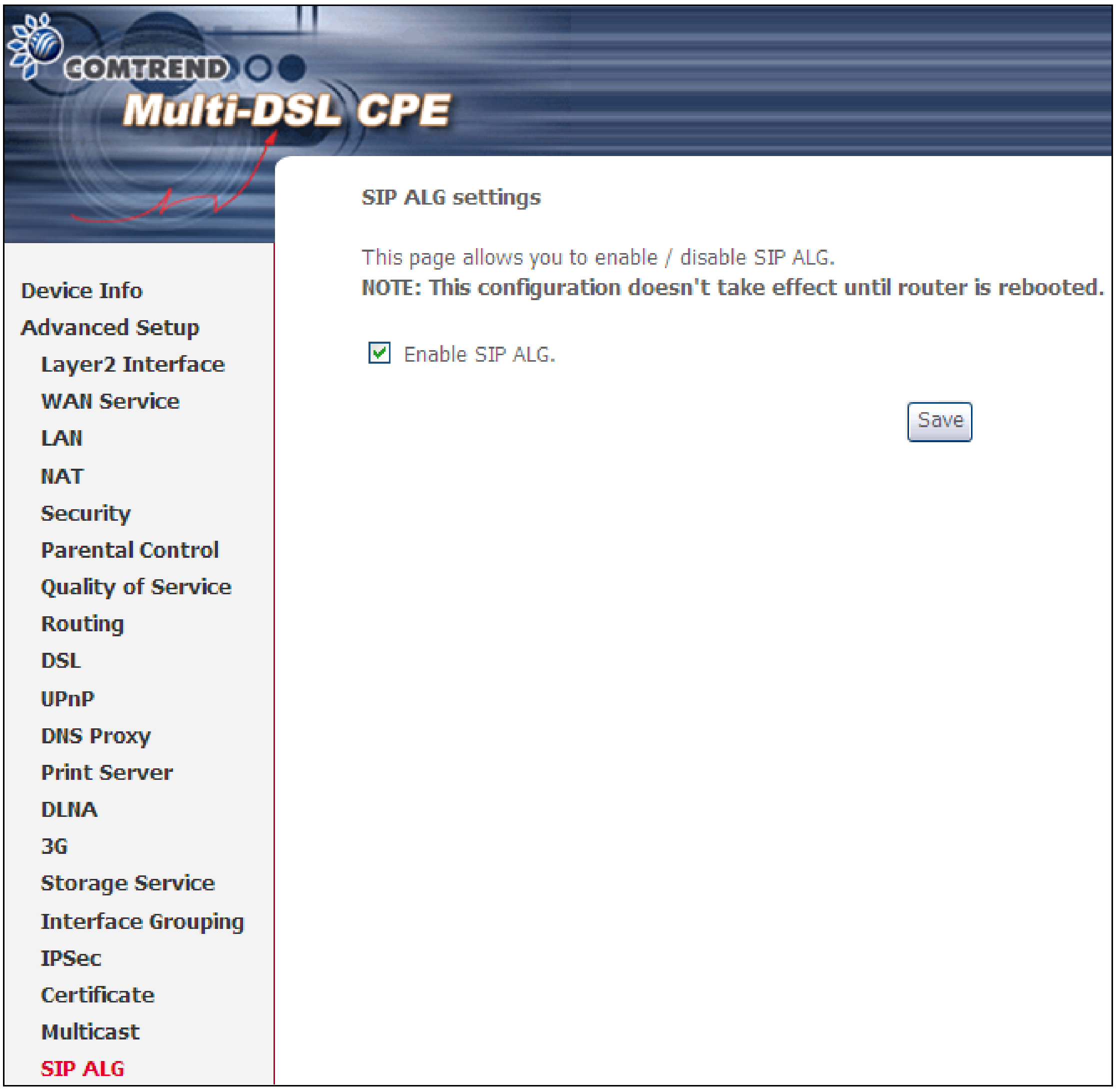
Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.

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

5.18 SIP ALG

SIP ALG is Application layer gateway. If the user has an IP phone (SIP) or VoIP gateway (SIP) behind the ADSL router, the SIP ALG can help VoIP packet passthrough the router (NAT enabled).

To enable the SIP ALG select the **Enable SIP ALG** checkbox and click **Save**.



SIP ALG settings

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

☑ Enable SIP ALG.

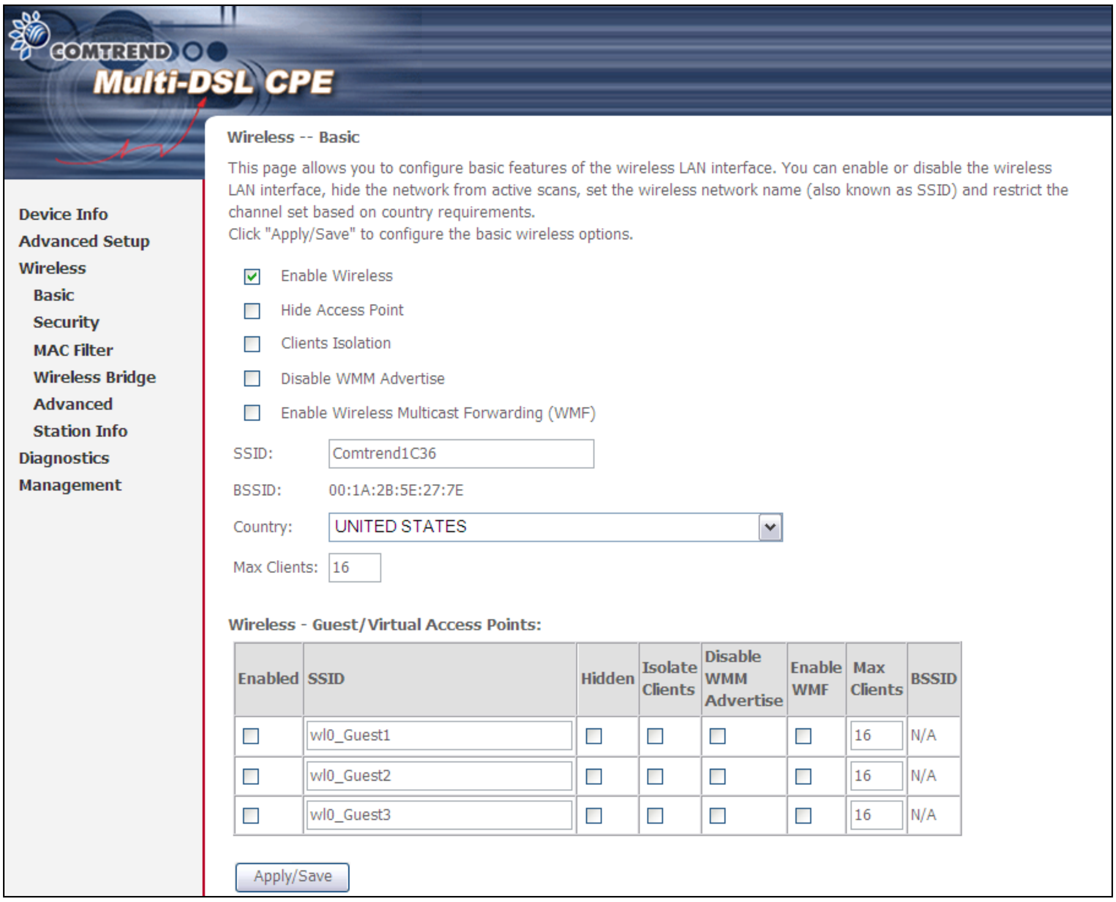
NOTE: SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. This ALG is only valid for SIP protocol running UDP port 5060.

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.



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: Comtrend1C36

BSSID: 00:1A:2B:5E:27:7E

Country: UNITED STATES

Max Clients: 16

Wireless - Guest/Virtual Access Points:

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

Apply/Save

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

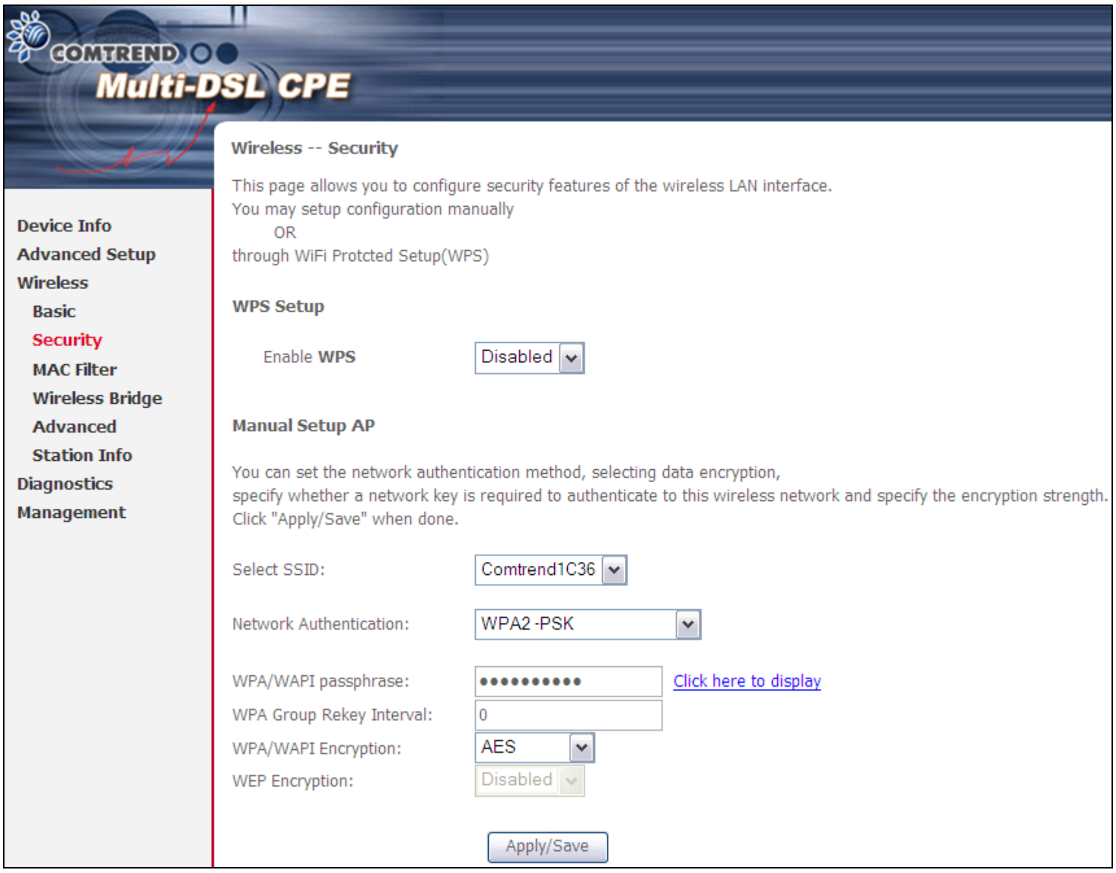
Consult the table below for descriptions of these options.

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

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

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 Protcted Setup(WPS)

WPS Setup

Enable WPS: Disabled

Manual Setup AP

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

Select SSID:	Comtrend1C36
Network Authentication:	WPA2 -PSK
WPA/WAPI passphrase:	••••••••••
WPA Group Rekey Interval:	0
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

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

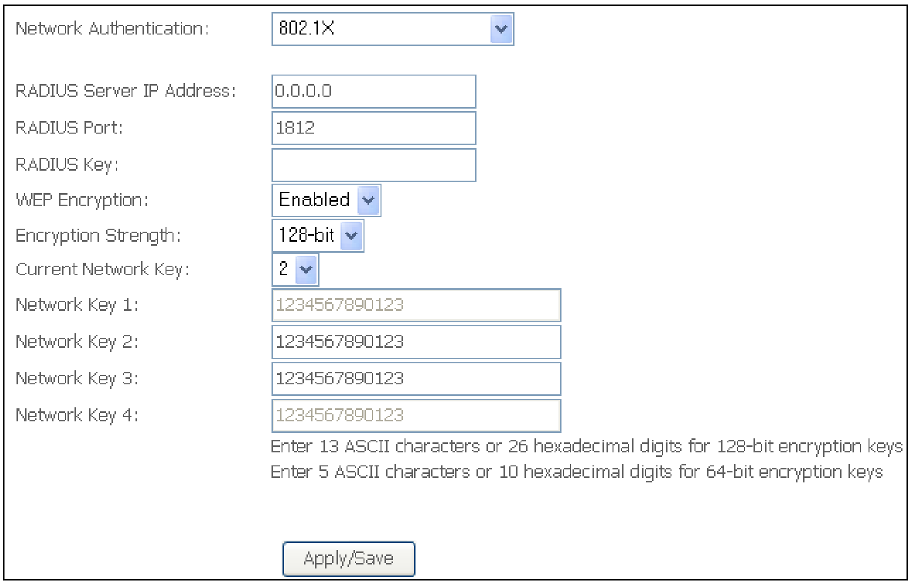
WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see 6.2.1 WPS) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

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

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

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



Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1: 1234567890123

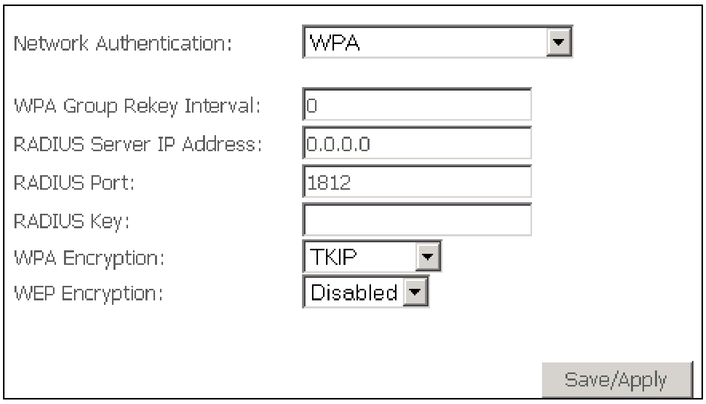
Network Key 2: 1234567890123

Network Key 3: 1234567890123

Network Key 4: 1234567890123

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

The settings for WPA authentication are shown below.



Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

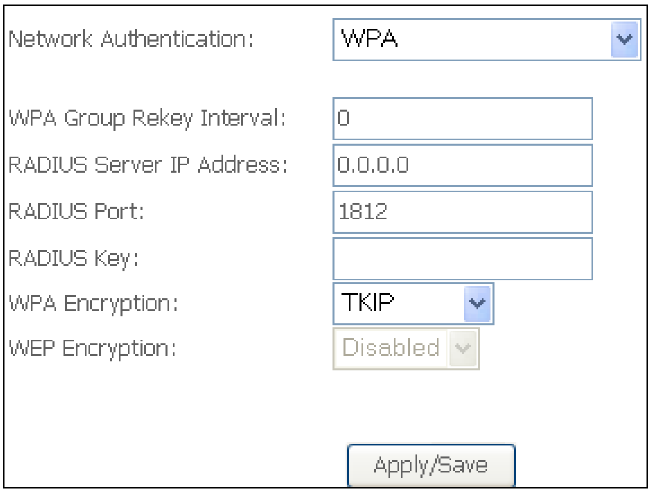
RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP

WEP Encryption: Disabled

The settings for WPA-PSK authentication are shown next.



Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP

WEP Encryption: Disabled

WEP Encryption

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

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

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

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 “3600”.

WPA/WAPI Encryption

Select the encryption algorithm you want to use: AES or TKIP+ AES (TKIP+ AES is an encryption method stronger than AES)

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.

6.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The CT-5374 has both a WPS button on the device and a virtual button accessible from the web user interface (WUI).

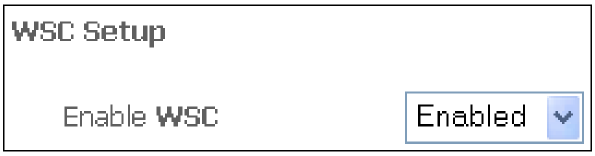
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase “Wi-Fi Protected Setup”.

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

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

I. Setup

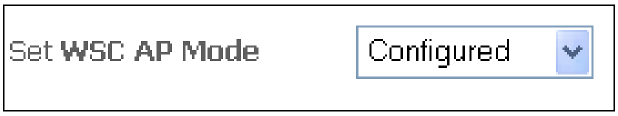
Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.



WSC Setup

Enable WSC: Enabled

Step 2: Set the WSC AP Mode. **Configured** is used when the CT-5374 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the CT-5374.



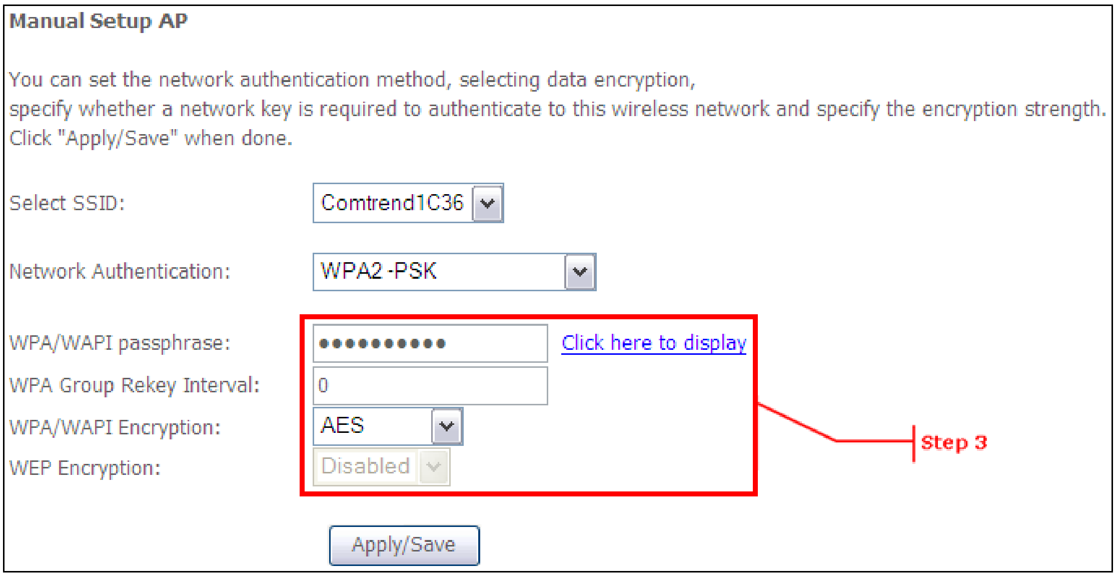
Set WSC AP Mode: Configured

NOTES: Your client may or may not have the ability to provide security settings to the CT-5374. If it does not, then you must set the WSC AP mode to Configured. Consult the device documentation to check its capabilities.

In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix E - WSC External Registrar has detailed instructions).

II. NETWORK AUTHENTICATION

Step 3: Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.



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: Comtrend1C36

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ●●●●●●●●●●

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

Step 4: Click the **Save / Apply** button at the bottom of the screen.

IIIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

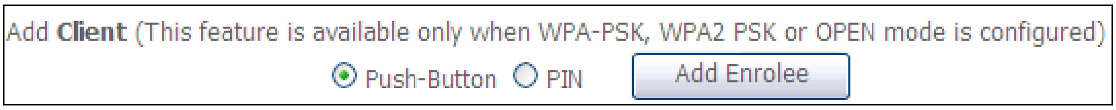
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

Step 6: **First method: WPS button**
Press the WPS button on the rear panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Second method: WUI virtual button
Select the Push-Button radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

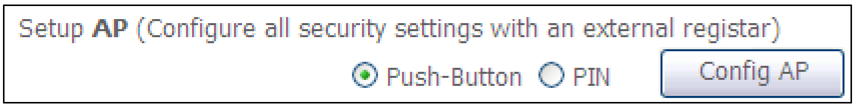
A - For **Configured** mode, click the **Add Enrollee** button.



Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

● Push-Button ○ PIN

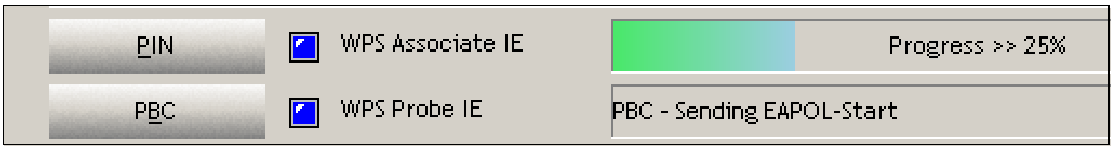
B - For **Unconfigured** mode, click the **Config AP** button.



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

● Push-Button ○ PIN

Step 7: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 25%

PBC - Sending EAPOL-Start

Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IIIb. WPS – PIN CONFIGURATION

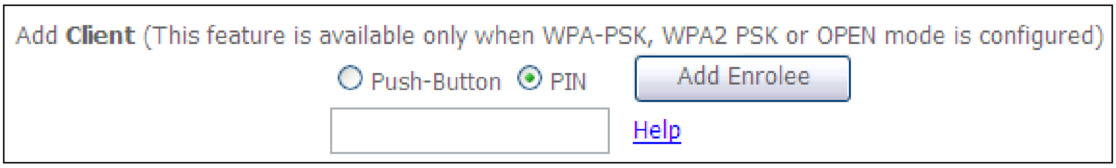
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

Step 6: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

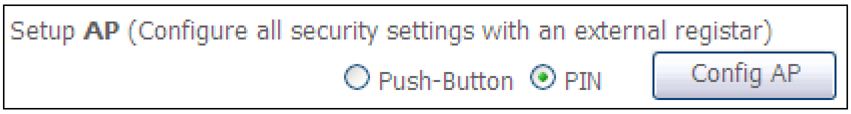
A - For **Configured** mode, enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).



Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)

○ Push-Button ● PIN

B - For **Unconfigured** mode, click the **Config AP** button.

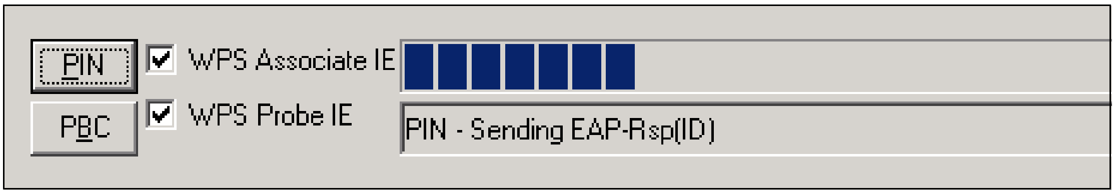


Setup **AP** (Configure all security settings with an external registar)

○ Push-Button ● PIN

Step 7: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

The figure below provides an example of a WPS client PIN function in-progress.

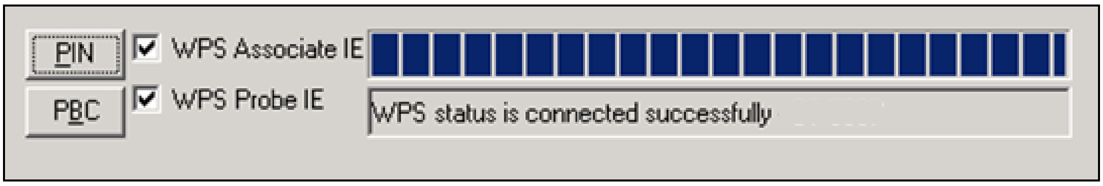


PIN - Sending EAP-Rsp(ID)

Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IV. CHECK CONNECTION

Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.

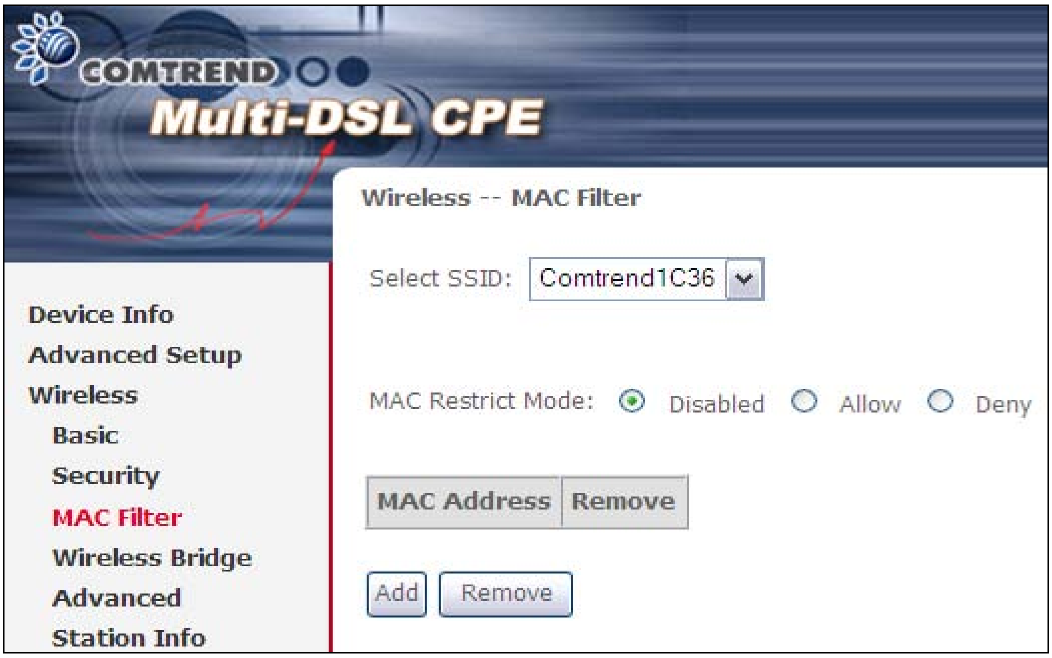


WPS status is connected successfully

You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

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.



Wireless -- MAC Filter

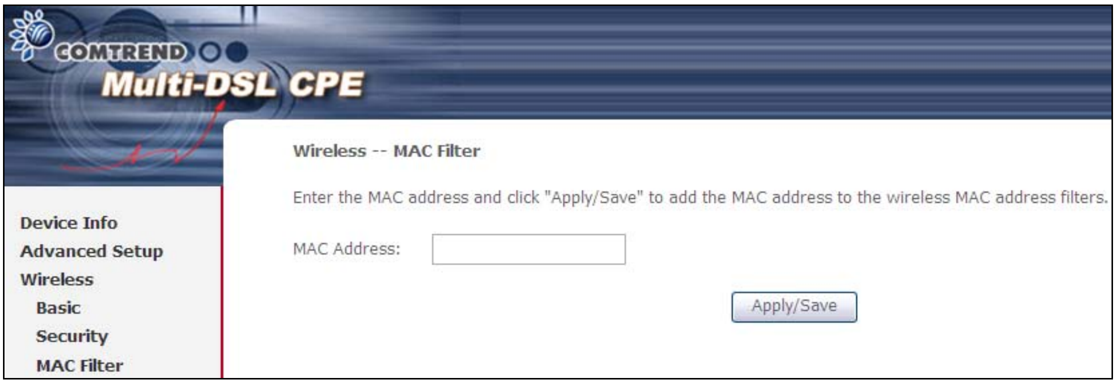
Select SSID: Comtrend1C36

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

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**.



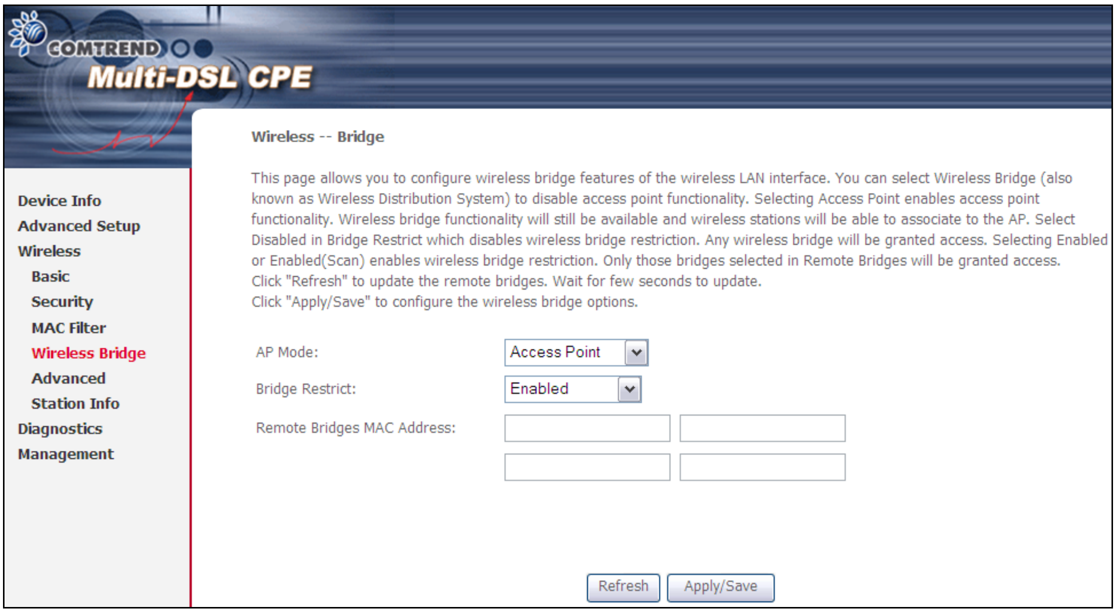
Wireless -- MAC Filter

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

MAC Address:

6.4 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.



Wireless -- Bridge

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.

AP Mode: Access Point

Bridge Restrict: Enabled

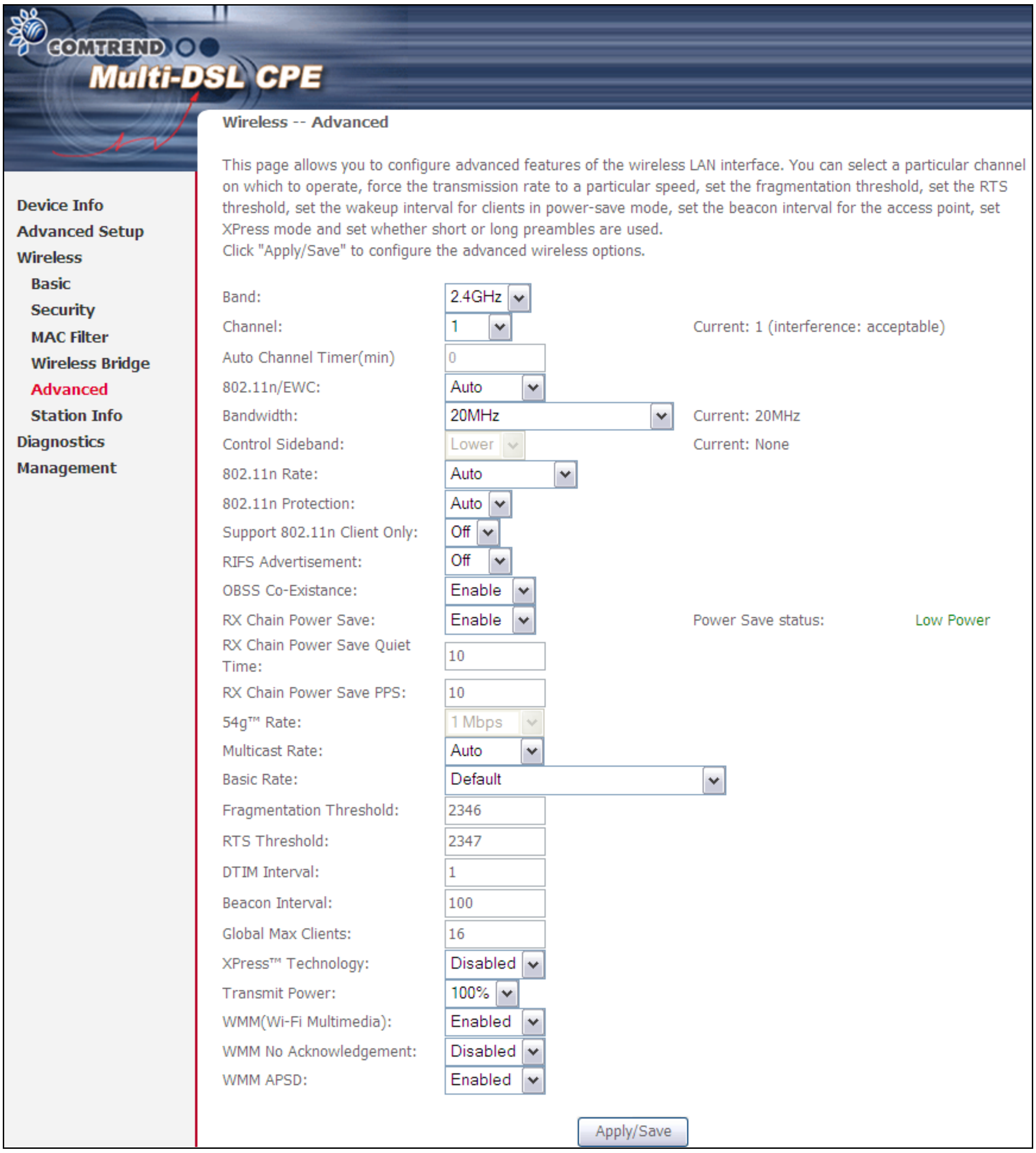
Remote Bridges MAC Address:

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.



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:	1	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existance:	Enable	
RX Chain Power Save:	Enable	Power Save status: Low Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

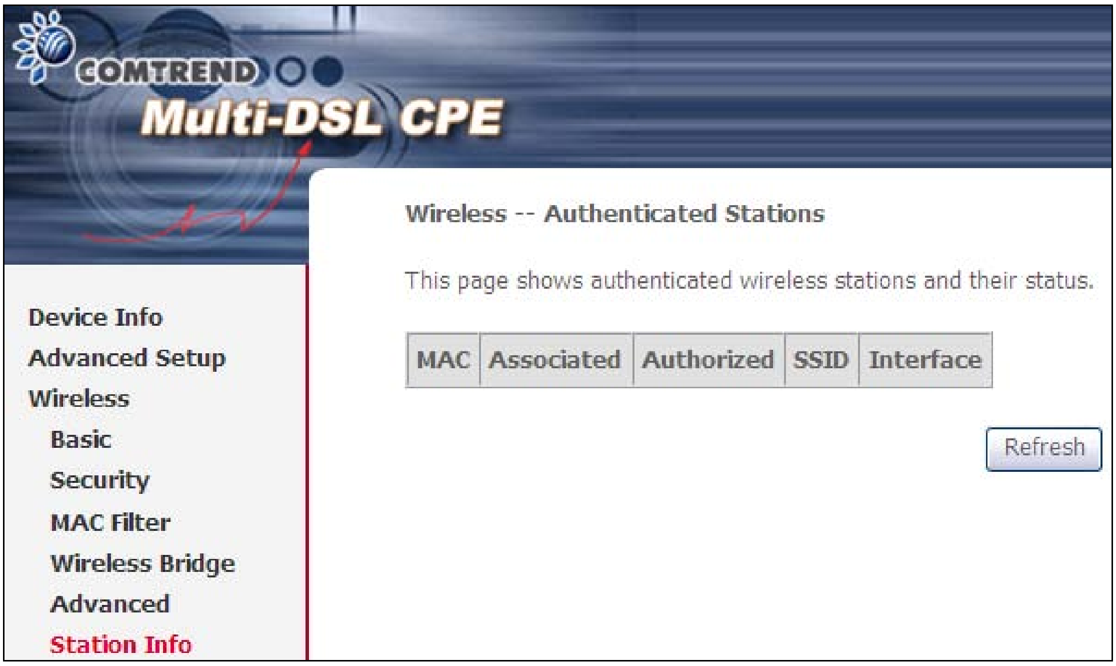
Field	**Description**
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a 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.)

Field	Description
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.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
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.

Field	Description
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 TM 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 Station Info

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



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

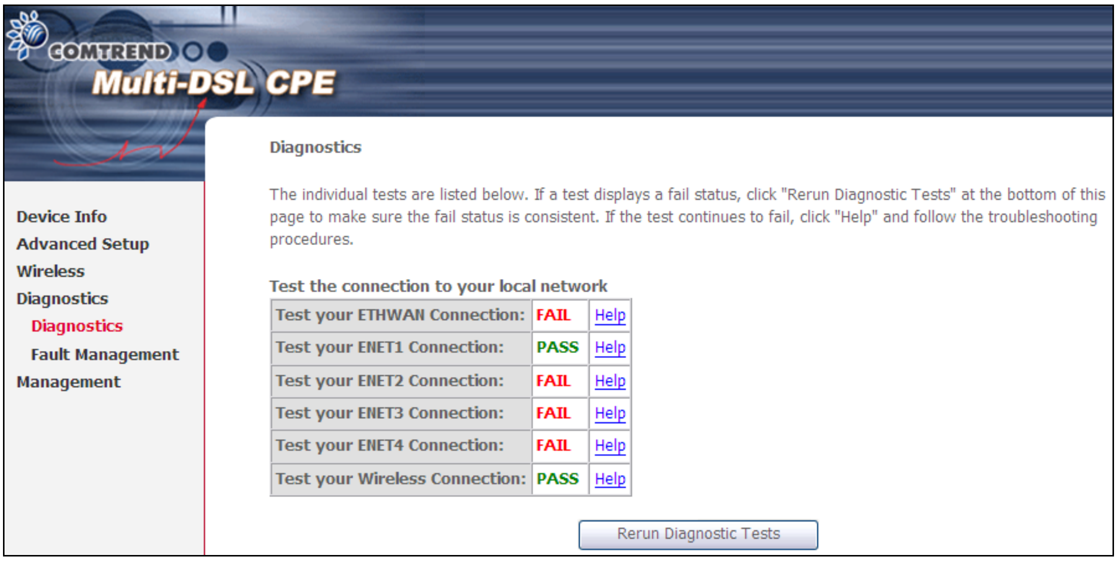
MAC	Associated	Authorized	SSID	Interface

Consult the table below for descriptions of each column heading.

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.



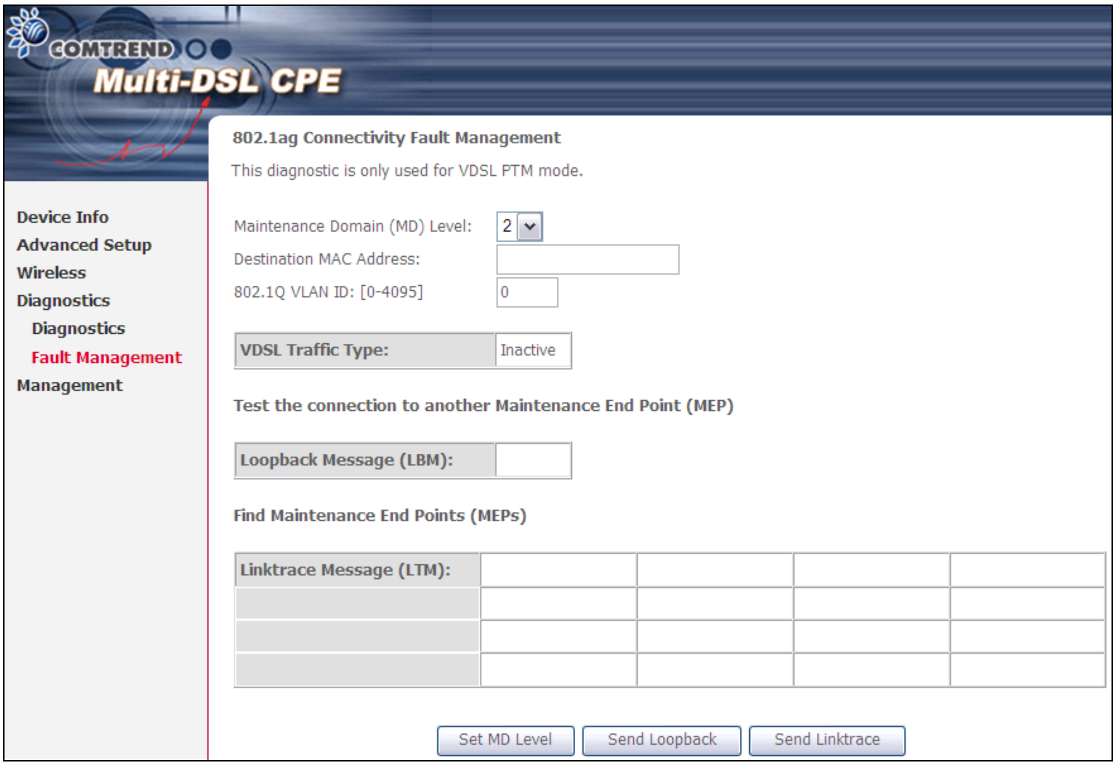
Diagnostics

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

Test the connection to your local network

Test your ETHWAN Connection:	FAIL	Help
Test your ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

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: 2

Destination MAC Address:

802.1Q VLAN ID: [0-4095] 0

VDSL Traffic Type:	Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):	

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

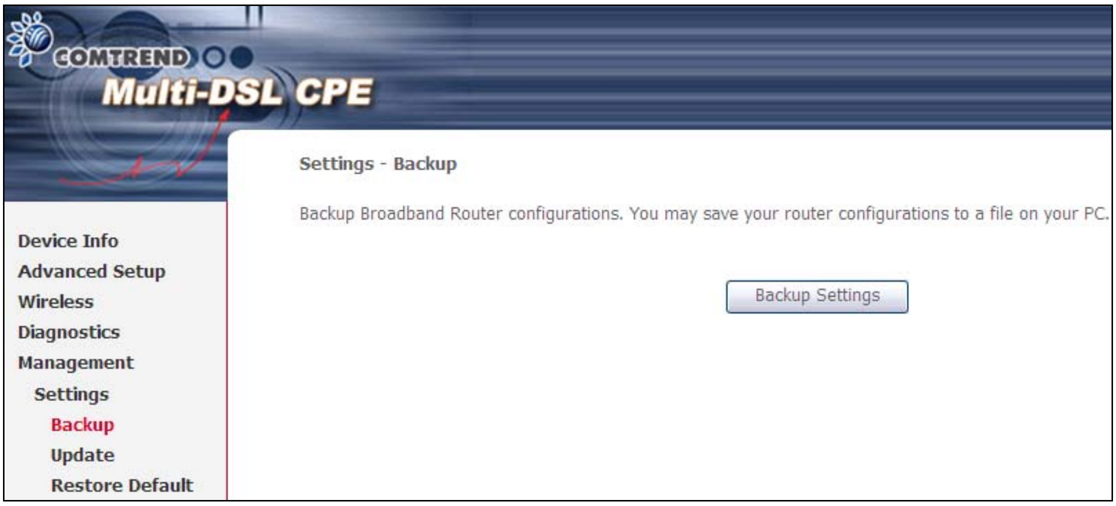
Chapter 8 Management

8.1 Settings

This includes 8.1.1 Backup Settings, 8.1.2 Update Settings, and 8.1.3 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.

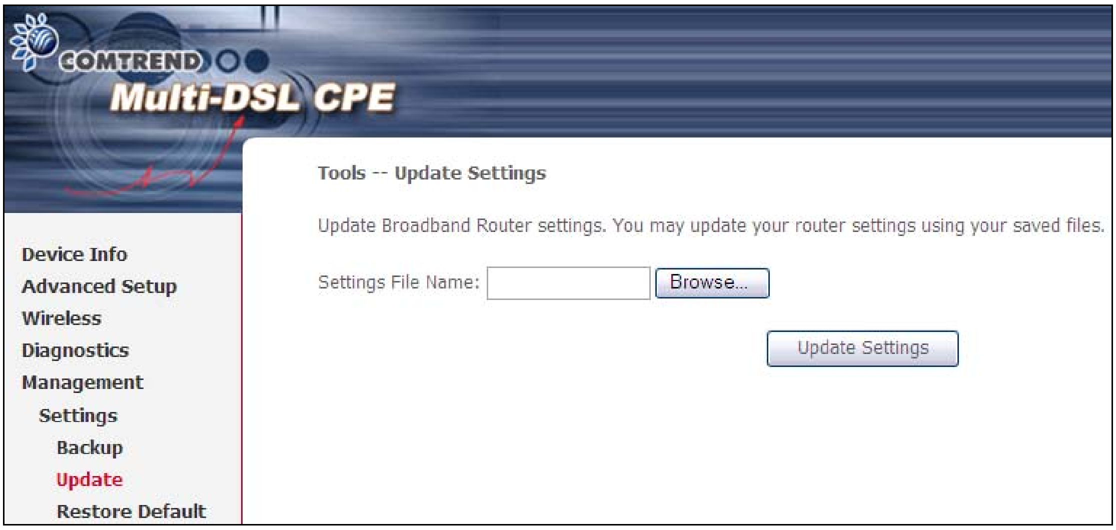


Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

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.



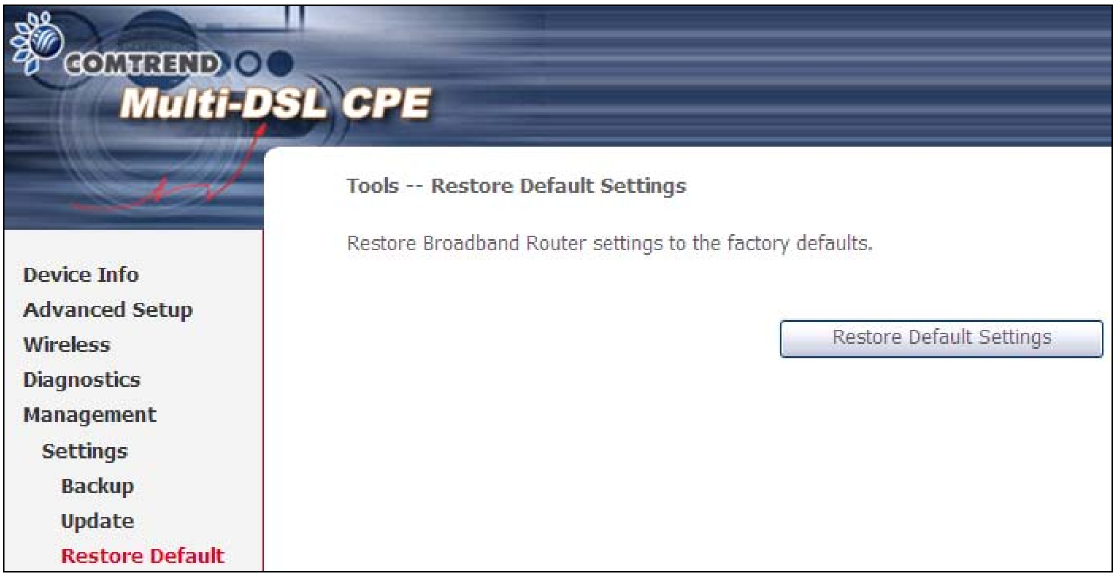
Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

8.1.3 Restore Default

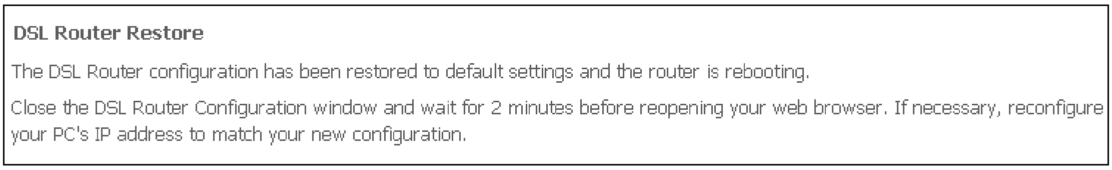
Click **Restore Default Settings** to restore factory default settings.



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

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



DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

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.

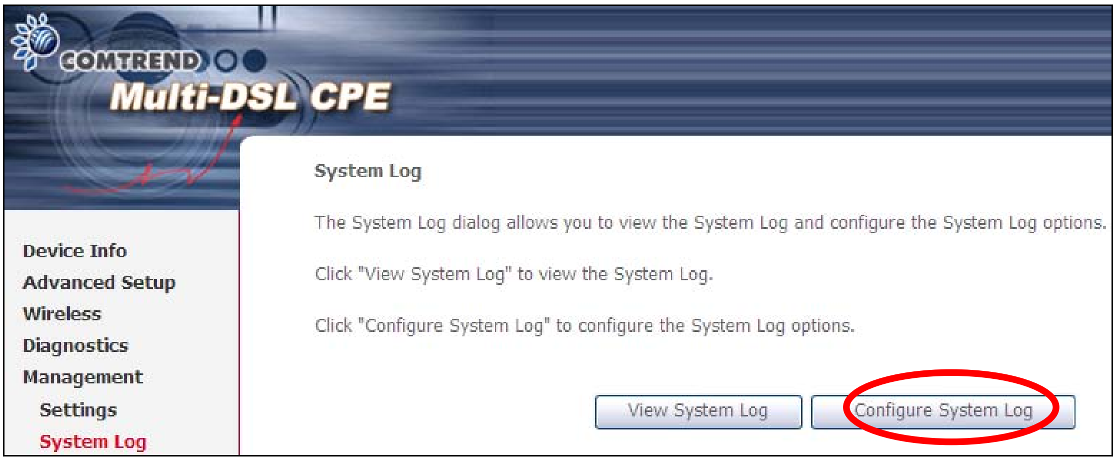
NOTE:	This entry has the same effect as the **Reset** button. The CT-5374 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

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**).



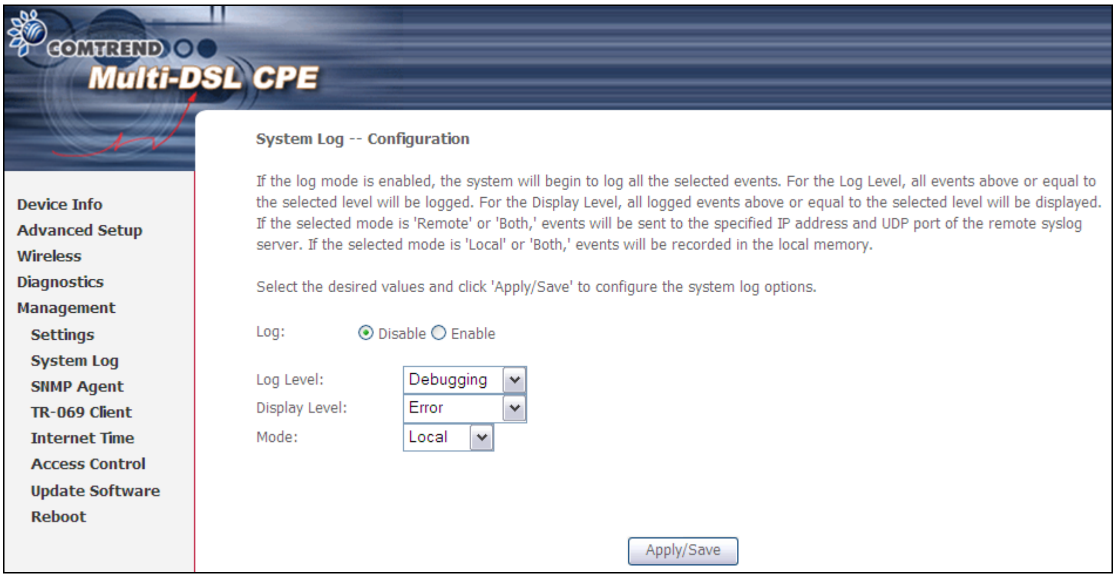
System Log

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

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

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

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



System Log -- Configuration

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

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

Log: ● Disable ○ Enable

Log Level: Debugging

Display Level: Error

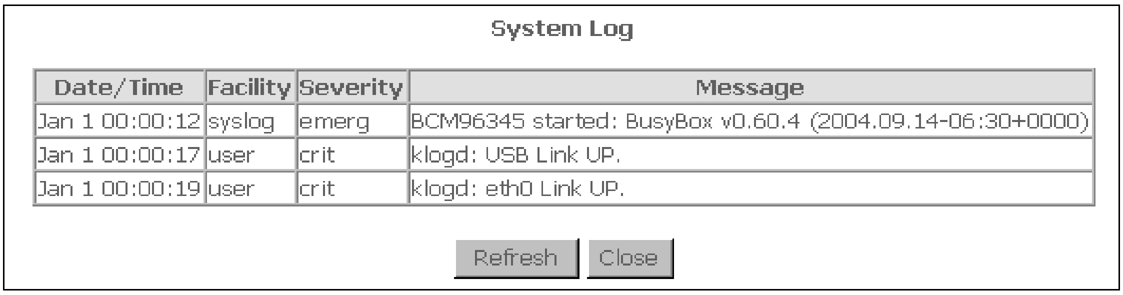
Mode: Local

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	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 CT-5374 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. The log levels are defined as follows: • 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 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.
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.

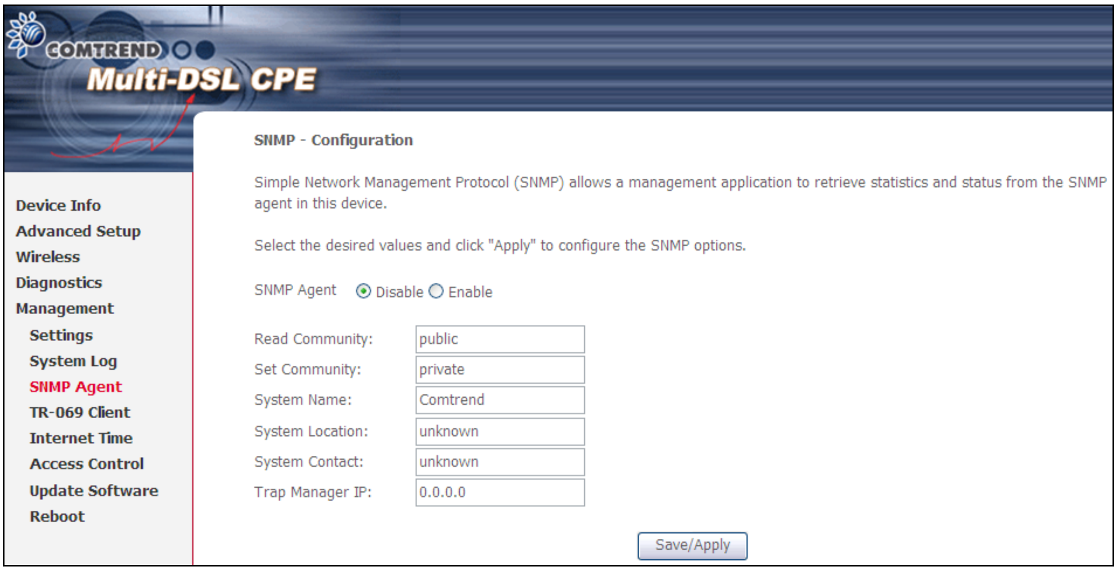


System Log

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 SNMP Agent

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



SNMP - Configuration

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

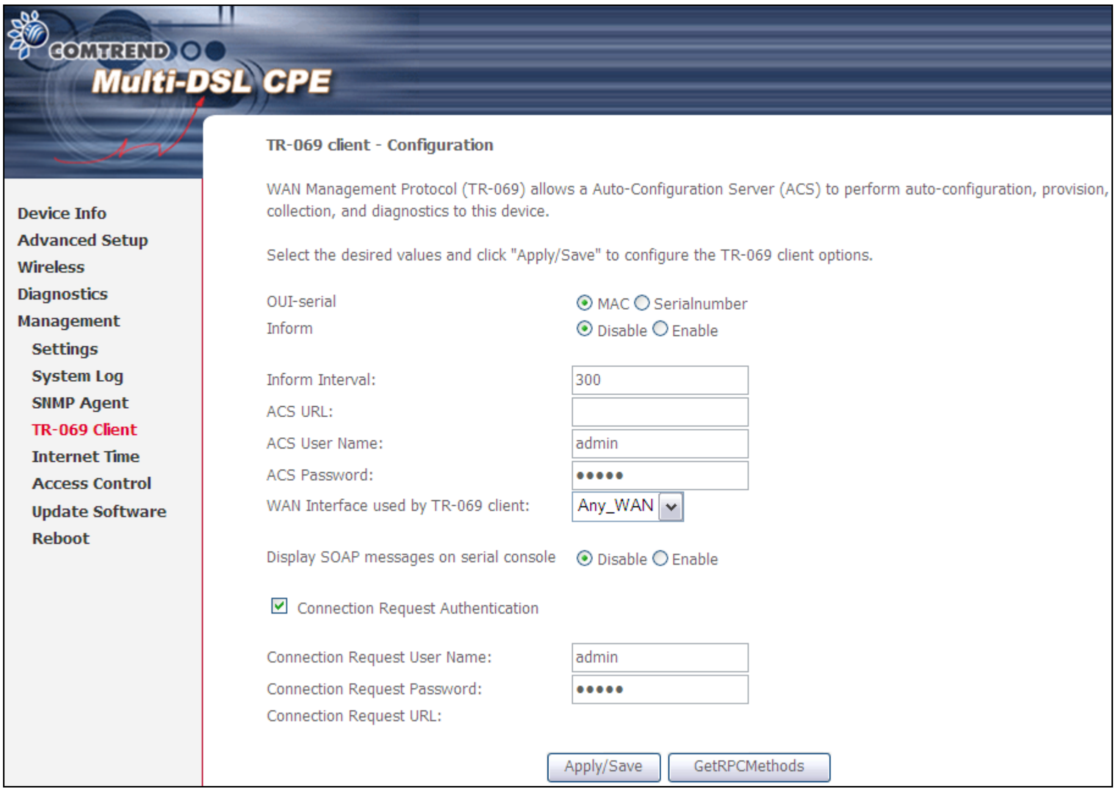
Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ● Disable ○ Enable

Read Community:	public
Set Community:	private
System Name:	Comtrend
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

8.4 TR-069 Client

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



TR-069 client - Configuration

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

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

OUI-serial ● MAC ○ Serialnumber
Inform ● Disable ○ Enable

Inform Interval: 300
ACS URL:
ACS User Name: admin
ACS Password: •••••
WAN Interface used by TR-069 client: Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name: admin
Connection Request Password: •••••
Connection Request URL:

The table below is provided for ease of reference.

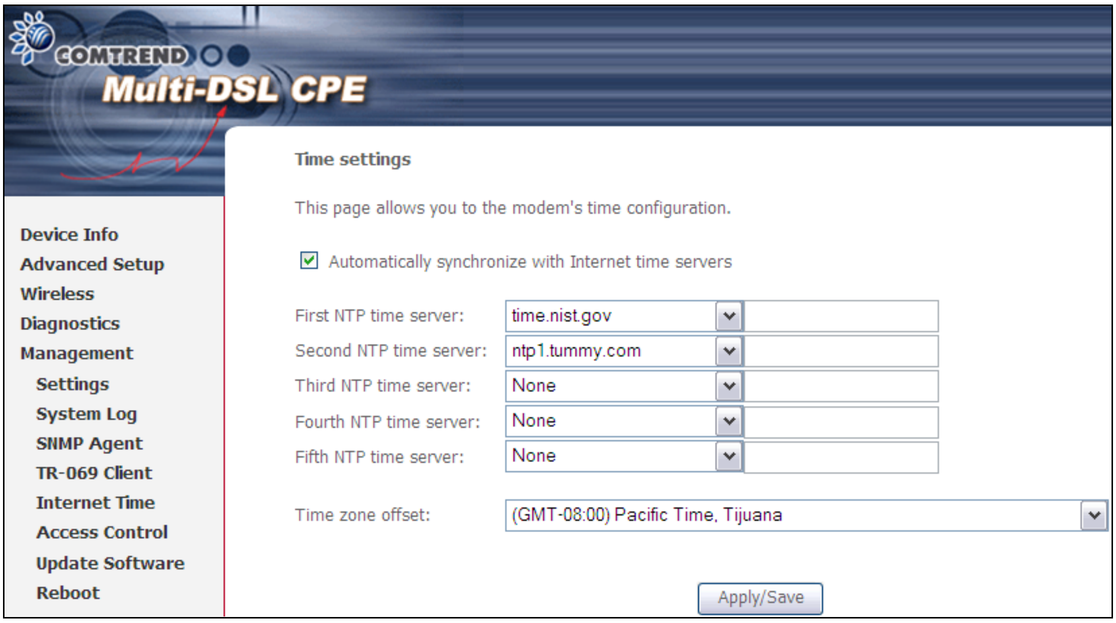
Option	Description
OUI-serial	Organizationally unique identifier of the device manufacturer. MAC address is set by default as the identifier to ACS.
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the 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 ☑ 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 CT-5374.

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.

8.5 Internet Time

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



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov

Second NTP time server: ntp1.tummy.com

Third NTP time server: None

Fourth NTP time server: None

Fifth NTP time server: None

Time zone offset: (GMT-08:00) Pacific Time, Tijuana

NOTE: Internet Time must be activated to use 5.7 Parental Control).
In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

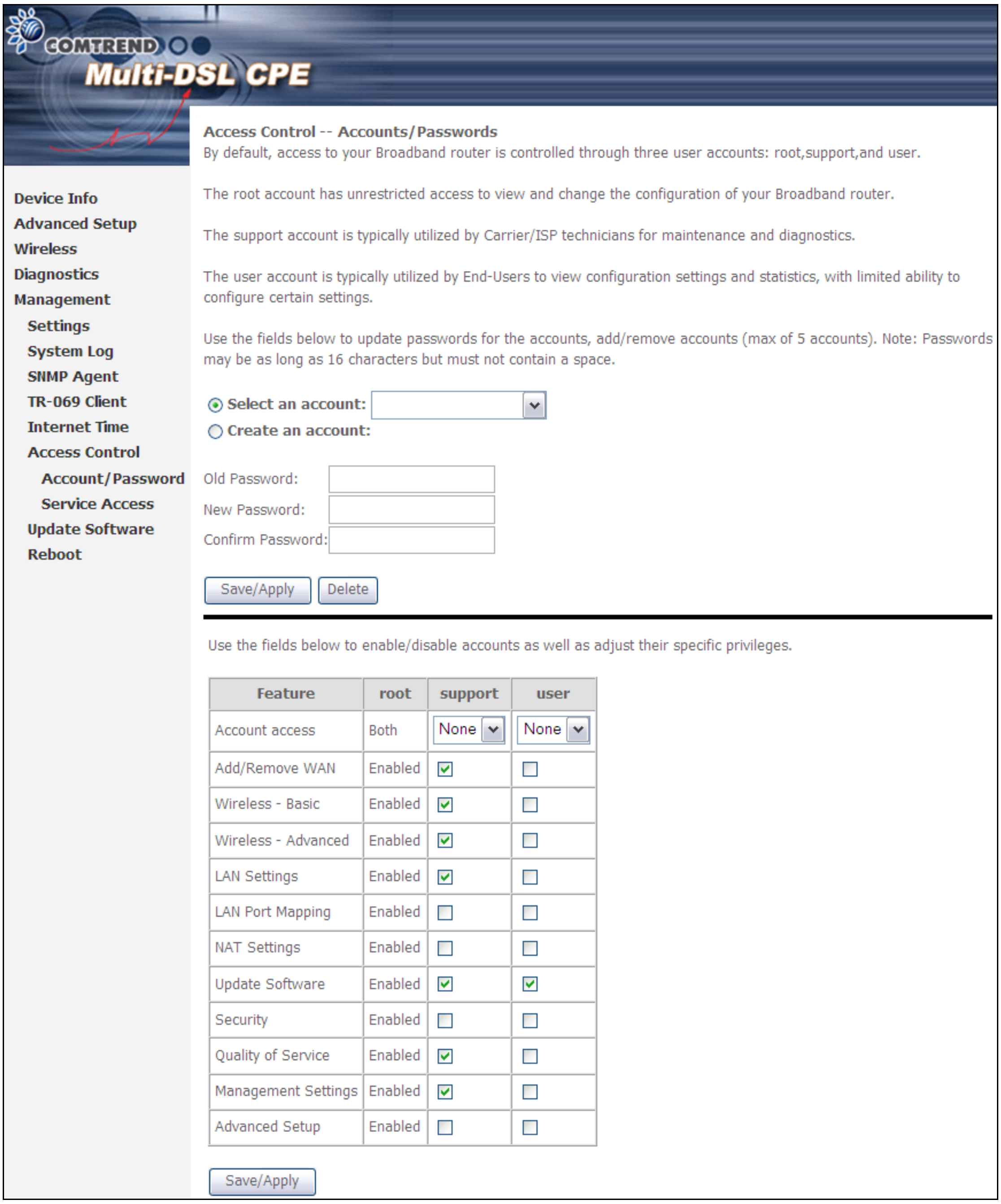
8.6 Access Control

8.6.1 Account/Password

This screen is used to configure the user account access passwords for the device. Access to the CT-5374 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.



Access Control -- Accounts/Passwords

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

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

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

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

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

● Select an account:

○ Create an account:

Old Password:

New Password:

Confirm Password:

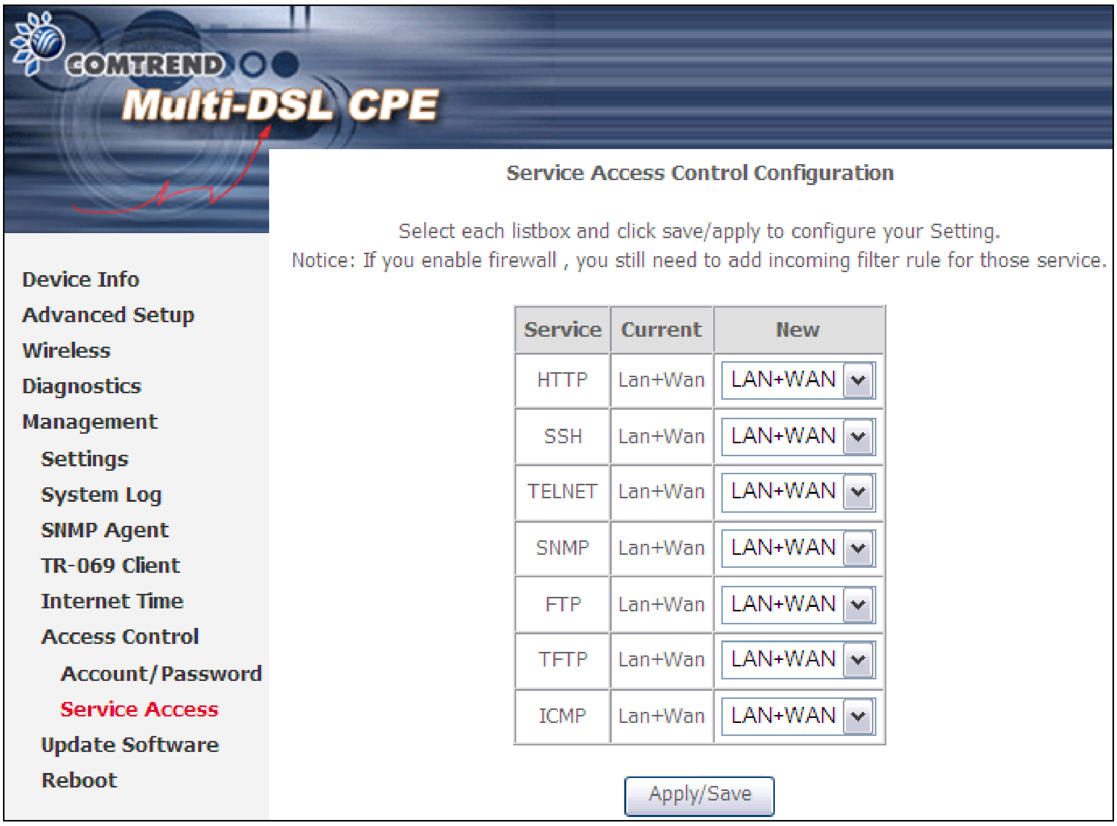
Use the fields below to enable/disable accounts as well as adjust their specific privileges.

Feature	root	support	user
Account access	Both	None	None
Add/Remove WAN	Enabled	☑	□
Wireless - Basic	Enabled	☑	□
Wireless - Advanced	Enabled	☑	□
LAN Settings	Enabled	☑	□
LAN Port Mapping	Enabled	□	□
NAT Settings	Enabled	□	□
Update Software	Enabled	☑	☑
Security	Enabled	□	□
Quality of Service	Enabled	☑	□
Management Settings	Enabled	☑	□
Advanced Setup	Enabled	□	□

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

8.6.2 Service Access

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



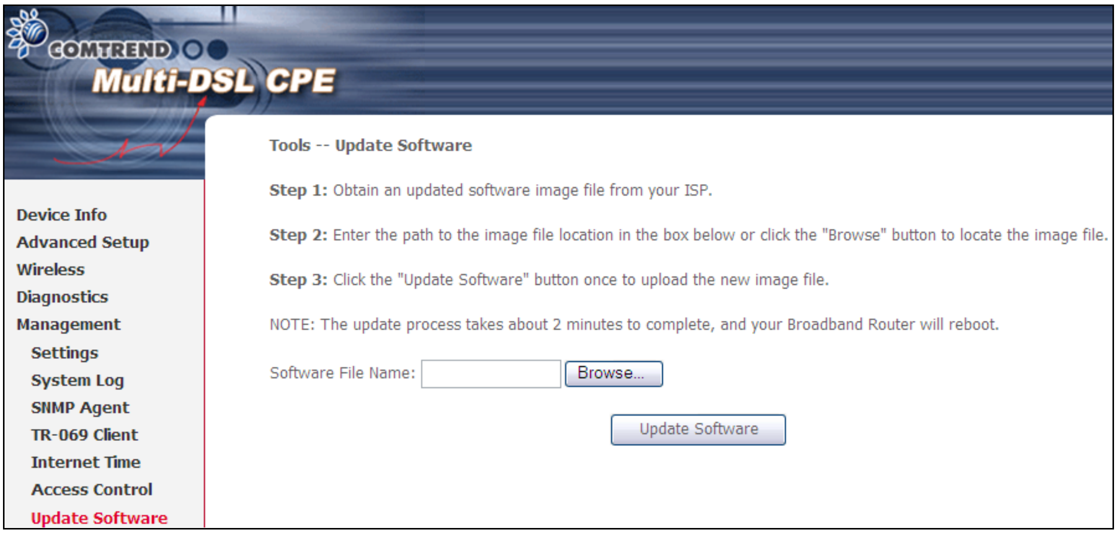
Service Access Control Configuration

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

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

8.7 Update Software

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



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.

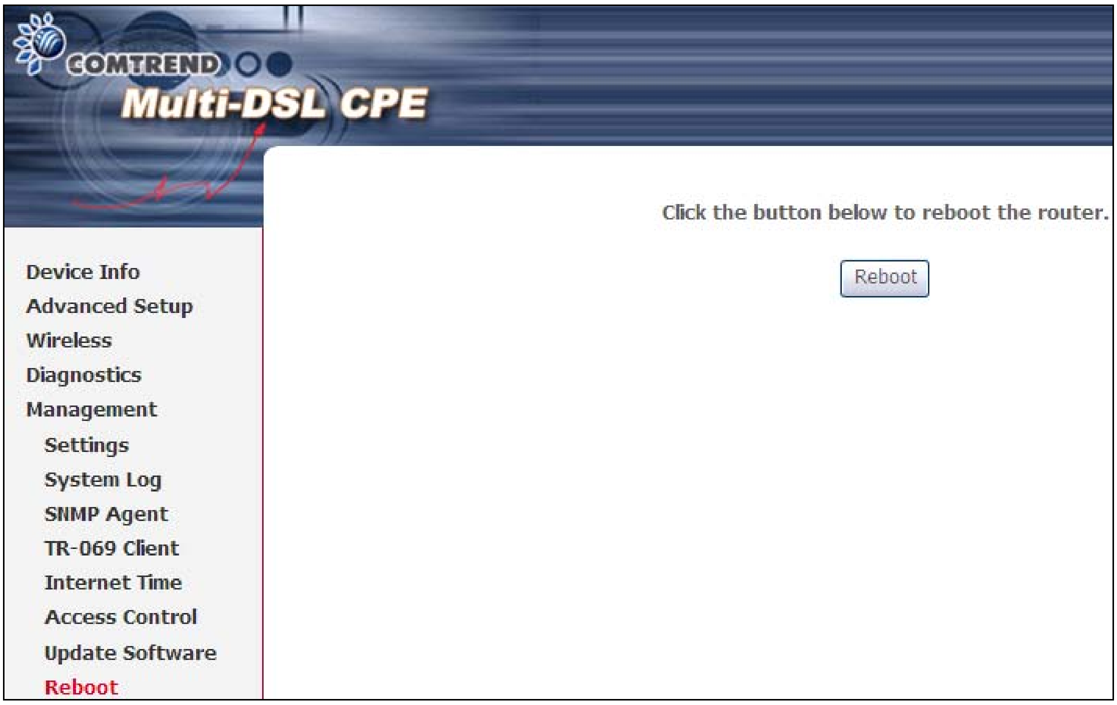
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

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 Chapter 4 Device Information screen with the firmware version installed, to confirm the installation was successful.

8.8 Reboot

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



Click the button below to reboot the router.

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 CT-5374, 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)

ETHERNET LAN Ports (10/100Base-T)

Pin	Signal name	Signal definition
1	TXP	Transmit data (positive lead)
2	TXN	Transmit data (negative lead)
3	RXP	Receive data (positive lead)
4	NC	Not used
5	NC	Not used
6	RXN	Receive data (negative lead)
7	NC	Not used
8	NC	Not used

Table 1

Signals for ETHERNET WAN port (10/1001000Base-T)

Pin	Signal name	Signal definition
1	TRD+(0)	Transmit/Receive data 0 (positive lead)
2	TRD-(0)	Transmit/Receive data 0 (negative lead)
3	TRD+(1)	Transmit/Receive data 1 (positive lead)
4	TRD+(2)	Transmit/Receive data 2 (positive lead)
5	TRD-(2)	Transmit/Receive data 2 (negative lead)
6	TRD-(1)	Transmit/Receive data 1 (negative lead)
7	TRD+(3)	Transmit/Receive data 3 (positive lead)
8	TRD-(3)	Transmit/Receive data 3 (negative lead)

Table 2

Appendix C - Specifications

Hardware Interface

- RJ-11 X 1 for ADSL2+/VDSL2
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- RJ-45X 1 for ETH WAN, (10/100/1000 BaseT auto-sense)
- Reset Button X 1
- WPS Button X 1
- Wi-Fi On/Off Button X 1
- Wi-Fi Antennas X 2
- Power Switch X 1
- USB Host X 1

WAN Interface

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

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

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u
- MDI/MDX support Yes
- Multiple Subnets on LAN

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
- 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)
- Up to 300Mbps data rate
- Multiple BSSID
- MAC address filtering, WDS, WEP, WPA, WPA2, IEEE 802.1x
- 10,25,50,100mW@22MHz channel bandwidth output power level can be selected according to the environment
- Optional Afterburner mode (Turbo mode)***

ATM Attributes

- RFC 2684 (RFC 1483) Bridge/Route;
- RFC 2516 (PPPoE); RFC 2364 (PPPoA); RFC 1577 (IPoA)
- Support up to 16 PVCs
- AAL type AAL5
- ATM service class UBR/CBR/VBR-rt/VBR-nrt
- ATM UNI support UNI 3.1/4.0
- OAM F4/F5

PTM Attributes

- Dual Latency.................Yes

Management

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

Networking Protocols

- RFC2684 VC-MUX, LLC/SNAP encapsulations for bridged or routed packet
- RFC2364 PPP over AAL5
- IPoA, PPPoA, PPPoE, Multiple PPPoE sessions on single PVC, PPPoE pass-through
- PPPoE filtering of on-PPPoE packets between WAN and LAN
- Transparent bridging between all LAN and WAN interfaces
- 802.1p/802.1q VLAN support
- Spanning Tree Algorithm
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP, DHCP Server/Client/Relay,
- DNS Relay, Dynamic DNS,
- IPv6 subset

Security Functions

- PAP, CHAP, Packet and MAC address filtering, SSH,
- VPN termination
- Configurable security login level

QoS

- Packet level QoS classification rules,
- Priority queuing using ATM TX queues,
- IP TOS/Precedence,
- 802.1p marking,
- DiffServ DSCP marking
- Src/dest MAC addresses classification

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Day-time Parental Control
- URI/URL filtering
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- TCP/IP/Port/interface filtering rules Support both incoming and outgoing filtering

NAT/NAPT

- Support Port Triggering and Port forwarding
- Symmetric port-overloading NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Support DMZ host
- Virtual Server
- VPN Passthrough (PPTP, L2TP, IPSec)

Application Layer Gateway (ALG)

SIP, H.323, Yahoo messenger, ICQ, RealPlayer, Net2Phone, NetMeeting, MSN, X-box, Microsoft DirectX games and etc.

Power Supply ....Input: 100 - 240 Vac
Output: 12 Vdc / 1.5 A

Environment Condition

Operating temperature ....0 ~ 50 degrees Celsius
Relative humidity ....5 ~ 95% (non-condensing)

Dimensions ....205 mm (W) x 48 mm (H) x 145 mm (D)

Certifications.................................. FCC Part 15, FCC Part 68

Kit Weight

(1*CT-5374, 1*RJ14 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 1.0 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

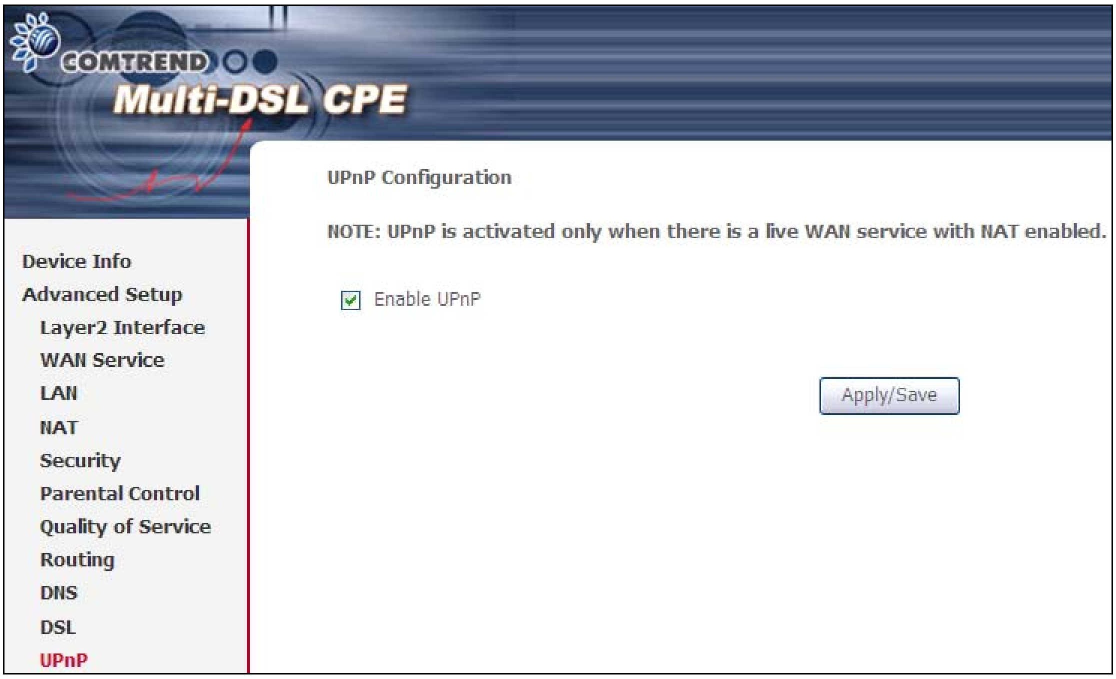
For WAN access, type: putty -ssh -l support *WAN IP address*

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.

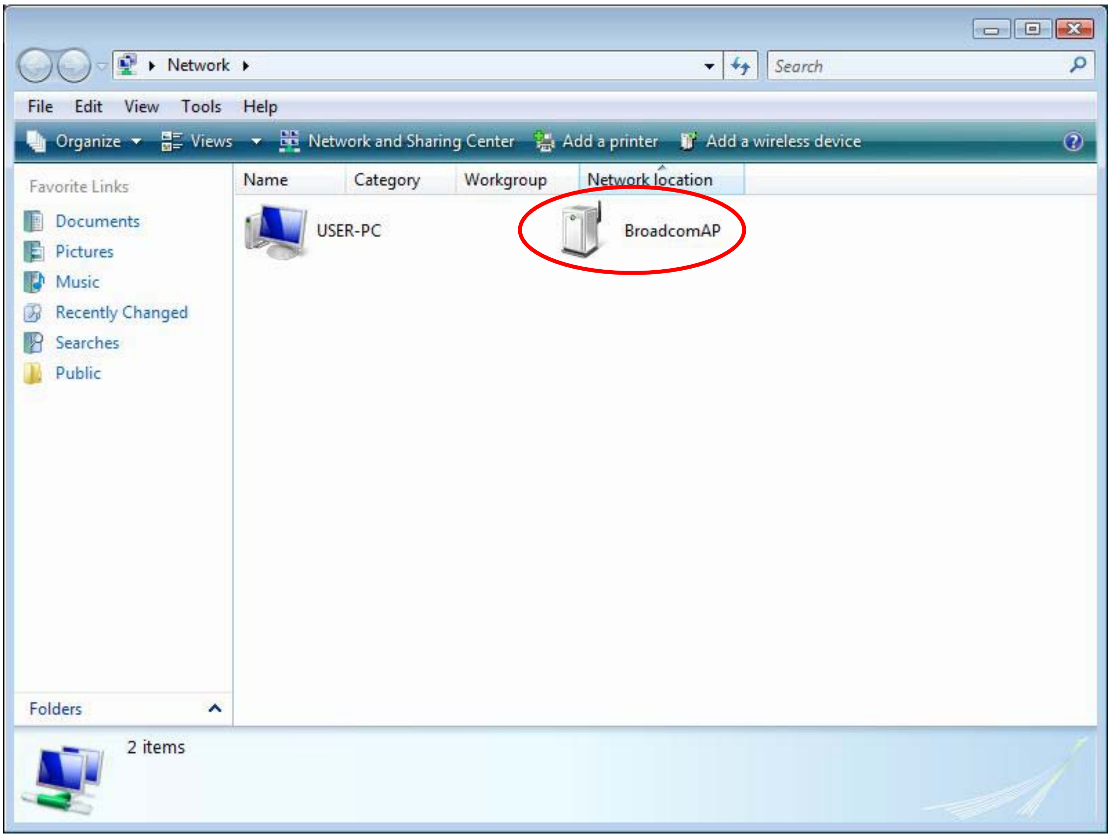


UPnP Configuration

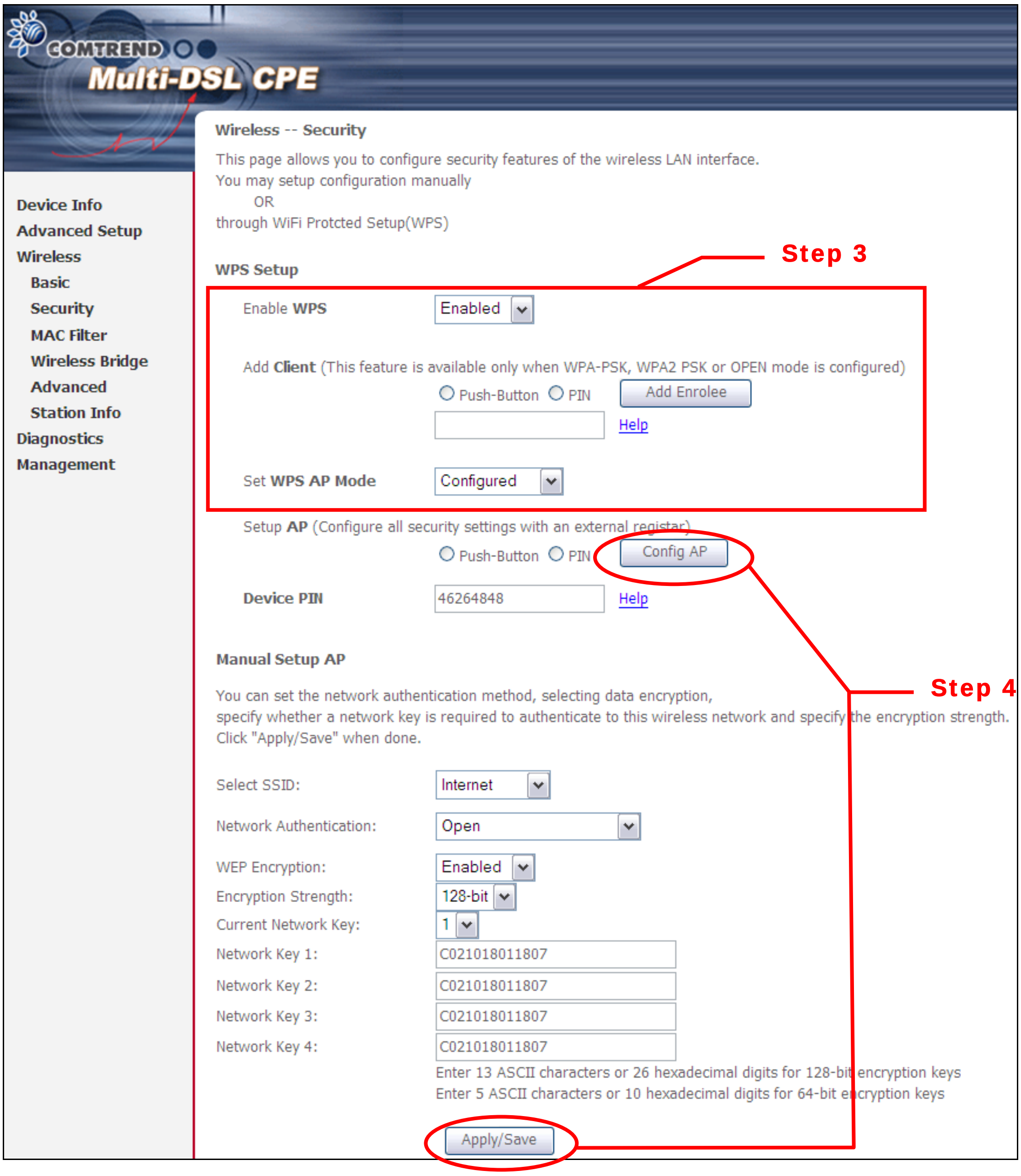
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ Enable UPnP

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



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



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)

WPS Setup

Enable **WPS**: Enabled

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
○ Push-Button ○ PIN

Set **WPS AP Mode**: Configured

Setup **AP** (Configure all security settings with an external registar)
○ Push-Button ○ PIN

Device PIN: 46264848

Manual Setup AP

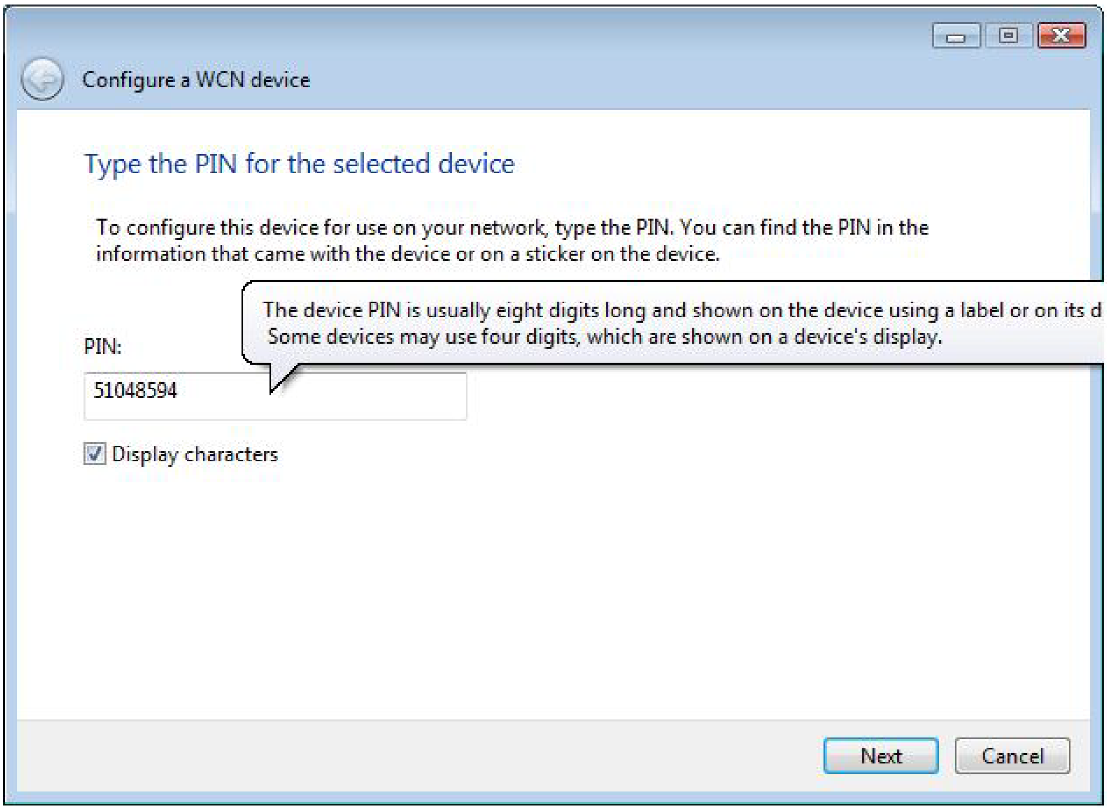
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	Internet
Network Authentication:	Open
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	1
Network Key 1:	C021018011807
Network Key 2:	C021018011807
Network Key 3:	C021018011807
Network Key 4:	C021018011807

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

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. When the screen returns, press the **Config AP** button, as shown above.

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**.



Configure a WCN device

Type the PIN for the selected device

To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

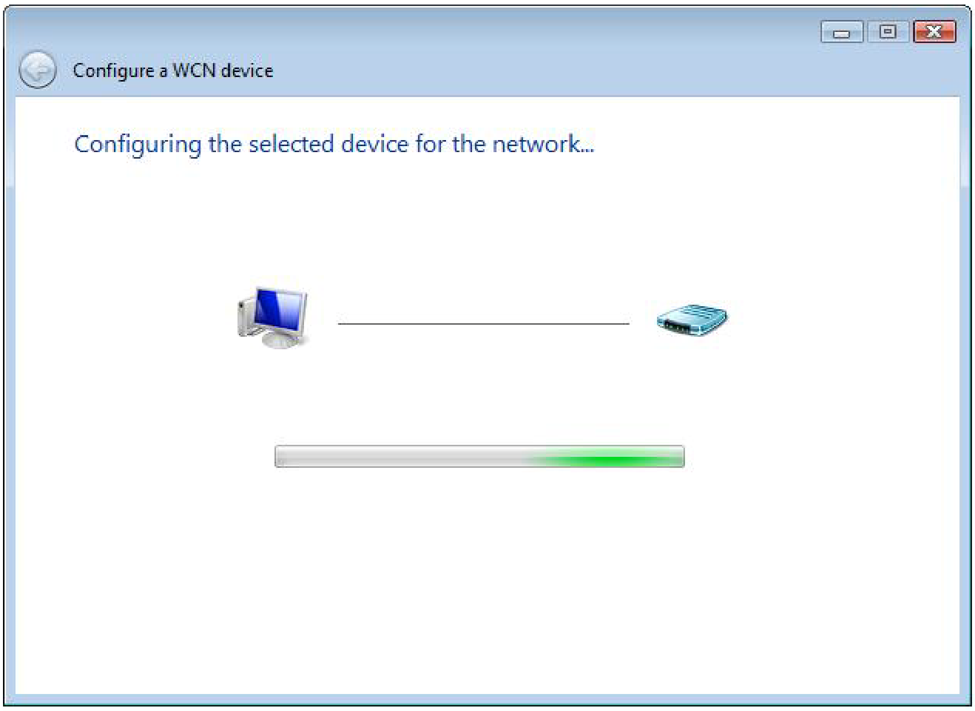
The device PIN is usually eight digits long and shown on the device using a label or on its d
Some devices may use four digits, which are shown on a device's display.

PIN:

51048594

☑ Display characters

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



Configure a WCN device

Configuring the selected device for the network...

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

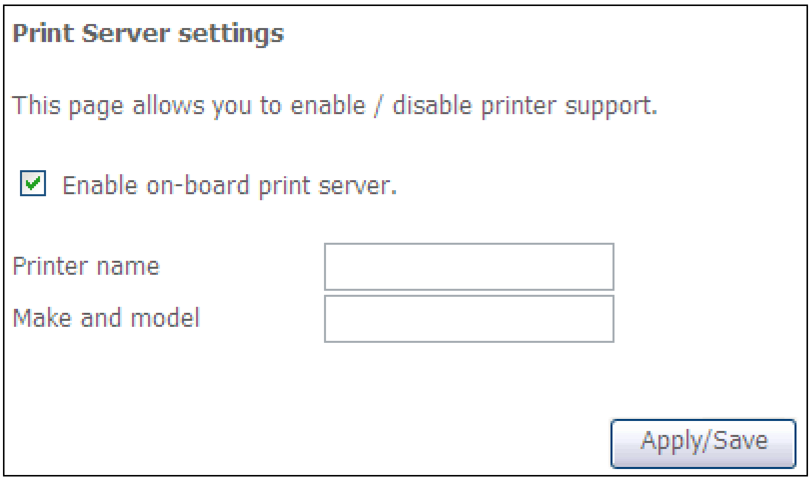
Appendix F - Printer Server

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

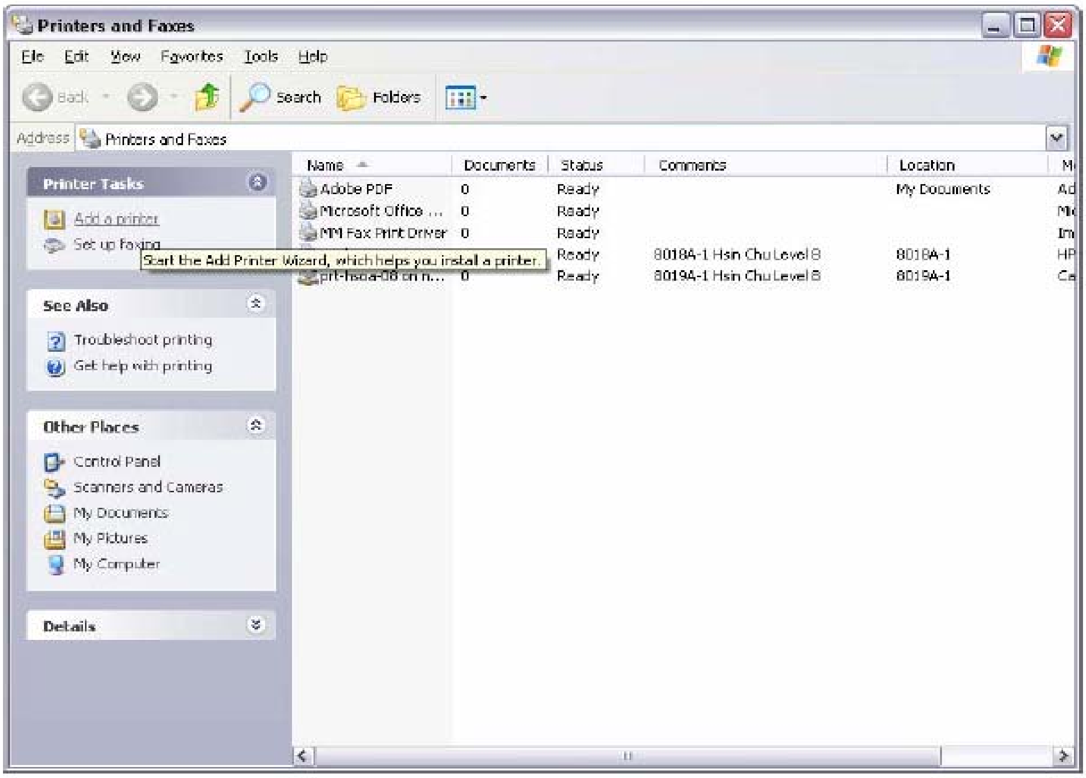
This page allows you to enable / disable printer support.

☑ Enable on-board print server.

Printer name

Make and model

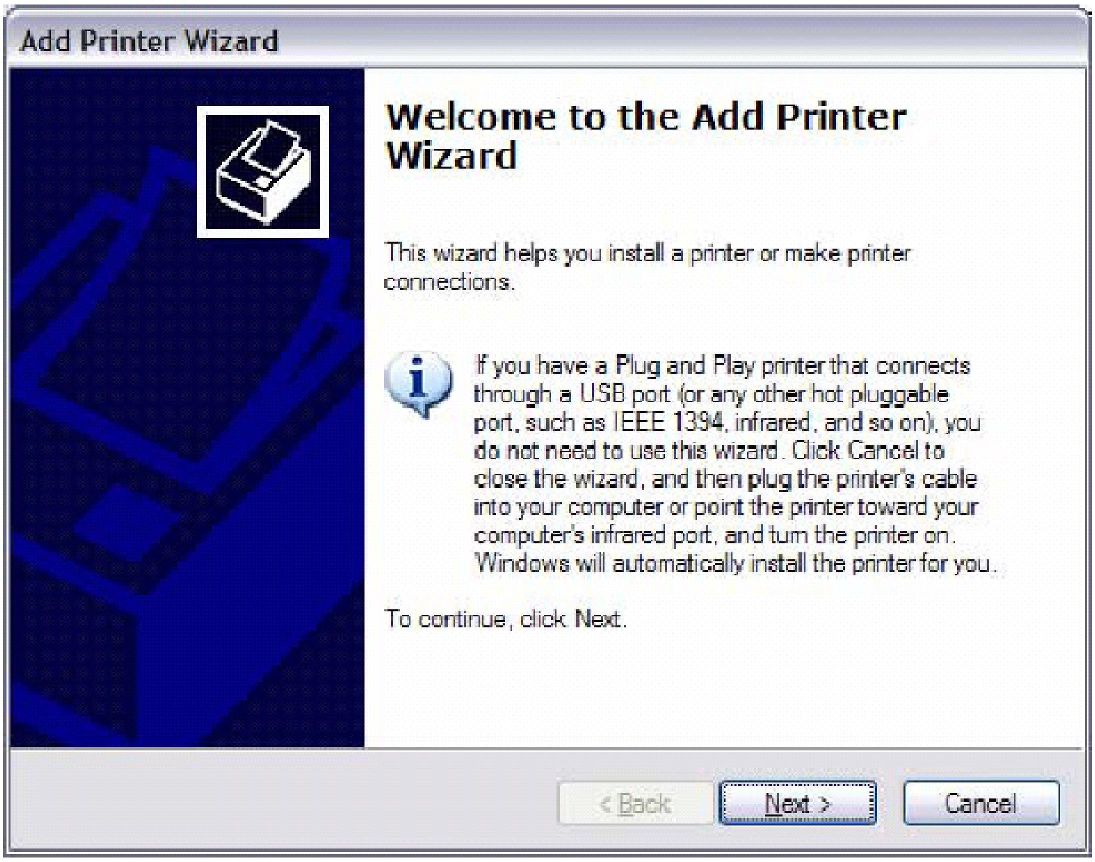
STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



Start the Add Printer Wizard, which helps you install a printer.

Name	Documents	Status	Comments	Location	M
Adobe PDF	0	Ready		My Documents	Ad
Microsoft Office ...	0	Ready			Mi
MM Fax Print Driver	0	Ready			Im
		Ready	8018A-1 Hsin Chu Level 8	8018A-1	HP
prt-hsoa-08 on n...	0	Ready	8019A-1 Hsin Chu Level 8	8019A-1	Ca

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



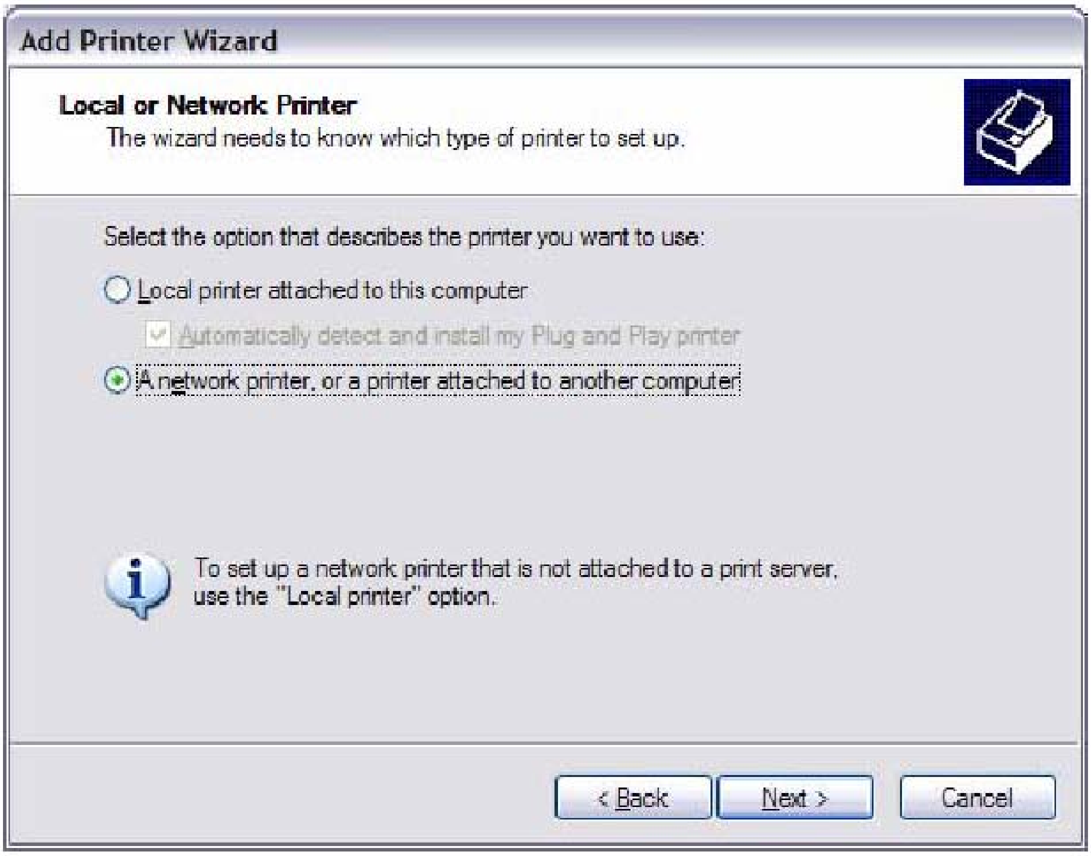
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

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


Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

○ Local printer attached to this computer

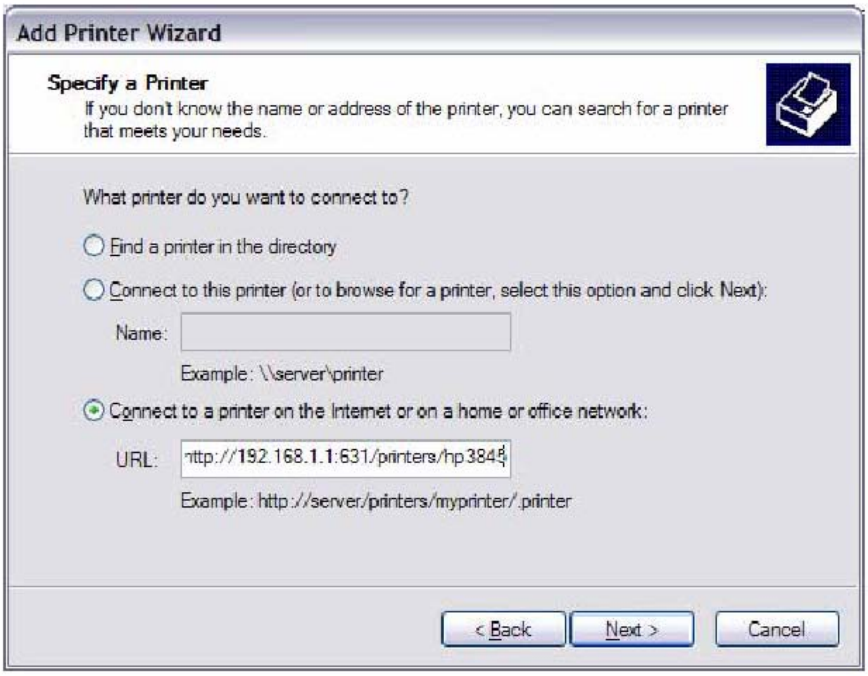
☑ Automatically detect and install my Plug and Play printer

● A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

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.


Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Find a printer in the directory

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

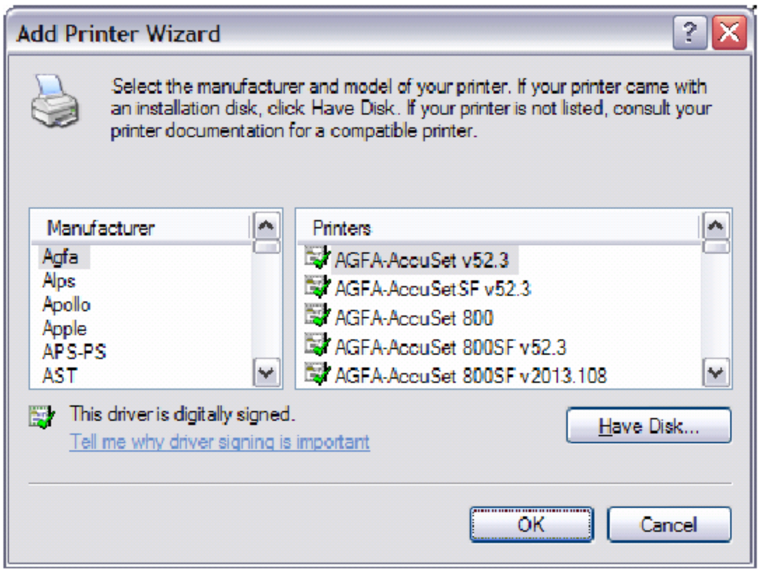
Example: \\server\printer

● Connect to a printer on the Internet or on a home or office network:

URL: nttp://192.168.1.1:631/printers/hp3845

Example: http://server/printers/myprinter/.printer

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

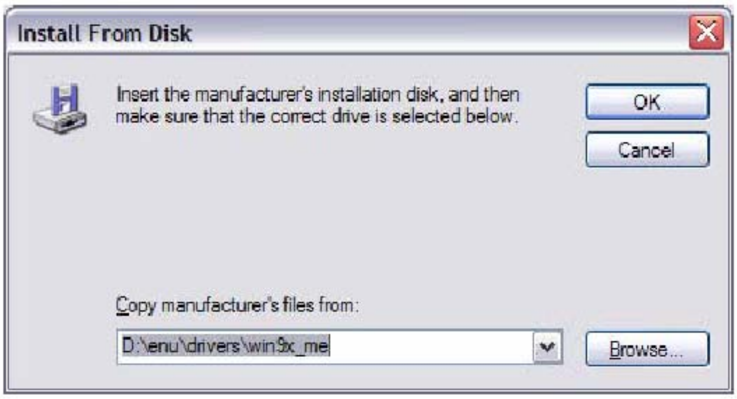


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSet SF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	AGFA-AccuSet 800SF v2013.108
AST	

This driver is digitally signed.
Tell me why driver signing is important

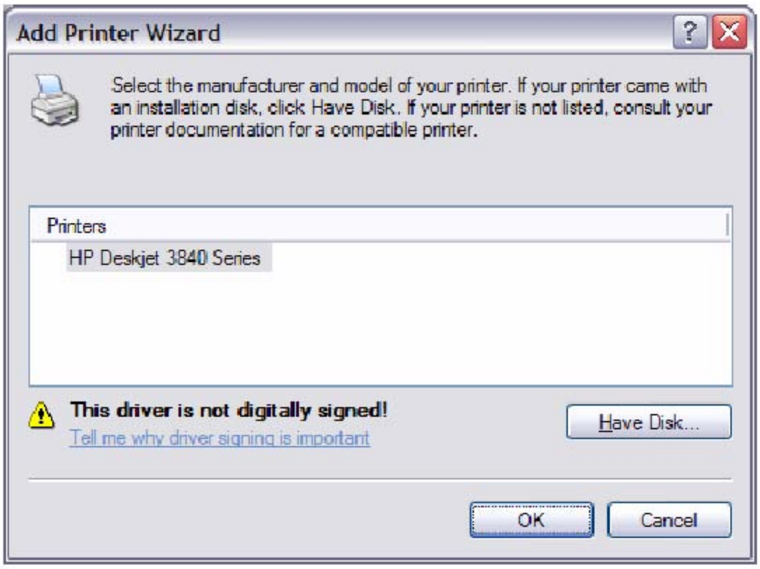
STEP 7: Select driver file directory on CD-ROM and click **OK.**



Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:
D:\enu\drivers\win9x_me

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

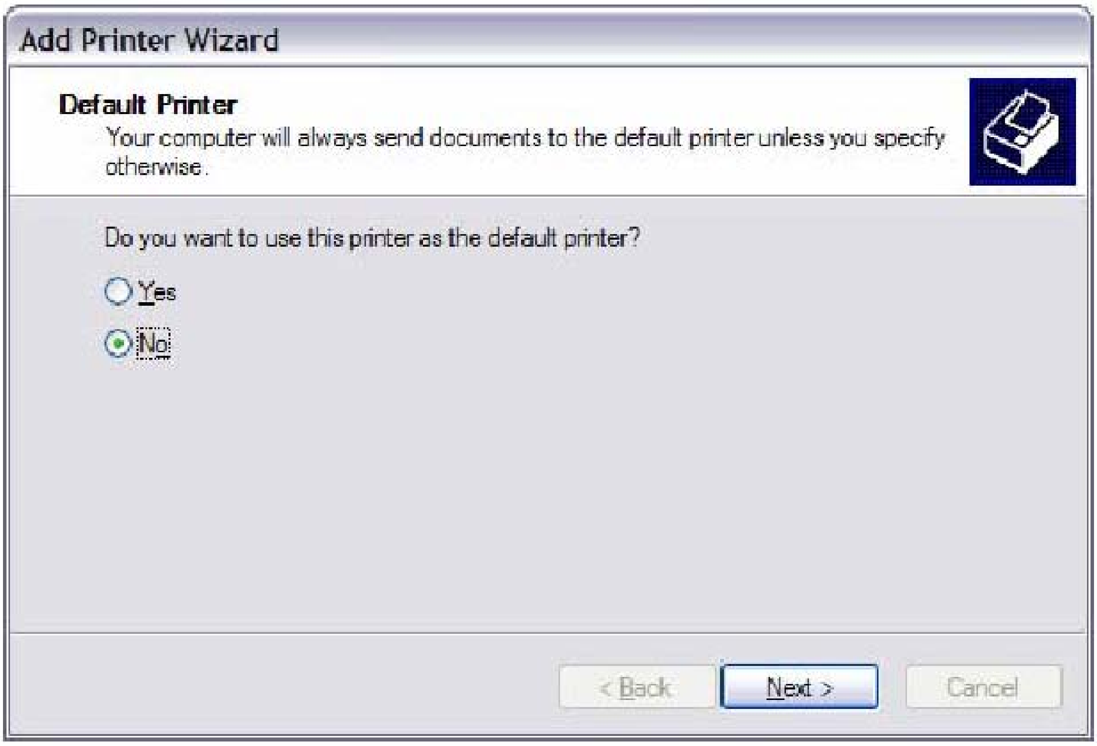


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Printers
HP Deskjet 3840 Series

This driver is not digitally signed!
Tell me why driver signing is important

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



Add Printer Wizard

Default Printer

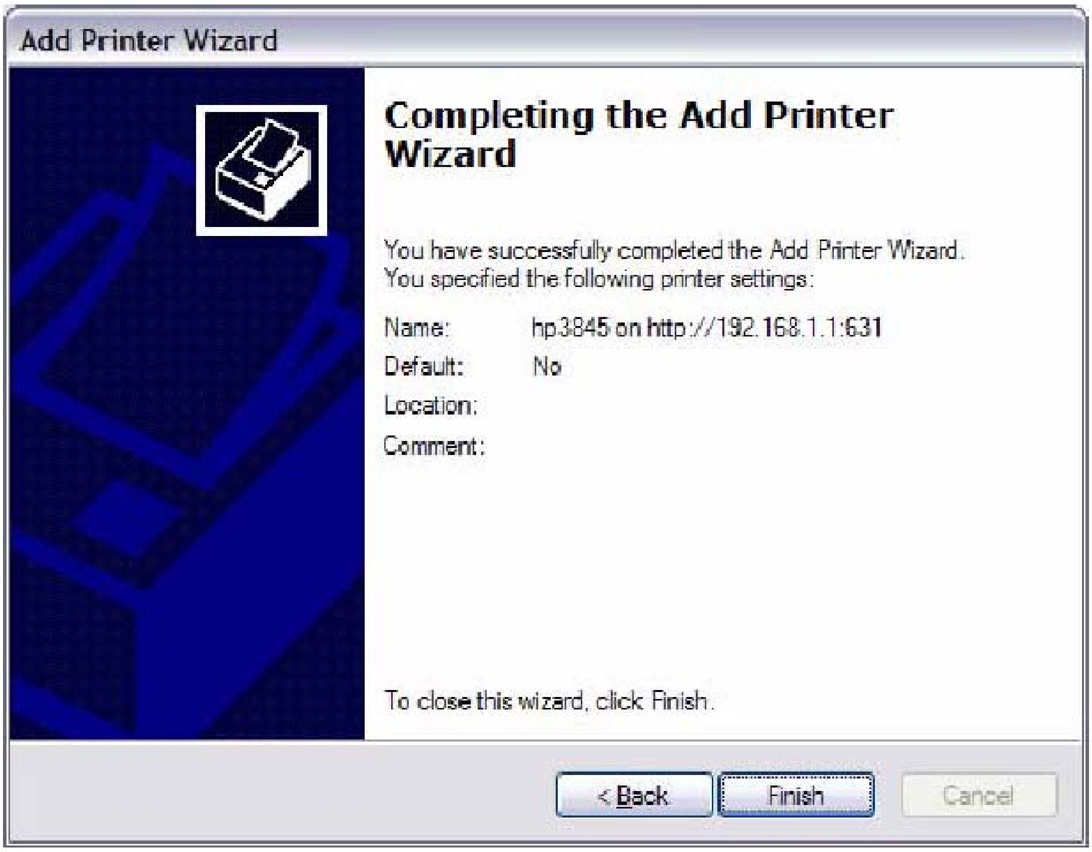
Your computer will always send documents to the default printer unless you specify otherwise.

Do you want to use this printer as the default printer?

○ Yes

● No

STEP 10: Click Finish.



Add Printer Wizard

Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard. You specified the following printer settings:

Name: hp3845 on http://192.168.1.1:631

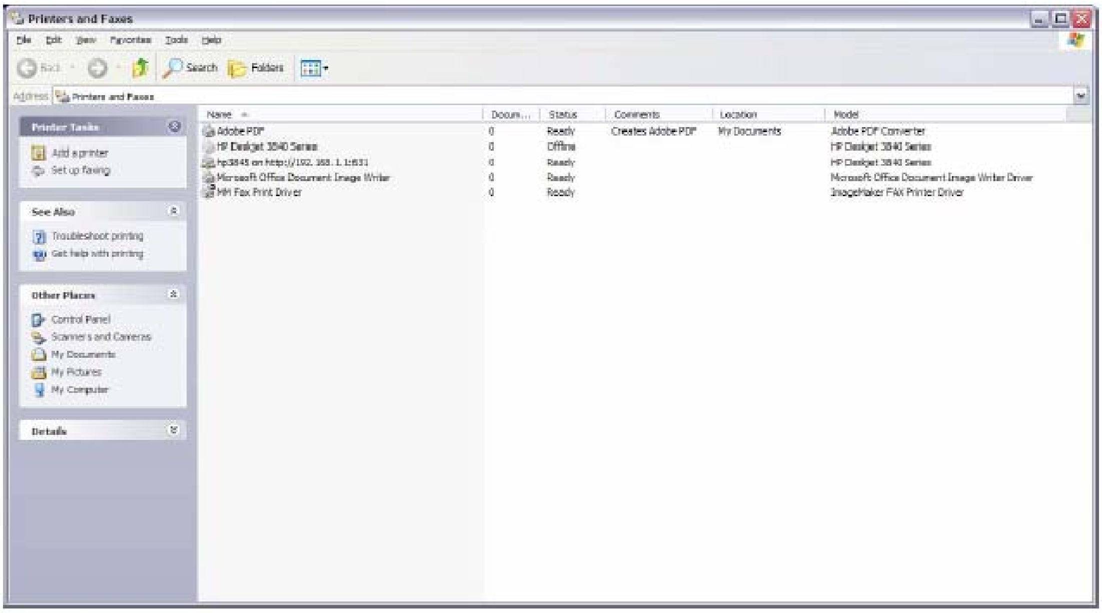
Default: No

Location:

Comment:

To close this wizard, click Finish.

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



Name	Docum...	Status	Comments	Location	Model
Adobe PDF	0	Ready	Creates Adobe PDF	My Documents	Adobe PDF Converter
HP Deskjet 3840 Series	0	Offline			HP Deskjet 3840 Series
hp3845 on http://192.168.1.1:631	0	Ready			HP Deskjet 3840 Series
Microsoft Office Document Image Writer	0	Ready			Microsoft Office Document Image Writer Driver
MM Fax Print Driver	0	Ready			ImageMaker FAX Printer Driver

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.

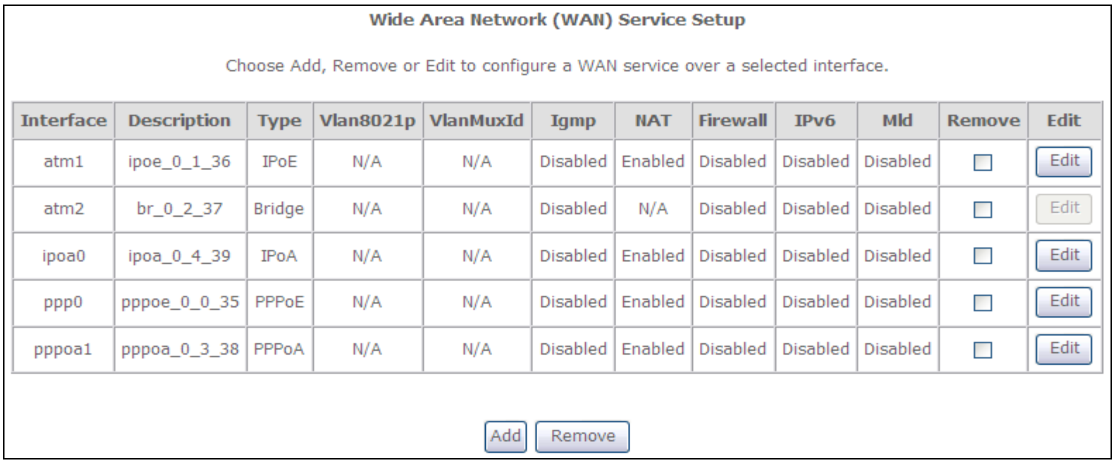
The following sections describe each stage in turn.

G1 ~ Layer 2 Interfaces

Every layer2 interface operates in one of two modes: Default or VLAN Mux. 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.

DEFAULT MODE

In this mode there is a 1:1 relationship between interfaces and WAN connections, in that an interface in default mode supports just one connection. However, unlike the multiple connection modes described below, it supports all five connection types. The figure below shows the five connection types available in ATM default mode.



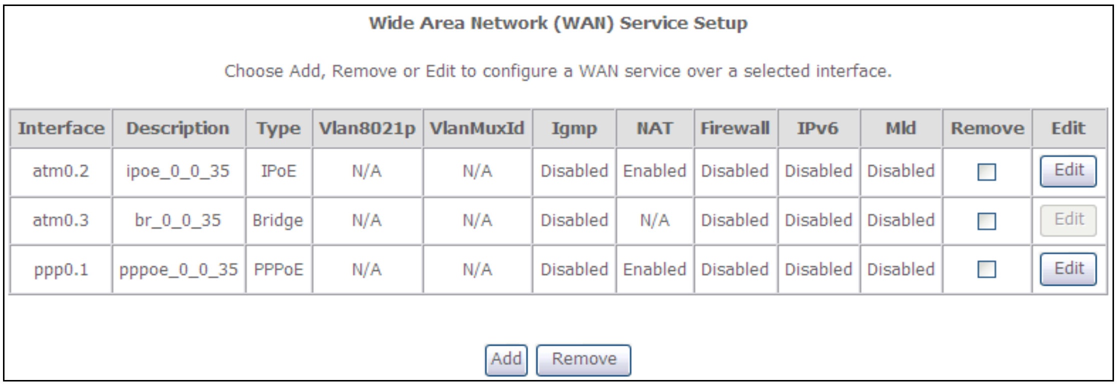
Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm1	ipoe_0_1_36	IPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
atm2	br_0_2_37	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	□	Edit
ipoa0	ipoa_0_4_39	IPoA	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
pppoa1	pppoa_0_3_38	PPPoA	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit

VLAN MUX MODE

This mode uses VLAN tags to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not. The figure below shows multiple connections over a single VLAN Mux interface.



Wide Area Network (WAN) Service Setup

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

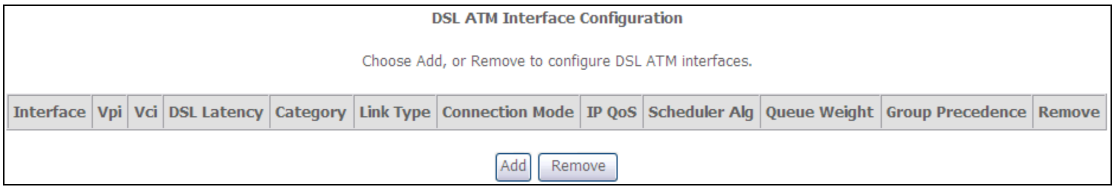
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.2	ipoe_0_0_35	IPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
atm0.3	br_0_0_35	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	□	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit

G1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE:	The CT-5374 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.

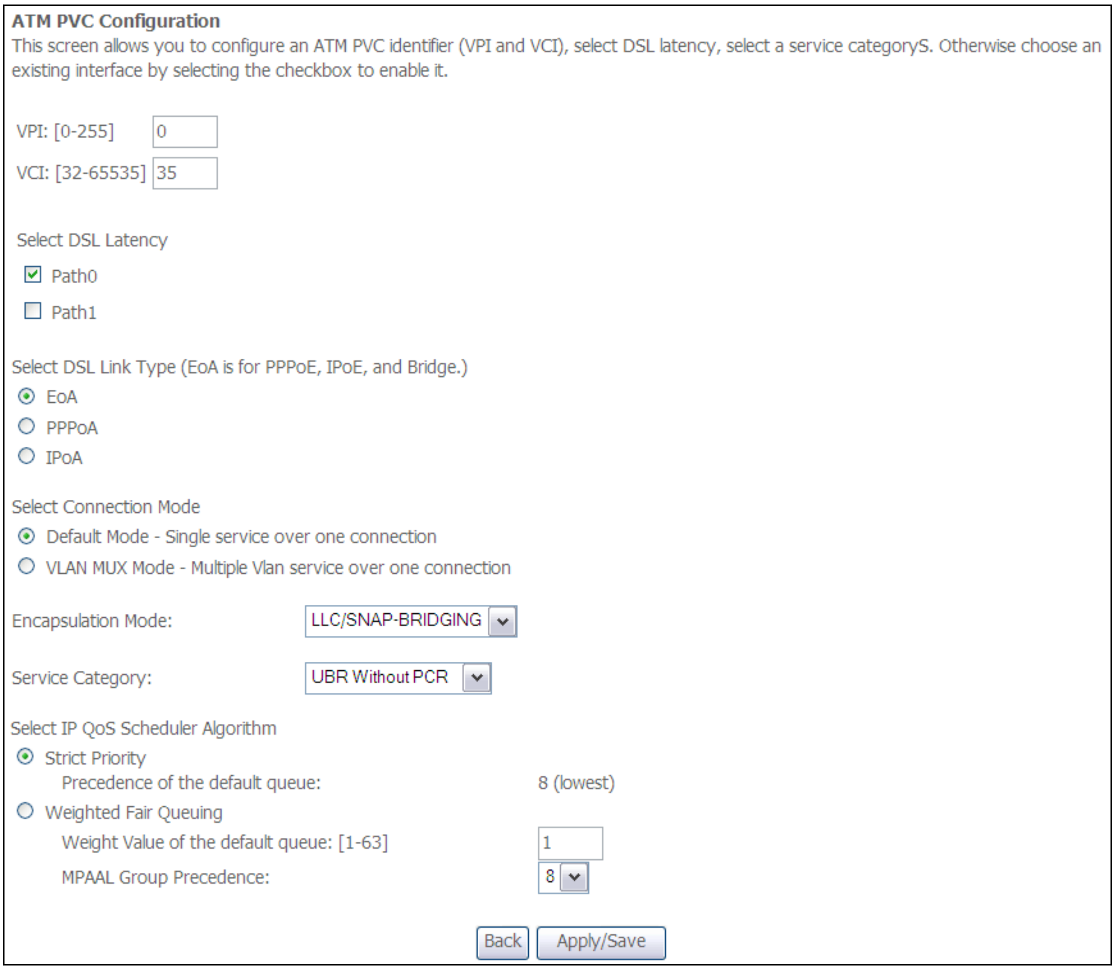
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
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
QoS	Quality of Service (QoS) status
Scheduler Alg	The algorithm used to schedule the dequeue behavior.
Queue Weight	The weight of the specified queue.
Group Precedence	The Precedence of the specified group.
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 an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0

VCI: [32-65535] 35

Select DSL Latency

☑ Path0

□ Path1

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

● EoA

○ PPPoA

○ IPoA

Select Connection Mode

● Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select IP QoS Scheduler Algorithm

● Strict Priority

Precedence of the default queue: 8 (lowest)

○ Weighted Fair Queuing

Weight Value of the default queue: [1-63] 1

MPAAL Group Precedence: 8

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

The table below shows xDSL Link Type availability with each Connection Mode.

	xDSL Link Type		
Connection Mode	EoA*	PPPoA	IPoA
Default Mode	OK	OK	OK
VLAN Mux Mode	OK	X	X

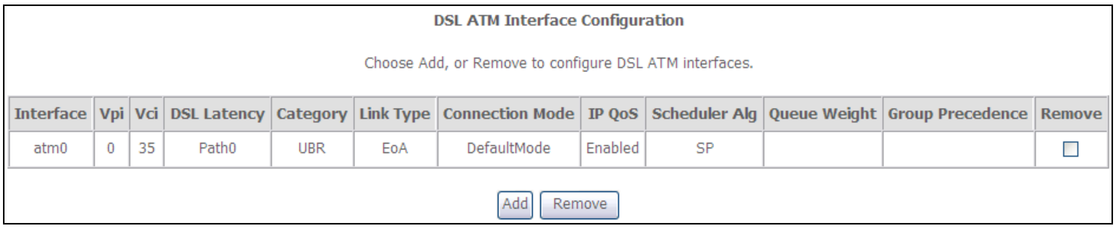
* EoA includes PPPoE, IPoE, and Bridge link types.

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	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			□

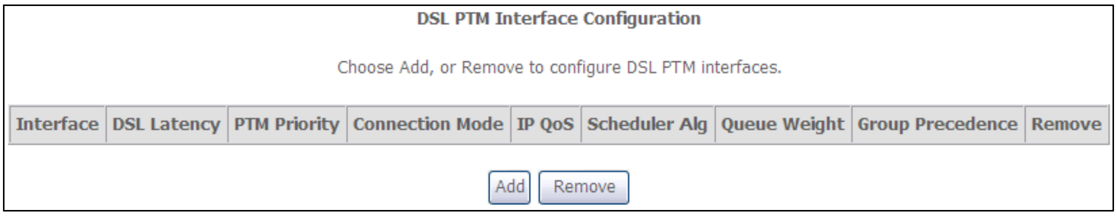
To add a WAN connection, go to section G2 ~ WAN Connections.

G1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The CT-5374 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.

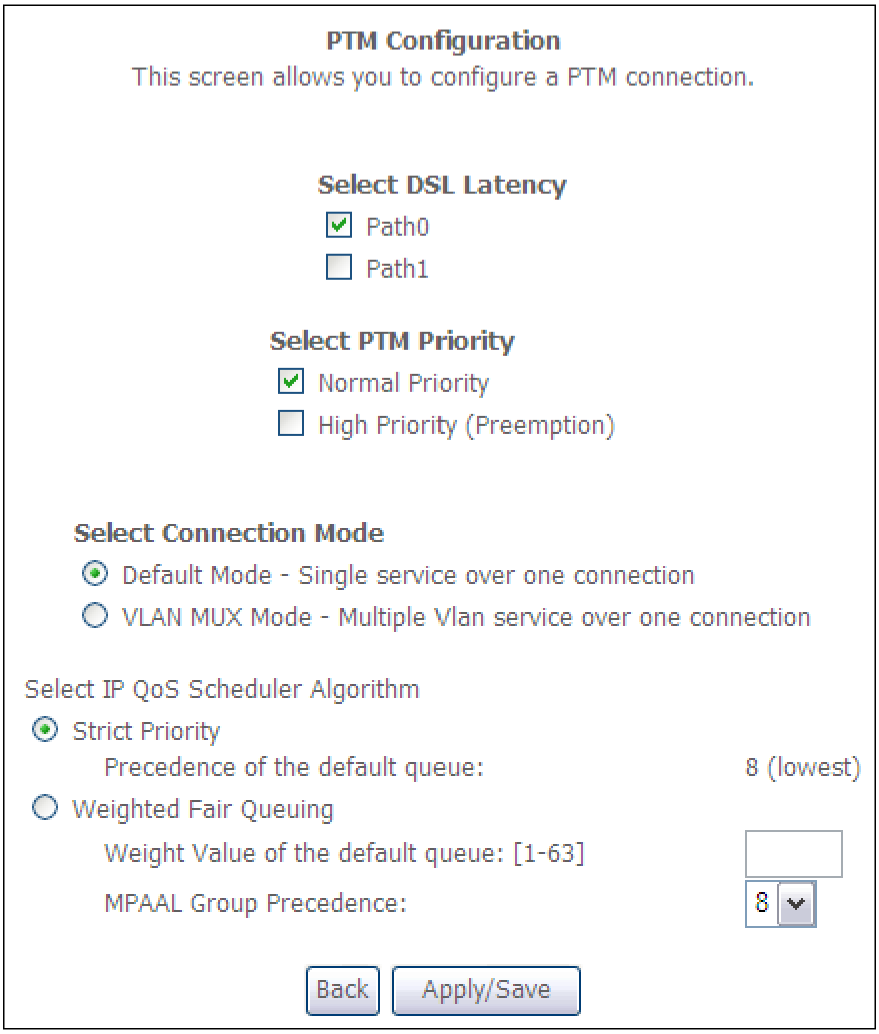
Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

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.
QoS	Quality of Service (QoS) status.
Scheduler Alg	The algorithm used to schedule the dequeue behavior.
Queue Weight	The weight of the specified queue.
Group Precedence	The Precedence of the specified group.
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 connection.

Select DSL Latency

☑ Path0

☐ Path1

Select PTM Priority

☑ Normal Priority

☐ High Priority (Preemption)

Select Connection Mode

● Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

Select IP QoS Scheduler Algorithm

● Strict Priority

Precedence of the default queue: 8 (lowest)

○ Weighted Fair Queuing

Weight Value of the default queue: [1-63]

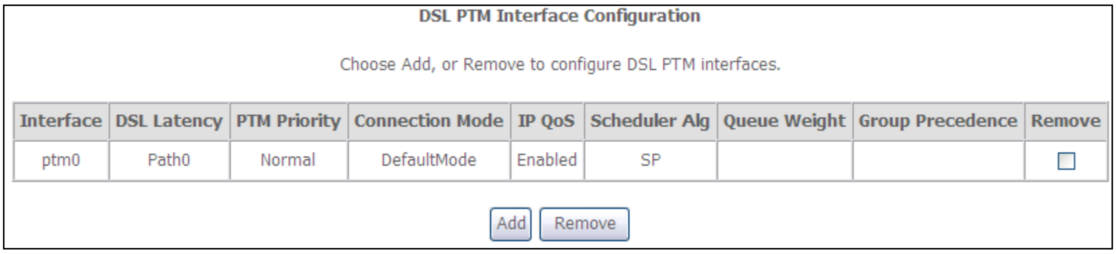
MPAAL Group Precedence: 8

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	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
ptm0	Path0	Normal	DefaultMode	Enabled	SP			☐

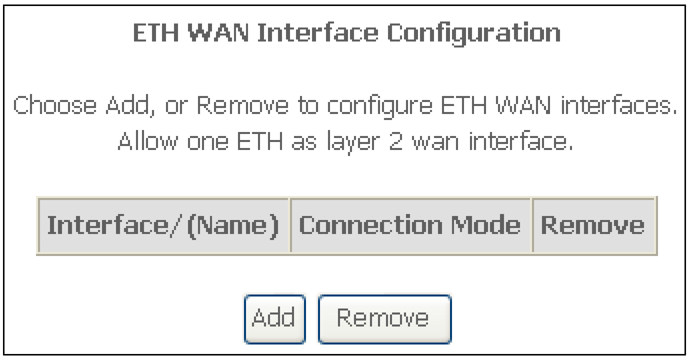
To add a WAN connection, go to section G2 ~ WAN Connections.

G1.3 Ethernet WAN Interface

Some models of the CT-5374 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.



ETH WAN Interface Configuration

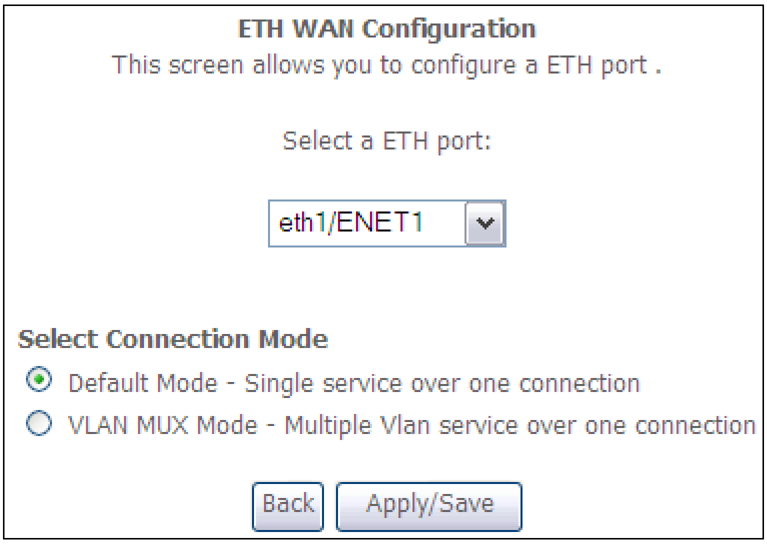
Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/ (Name)	Connection Mode	Remove

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
Remove	Select the checkbox and click **Remove** to remove the connection.

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



ETH WAN Configuration
This screen allows you to configure a ETH port .

Select a ETH port:

eth1/ENET1

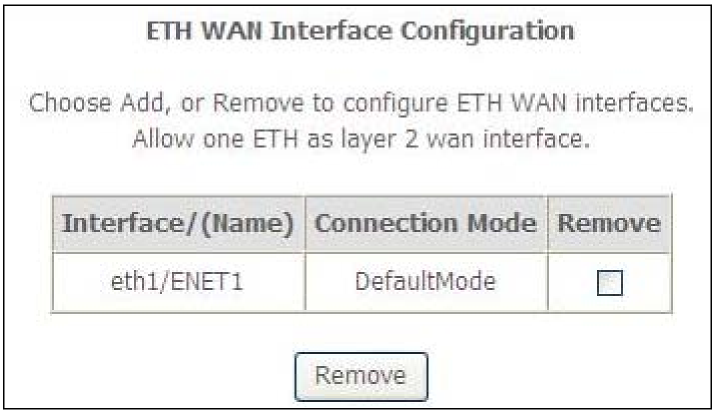
Select Connection Mode

● Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection

STEP 3: Select a Connection Mode from the options shown above.

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

The figure below shows an Ethernet WAN interface configured in Default Mode.



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/ENET1	DefaultMode	□

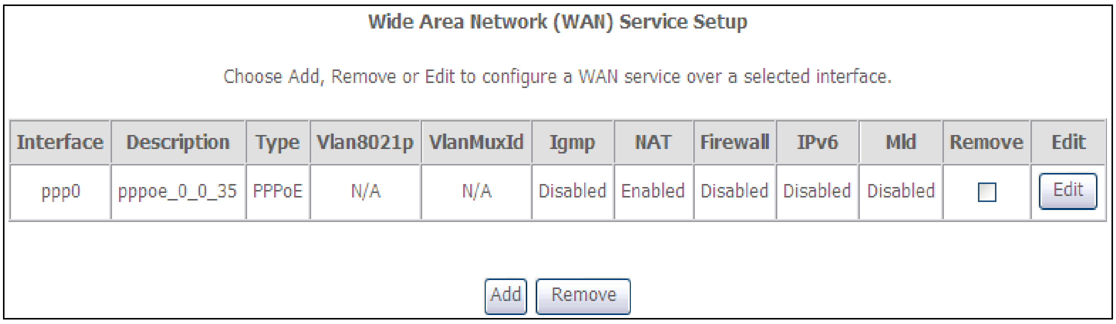
To add a WAN connection, go to section G2 ~ WAN Connections.

G2 ~ WAN Connections

In Default Mode, the CT-5374 supports one WAN connection for each interface, up to a maximum of 8 connections. VLAN Mux supports up to 16 connections.

To setup a WAN connection follow these instructions.

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

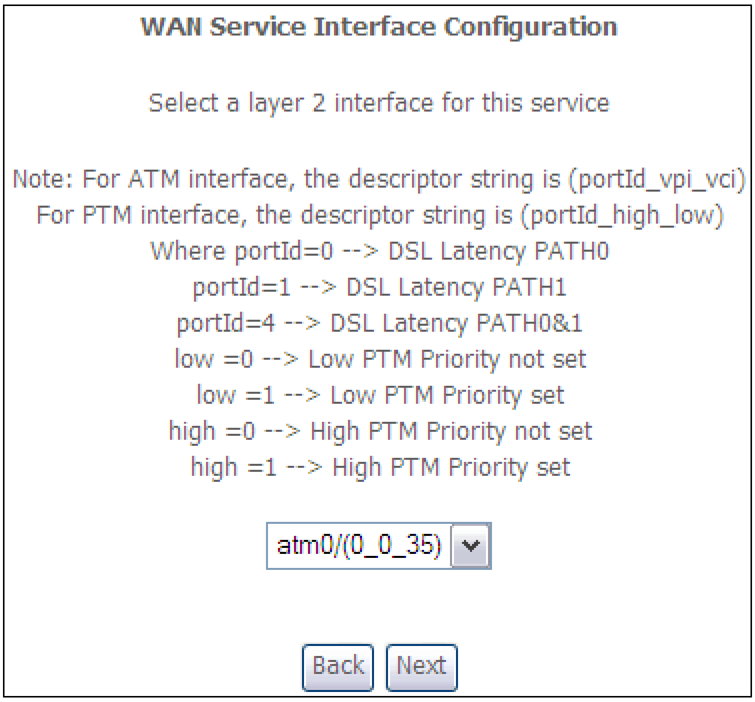


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit

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



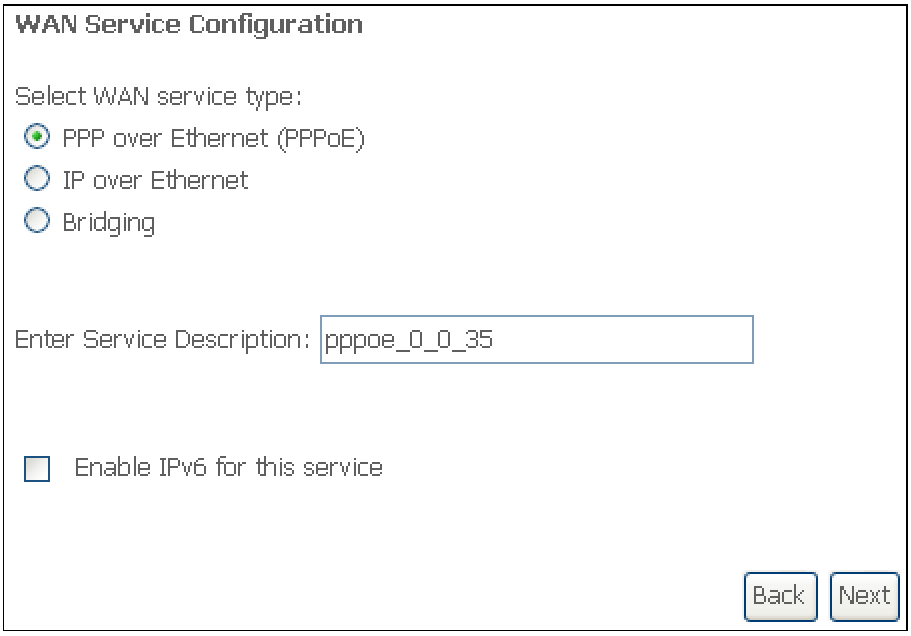
WAN Service Interface Configuration

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

atm0/(0_0_35)

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



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

○ IP over Ethernet

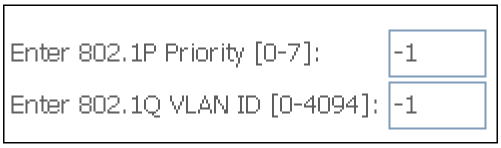
○ Bridging

Enter Service Description: pppoe_0_0_35

□ Enable IPv6 for this service

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]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

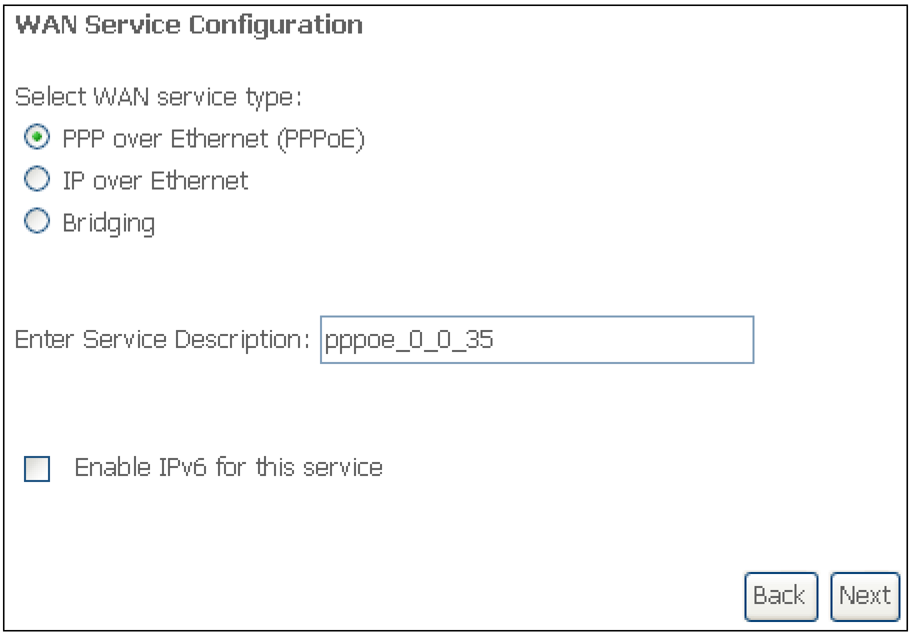
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For G2.1 PPP over ETHERNET (PPPoE), go to page 132.
(2) For G2.2 IP over ETHERNET (IPoE), go to page 137.
(3) For G2.3 Bridging, go to page 141.
(4) For G2.4 PPP over ATM (PPPoA), go to page 142.
(5) For G2.5 IP over ATM (IPoA), go to page 146.

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.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

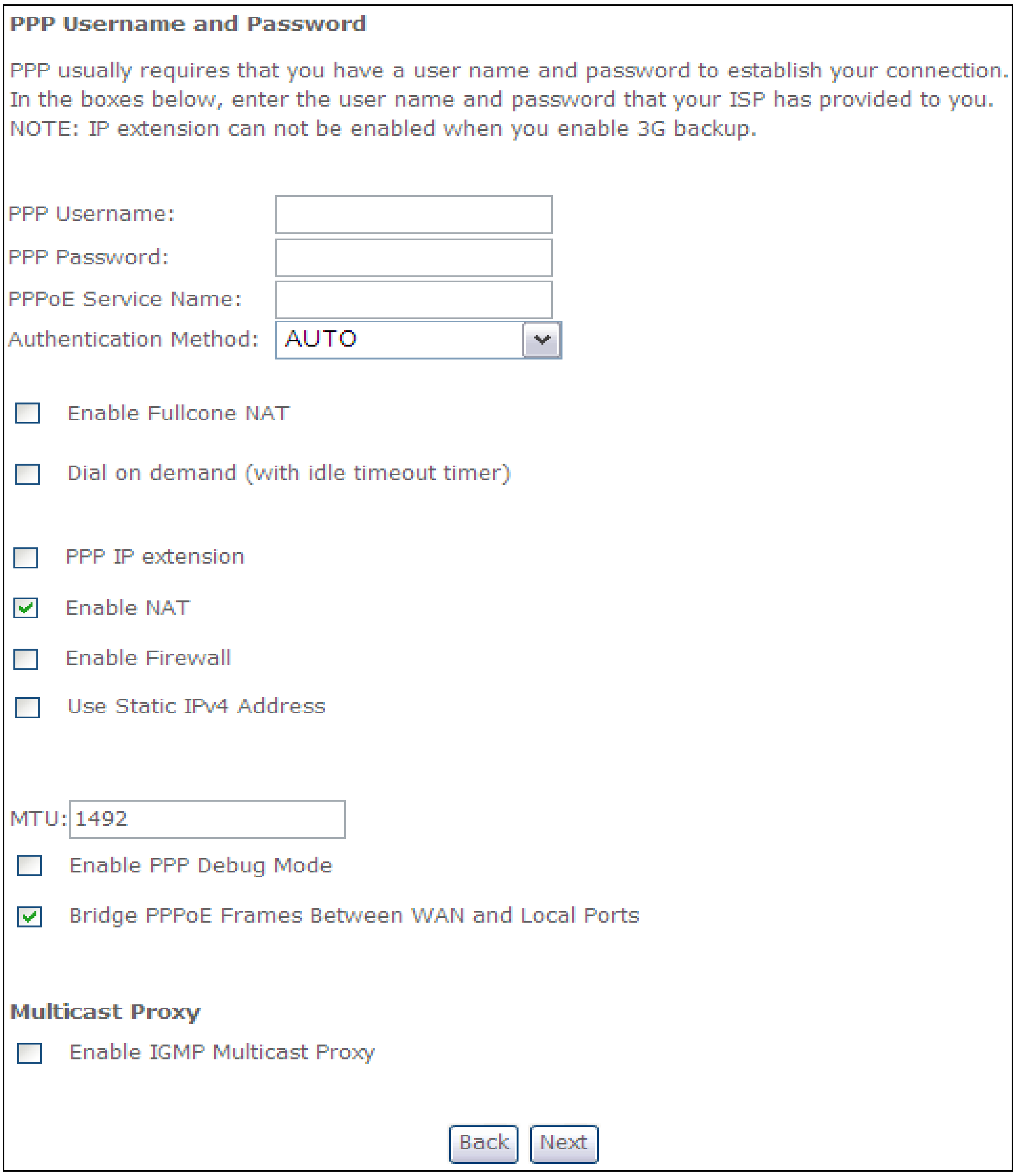
○ IP over Ethernet

○ Bridging

Enter Service Description: pppoe_0_0_35

□ Enable IPv6 for this service

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



PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

☑ Enable NAT

□ Enable Firewall

□ Use Static IPv4 Address

MTU: 1492

□ Enable PPP Debug Mode

☑ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

The settings shown above are described below.

PPP SETTINGS

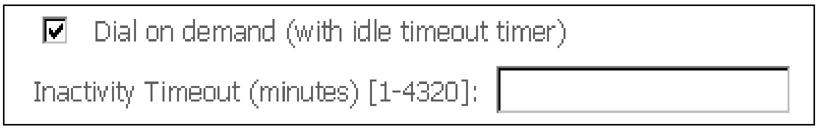
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

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

DIAL ON DEMAND

The CT-5374 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP EXTENSION

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

PPP IP Extension does the following:

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

ENABLE 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 3.2 IP Configuration.

ENABLE PPP DEBUG MODE

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

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

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

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The CT-5374 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

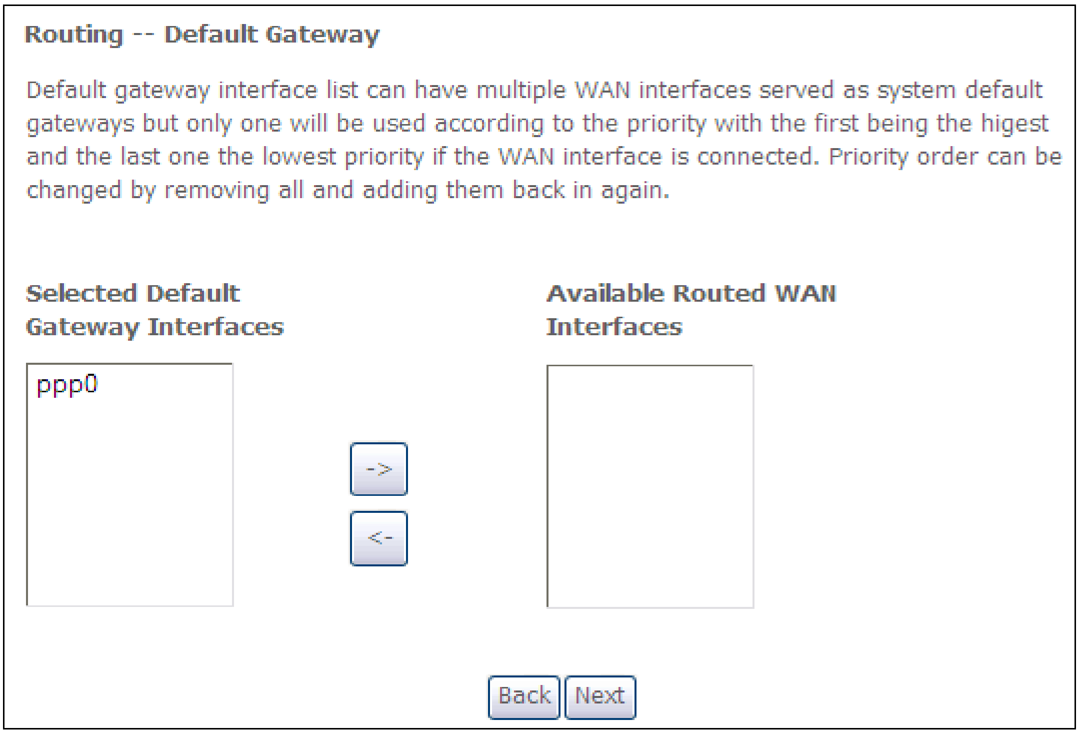
ENABLE IGMP MULTICAST PROXY

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

ENABLE MLD MULTICAST PROXY

This option displays when IPv6 is enabled. Tick the checkbox ☑ to enable Multicast Listener Discovery (MLD). This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

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

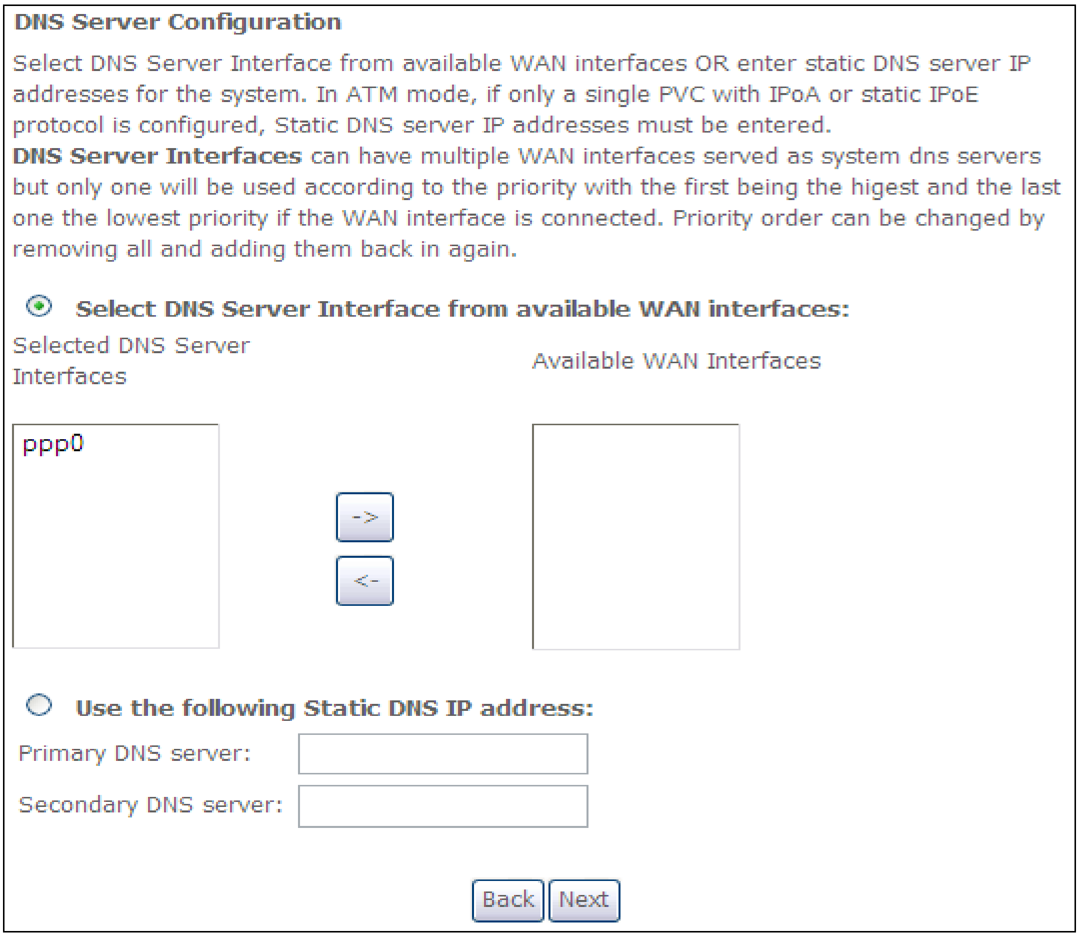
Selected Default Gateway Interfaces: ppp0

Available Routed WAN Interfaces:

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

STEP 4:

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



DNS Server Configuration

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

● Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ppp0

Available WAN Interfaces:

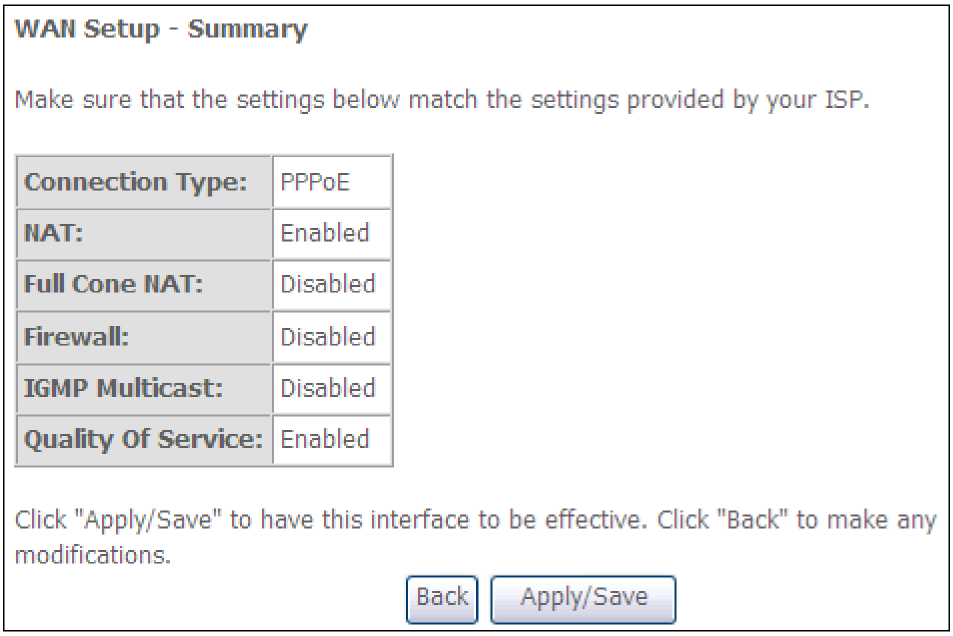
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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

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



WAN Setup - Summary

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

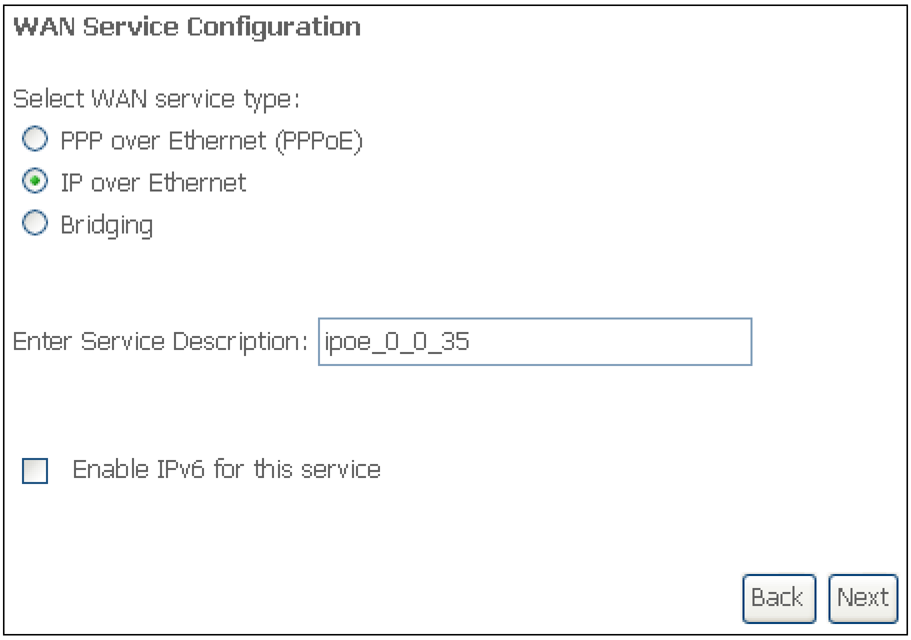
Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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.**

G2.2 IP over ETHERNET (IPoE)

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



WAN Service Configuration

Select WAN service type:

○ PPP over Ethernet (PPPoE)

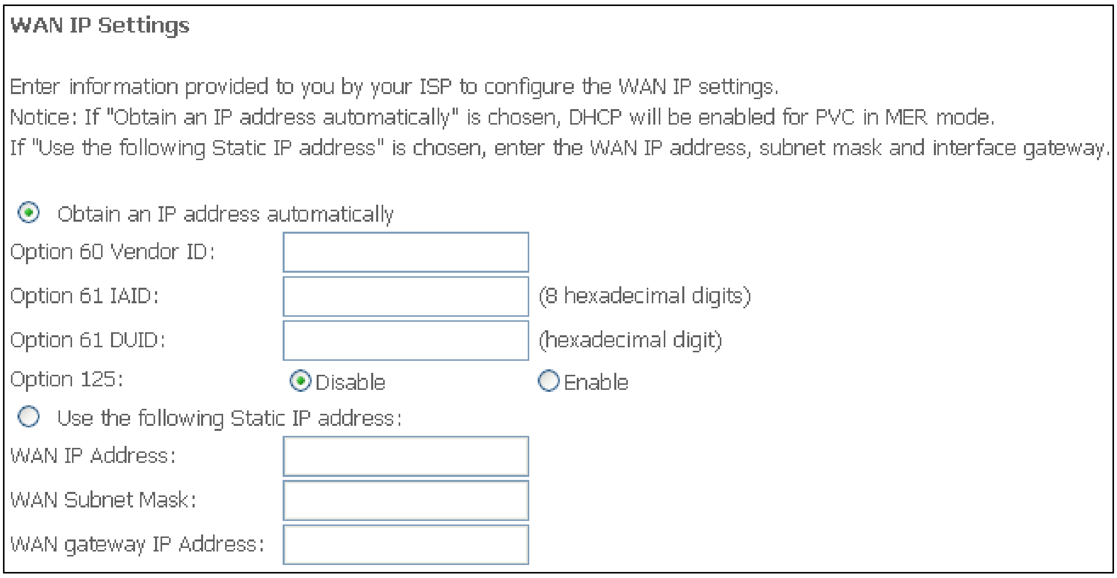
● IP over Ethernet

○ Bridging

Enter Service Description: ipoe_0_0_35

□ Enable IPv6 for this service

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 MER mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

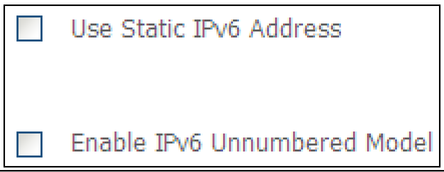
● Obtain an IP address automatically

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:	

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

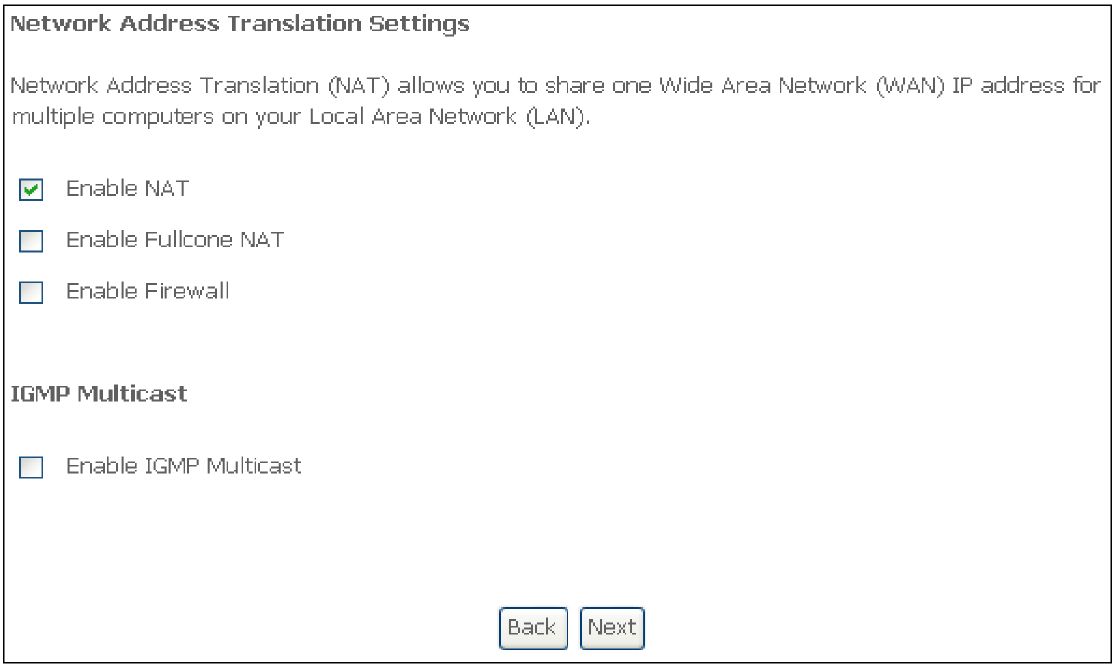


□ Use Static IPv6 Address

□ Enable IPv6 Unnumbered Model

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

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

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

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

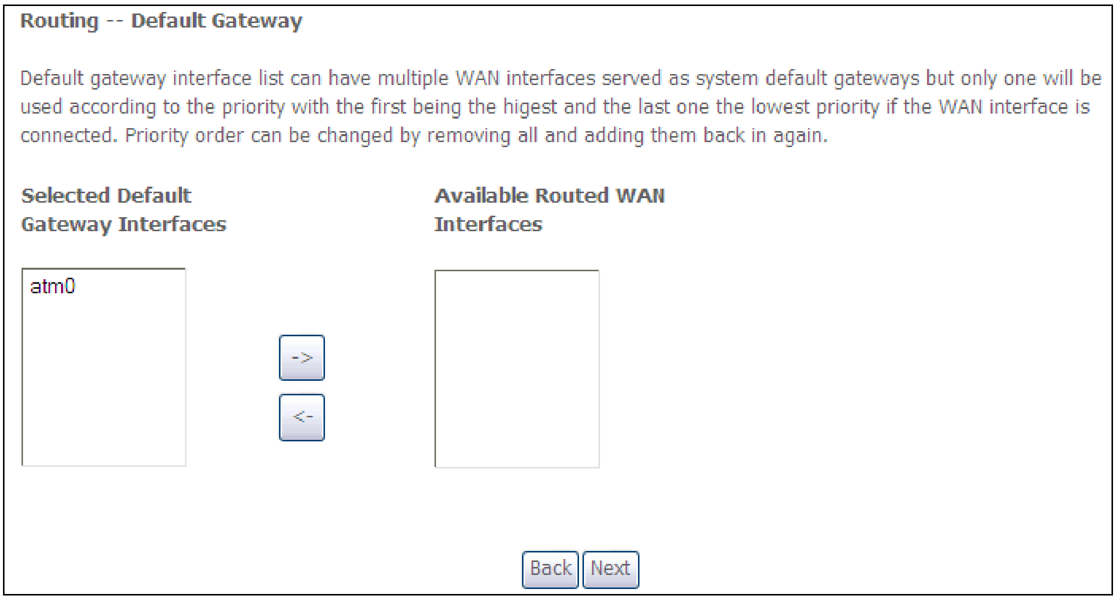
ENABLE IGMP MULTICAST

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

ENABLE MLD MULTICAST PROXY

<u>This option displays when IPv6 is enabled.</u> Tick the checkbox ☑ to enable Multicast Listener Discovery (MLD). This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

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



Routing -- Default Gateway

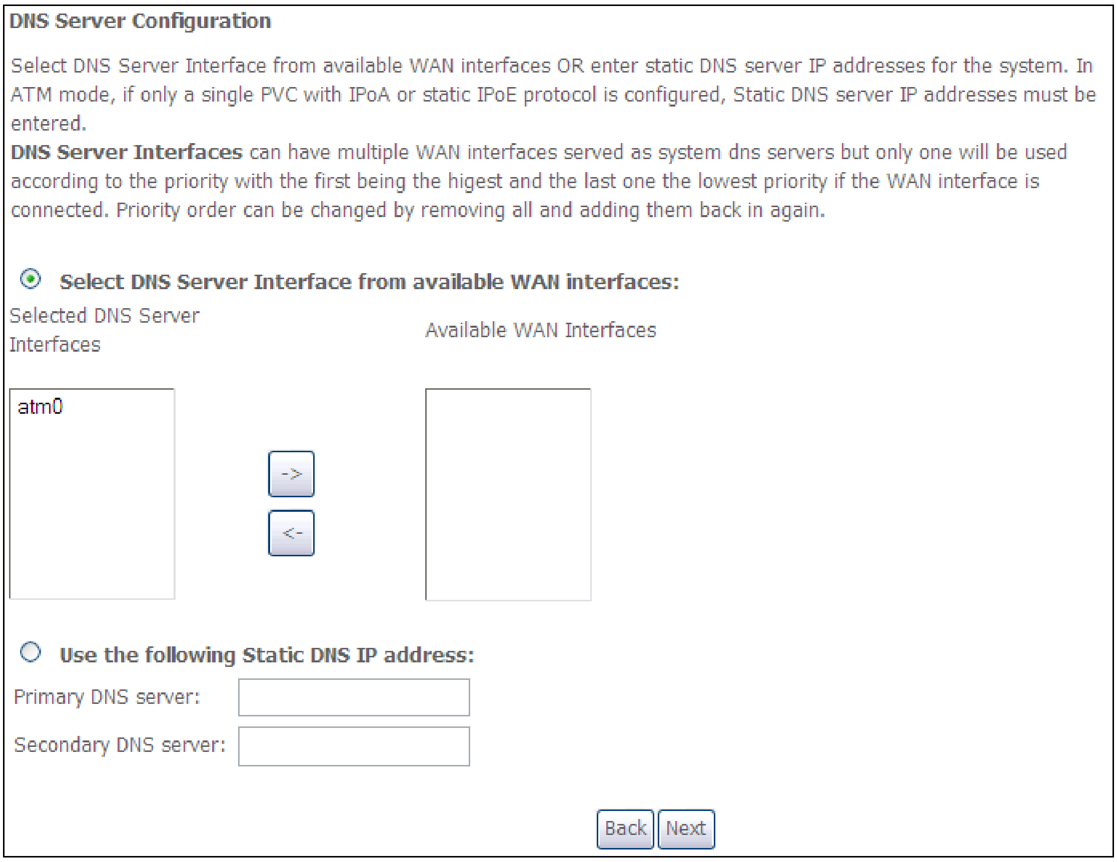
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
atm0	

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

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

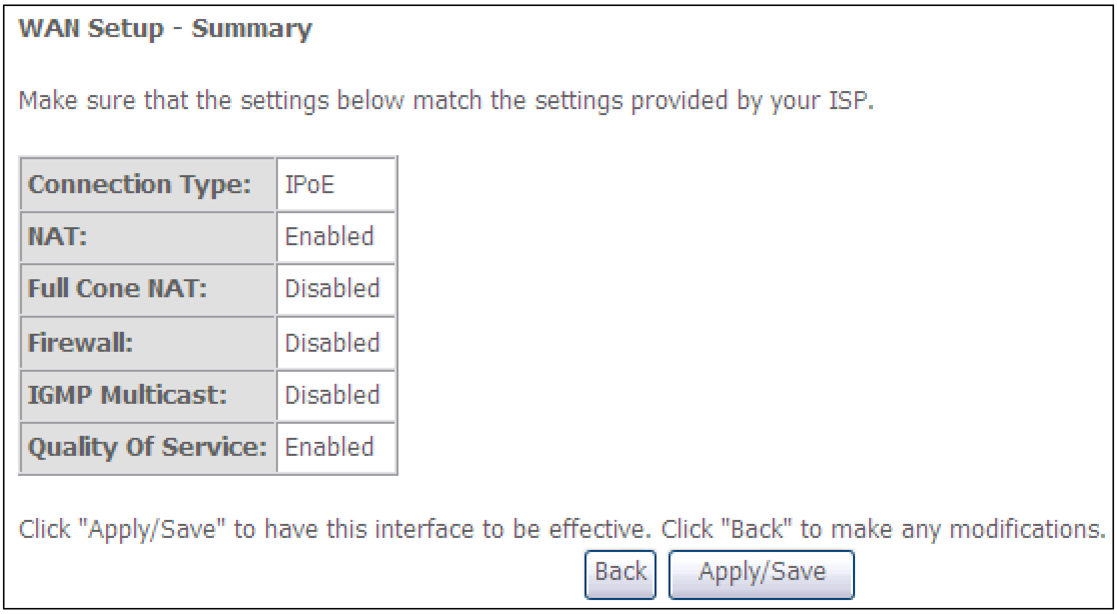
Selected DNS Server Interfaces	Available WAN Interfaces
atm0	

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

Primary DNS server:

Secondary DNS server:

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:	Enabled

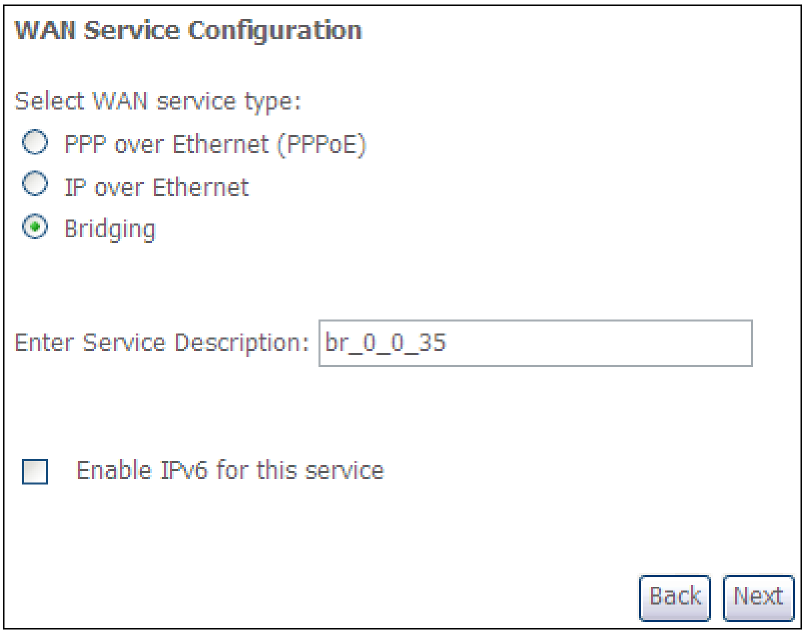
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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**.

G2.3 Bridging

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

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



WAN Service Configuration

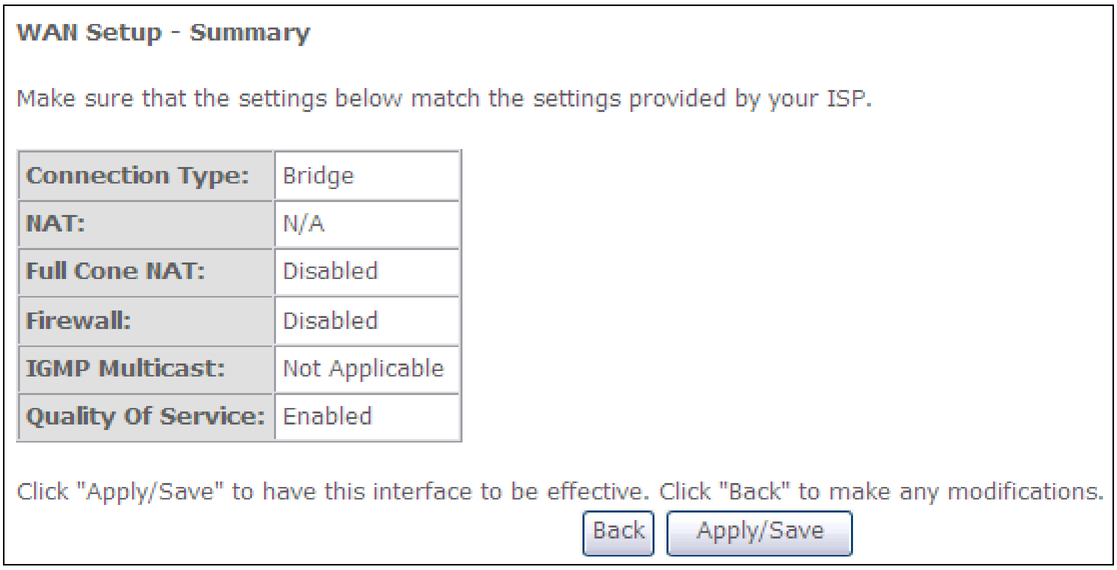
Select WAN service type:

○ PPP over Ethernet (PPPoE)
○ IP over Ethernet
● Bridging

Enter Service Description: br_0_0_35

□ Enable IPv6 for this service

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



WAN Setup - Summary

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

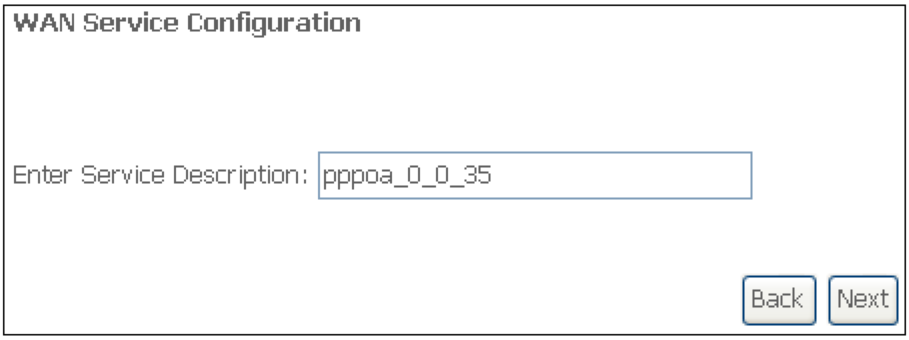
Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

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

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

NOTE:	If this bridge connection is your only WAN service, the CT-5374 will be inaccessible for remote management or technical support from the WAN.

G2.4 PPP over ATM (PPPoA)

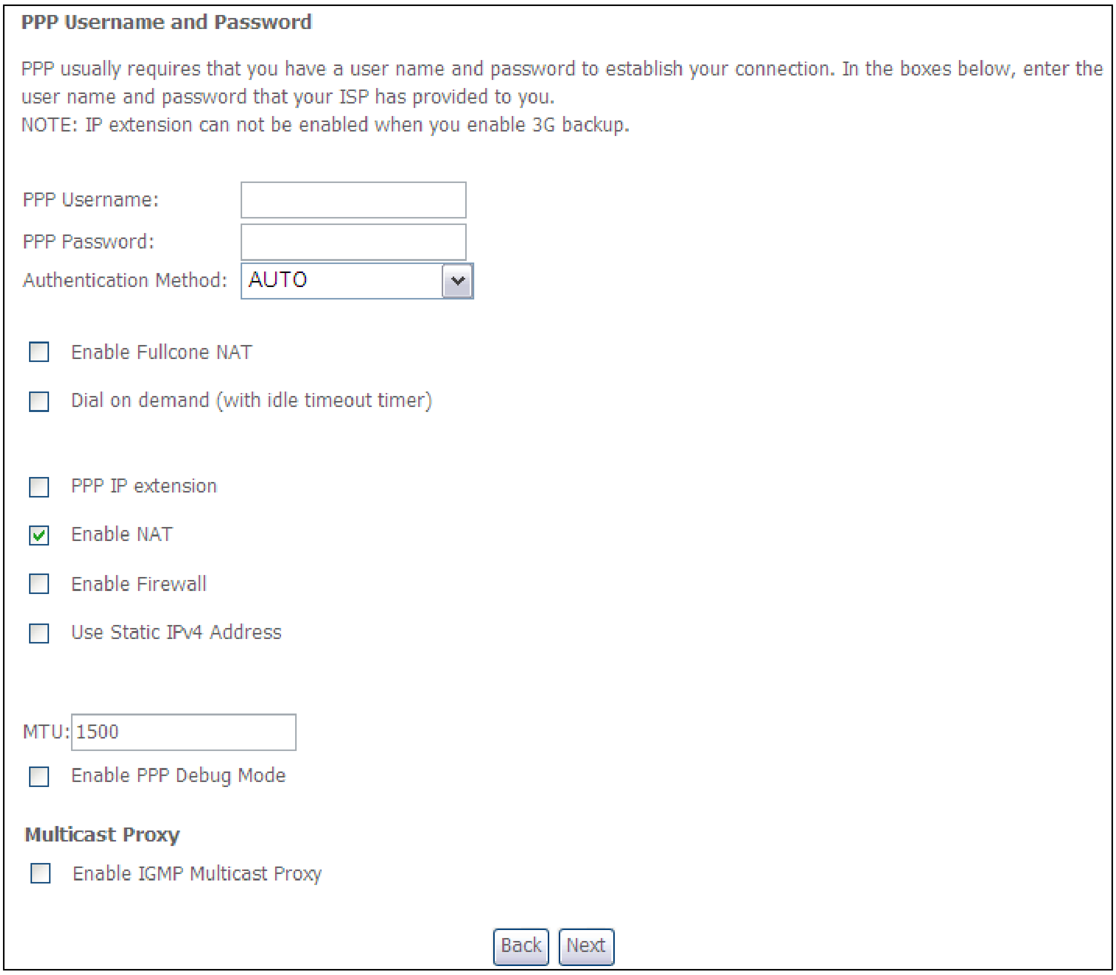


WAN Service Configuration

Enter Service Description: pppoa_0_0_35

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

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



PPP Username and Password

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

PPP Username:

PPP Password:

Authentication Method: AUTO

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☑ Enable NAT

☐ Enable Firewall

☐ Use Static IPv4 Address

MTU: 1500

☐ Enable PPP Debug Mode

Multicast Proxy

☐ Enable IGMP Multicast Proxy

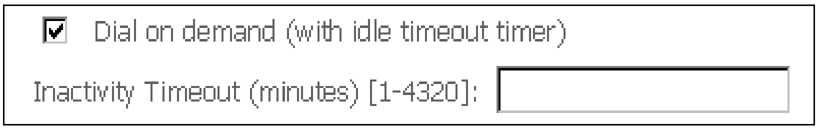
PPP SETTINGS
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

ENABLE FULLCONE NAT

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

DIAL ON DEMAND

The CT-5374 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP EXTENSION

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

PPP IP Extension does the following:

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

ENABLE 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 3.2 IP Configuration.

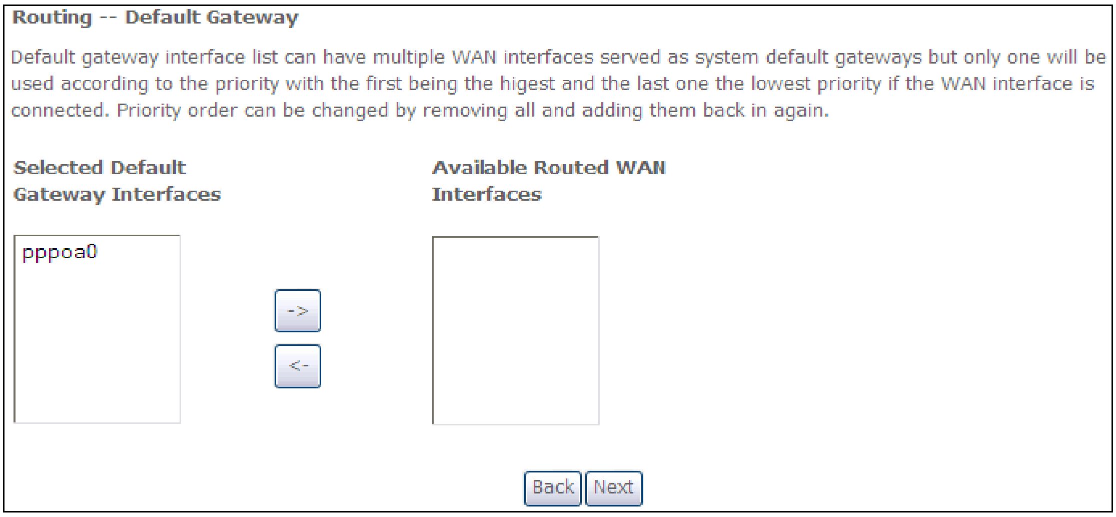
ENABLE PPP DEBUG MODE

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. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

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

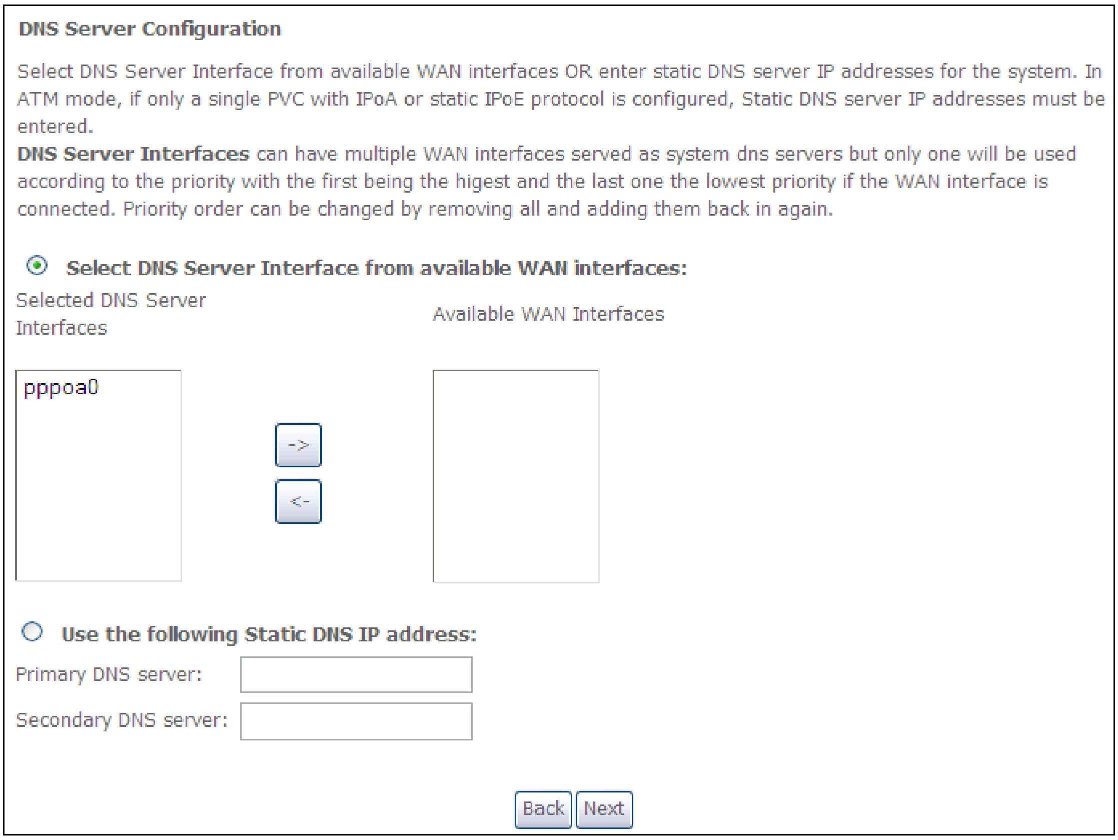
Selected Default Gateway Interfaces

pppoa0

Available Routed WAN Interfaces

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

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

Selected DNS Server Interfaces

pppoa0

Available WAN Interfaces

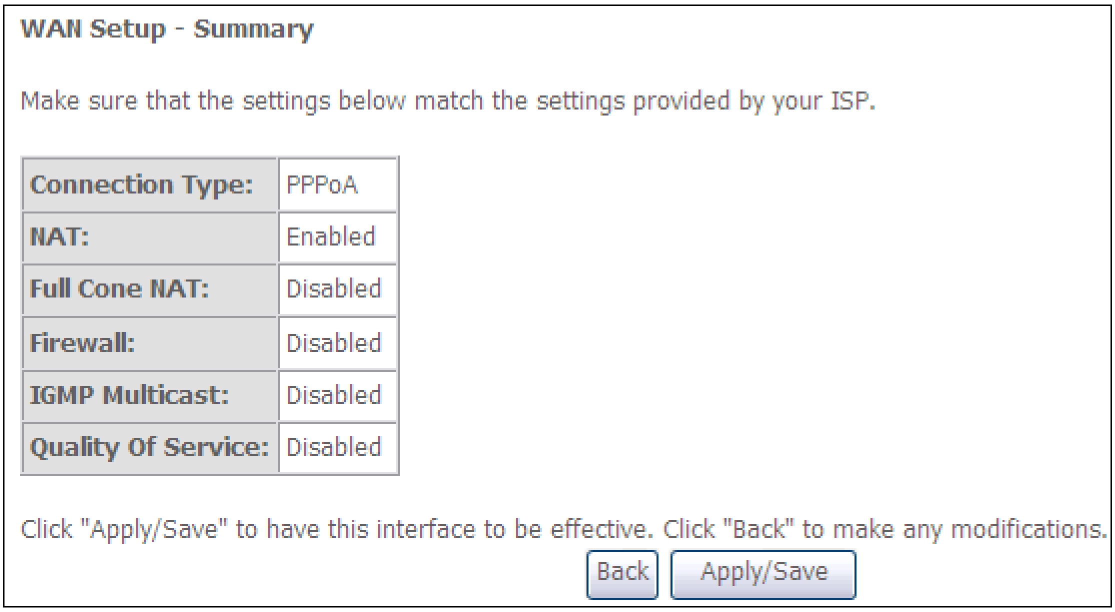
○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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

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



WAN Setup - Summary

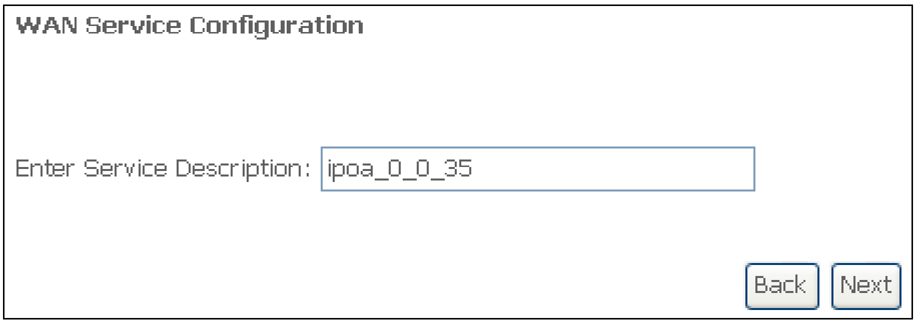
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoA
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**.

G2.5 IP over ATM (IPoA)

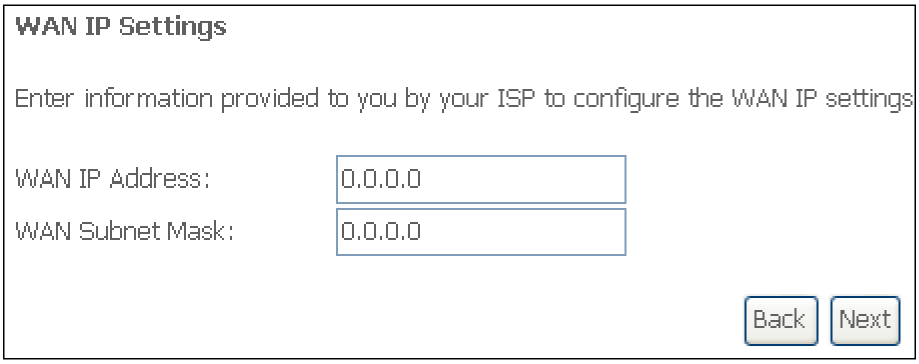


WAN Service Configuration

Enter Service Description: ipoa_0_0_35

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

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



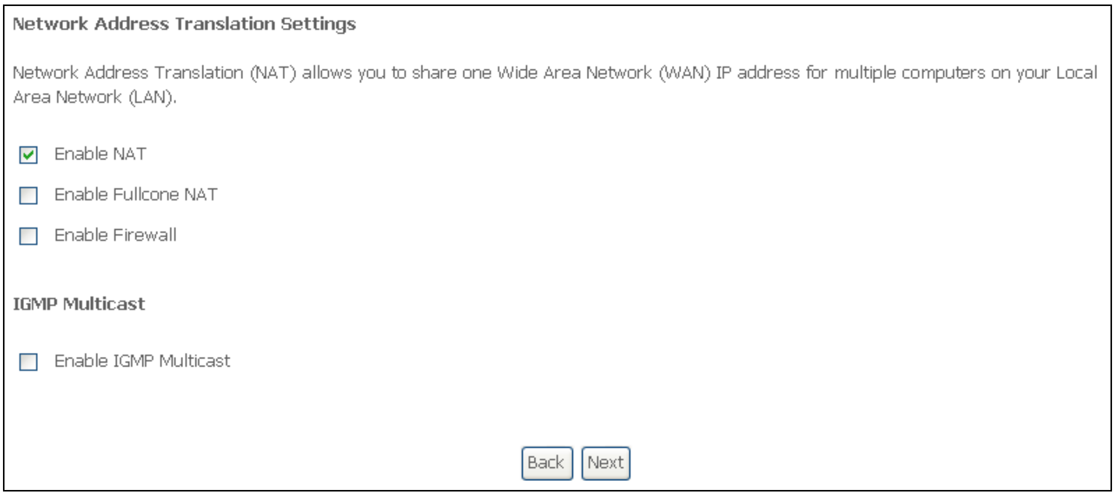
WAN IP Settings

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

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 0.0.0.0

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

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.

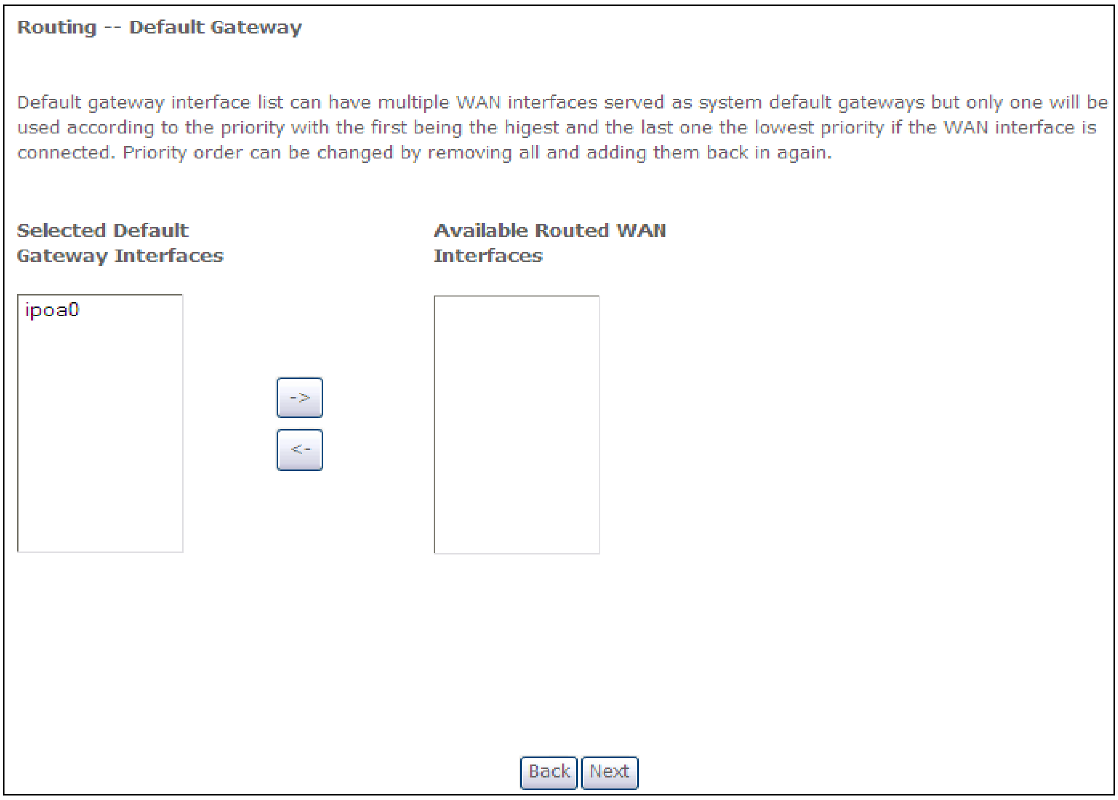
ENABLE FIREWALL

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.

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



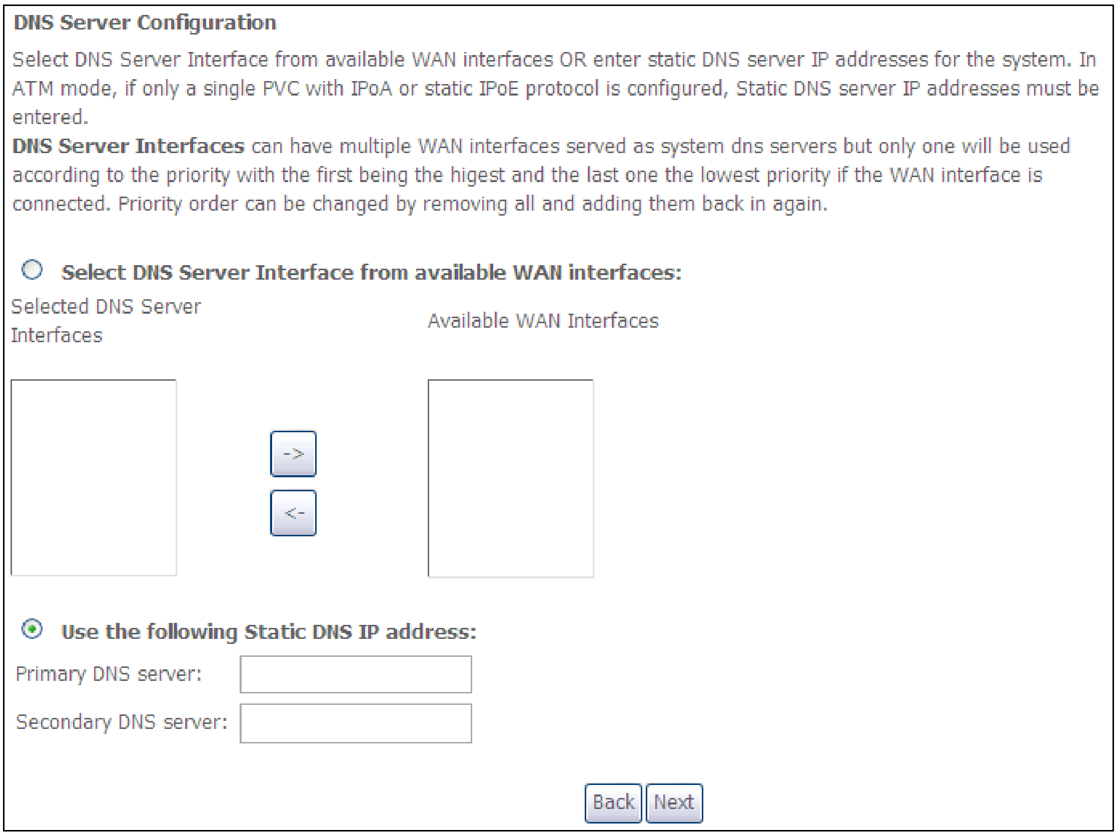
Routing -- Default Gateway

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

Selected Default Gateway Interfaces
ipoa0
->
<-
Available Routed WAN Interfaces
Back
Next

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

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

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

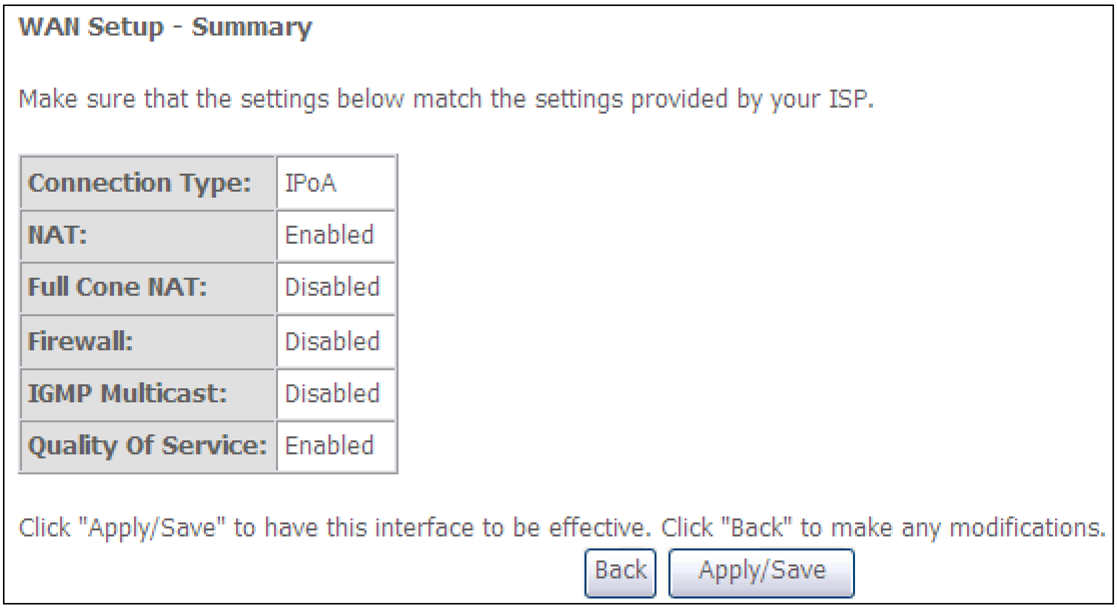
● **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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

STEP 7: 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**.