



COMTREND CORPORATION

CT-5367

Wireless ADSL2+ Router

User Manual

Version A2.1, August 26, 2010



Preface

This manual provides information related to the installation, operation, and application 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 lightning. 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](#)

Copyright

Copyright©2010 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

NOTE: This document is subject to change without notice.

FCC Interference Statement

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 dose 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

FCC Caution: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

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 20cmbetween the radiator & your body

Save 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, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

CHAPTER 1 SUMMARY	5
CHAPTER 2 INSTALLATION.....	6
2.1 REAR PANEL	6
2.2 FRONT PANEL	7
CHAPTER 3 WEB USER INTERFACE.....	8
3.1 DEFAULT SETTINGS	8
3.2 IP CONFIGURATION.....	9
3.3 LOGIN PROCEDURE.....	10
CHAPTER 4 QUICK SETUP	12
4.1 AUTO QUICK SETUP.....	12
4.2 MANUAL QUICK SETUP	13
4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....	14
4.2.2 MAC Encapsulation Routing (MER)	20
4.2.3 IP Over ATM.....	24
4.2.4 Bridging.....	27
CHAPTER 5 DEVICE INFORMATION.....	30
5.1 WAN	31
5.2 STATISTICS.....	32
5.2.1 LAN Statistics.....	32
5.2.2 WAN Statistics.....	32
5.2.3 ATM statistics	33
5.2.4 ADSL Statistics	35
5.3 ROUTE.....	38
5.4 ARP.....	39
5.5 DHCP.....	39
CHAPTER 6 ADVANCED SETUP.....	40
6.1 WAN	40
6.1.1 VLAN Mux	41
6.1.2 MSP	43
6.2 LAN.....	46
6.3 NAT	47
6.3.1 Virtual Servers	47
6.3.2 Port Triggering.....	49
6.3.3 DMZ Host	50
6.3.4 ALG.....	51
6.4 SECURITY	52
6.4.1 MAC Filtering.....	52
6.4.2 IP Filtering	53
6.5 PARENTAL CONTROL.....	55
6.5.1 URL Filter.....	56
6.6 QUALITY OF SERVICE	58
6.6.1 Queue Management Configuration	58
6.6.2 Queue Configuration.....	58
6.6.3 QoS Classification	59
6.7 ROUTING	61
6.7.1 Default Gateway.....	62
6.7.2 Static Route.....	62
6.7.3 RIP.....	63
6.8 DNS	64
6.8.1 DNS Server	64
6.8.2 Dynamic DNS.....	64
6.9 DSL.....	66
6.10 INTERFACE GROUP.....	67
6.11 CERTIFICATE	69

6.11.1	<i>Local</i>	69
6.11.2	<i>Trusted CA</i>	72
CHAPTER 7 WIRELESS		73
7.1	BASIC	73
7.2	SECURITY	74
7.2.1	<i>WPS</i>	77
7.3	MAC FILTER	85
7.4	WIRELESS BRIDGE	86
7.5	ADVANCED	86
7.6	STATION INFO	88
CHAPTER 8 DIAGNOSTICS		90
CHAPTER 9 MANAGEMENT		92
9.1	SETTINGS	92
9.1.1	<i>Backup</i>	92
9.1.2	<i>Update Settings</i>	93
9.1.3	<i>Restore Default</i>	93
9.2	SYSTEM LOG	94
9.3	TR-069 CLIENT	96
9.4	INTERNET TIME	97
9.5	ACCESS CONTROL	97
9.5.1	<i>Services</i>	98
9.5.2	<i>IP Addresses</i>	99
9.5.3	<i>Passwords</i>	99
9.6	UPDATE SOFTWARE	100
9.7	SAVE AND REBOOT	101
APPENDIX A: SECURITY		102
APPENDIX B: PIN ASSIGNMENTS		106
APPENDIX C: SPECIFICATIONS		107
APPENDIX D: SSH CLIENT		109
APPENDIX E: WSC EXTERNAL REGISTRAR		110

Chapter 1 Summary

The CT-5367 is an 802.11g (54Mbps) Wireless and Wired ADSL2+ router. It comes equipped with four 10/100 Base-T Ethernet ports and an ADSL2+ port for wired connectivity. An integrated 802.11g WLAN Access Point (AP) with Wi-Fi Protected Setup (WPS) provides wireless coverage. This model is designed for both residential and business applications that require wireless and wired connectivity to an ADSL broadband network.

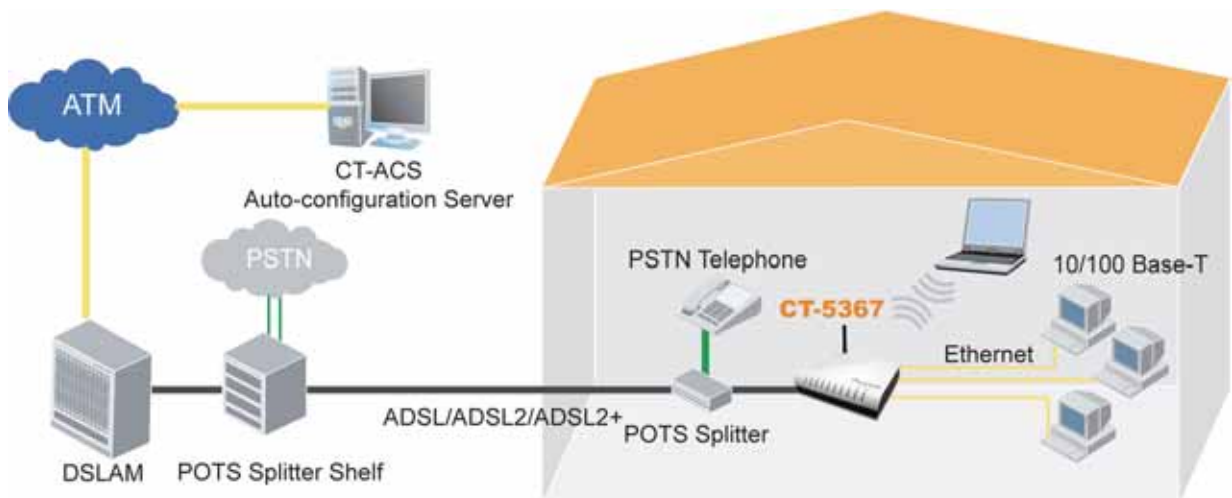
The CT-5367 ADSL2+ router also provides state of the art security features such as WPA data encryption, Firewall and VPN pass through. The CT-5367 supports up to 16 virtual connections allowing multiple users access to the Internet. The CT-5367 is also designed with TR-068 compliant color panel which eases the installation of the modem and makes it more user-friendly.

FEATURES

- Auto PVC configuration
- Per-VC packet level QoS
- Up to 16 VCs
- Embedded SNMP agent
- UPnP
- MAC address filtering
- IP filtering
- Static route and RIP v1/v2
- Dynamic IP assignment
- IP QoS
- NAT/PAT
- IGMP Proxy
- DNS Proxy
- TR-068 compliant
- Integrated 802.11b/g Access Point
- Wi-Fi Protected Setup (WPS)
- WPA/WPA2 and 802.1x
- Optional Turbo mode (After burner)
- WMM
- Web-based management
- Configuration backup/restoration
- RADIUS client
- FTP/TFTP server
- DHCP Server/Relay/Client
- TR-069/TR-098/TR-111 support
- Supports remote administration, automatic firmware upgrade and configuration

APPLICATION

The following diagram shows the application of the CT-5367.

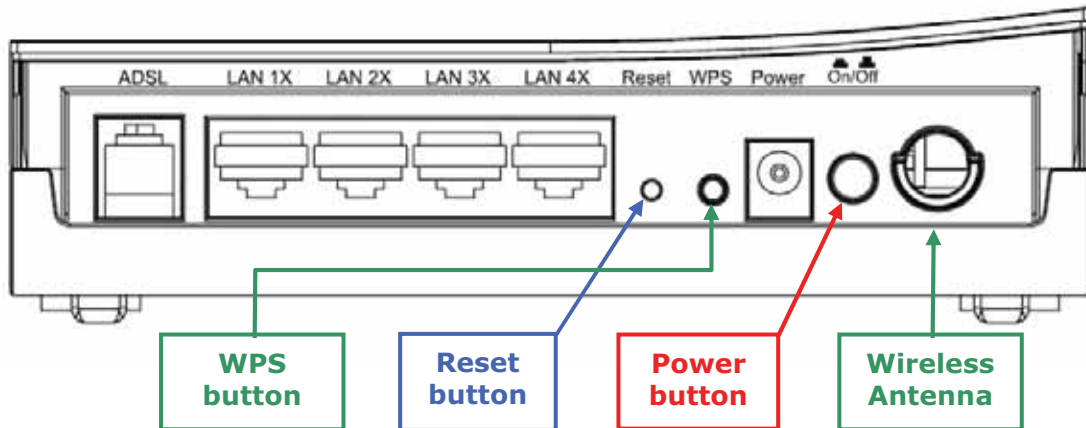


Chapter 2 Installation

2.1 Rear Panel

Follow the instructions below to complete the hardware installation.

For your reference, the diagram below shows the back panel of the CT-5367.



ADSL PORT

Connect the ADSL line to the ADSL port with a RJ11 cable.

LAN PORT

Use RJ45 straight through or crossover MDI/X cable to connect up to four devices.

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 indicator lights up green then the device is ready for setup (see section [2.2 Front Panel](#)).

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

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

RESET BUTTON

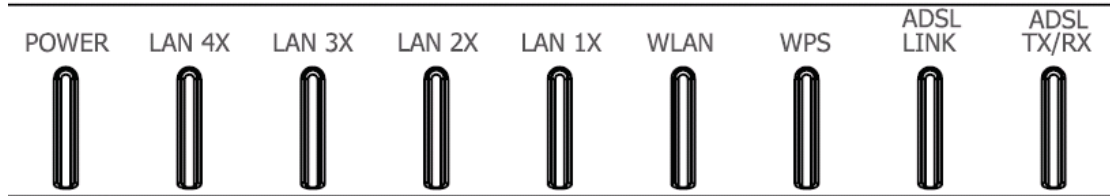
Restore the default settings of the device by holding down the Reset button until the front panel LED indicators blink simultaneously (~ 5 seconds). This action may be required if the router fails to respond normally or if the router configuration changes. The router has rebooted successfully when the LED indicators display correctly (see section [2.2 Front Panel](#)).

WPS BUTTON

Press this button to begin searching for WPS clients. The clients must also enable WPS push button mode. When WPS is available (the WPS LED will be ON), pressing the button for 5 seconds or more will disable Wireless function.

2.2 Front Panel

The LED indicators are shown below and explained in the table that follows. They are useful for checking the power and connection status of the router.



LED	Color	Mode	Function
POWER	Green	On	The router is powered up
		Off	The router is powered down
LAN 4X~1X	Green	On	An Ethernet Link is established
		Off	An Ethernet Link is not established
		Blink	Data transmitting or receiving over LAN
WLAN	Green	On	The wireless module is ready and idle
		Off	The wireless module is not installed
		Blink	Data transmitting or receiving over WLAN
WPS	Green	On	WPS enabled
		Off	WPS disabled
		Blink	The router is searching for WPS clients
ADSL LINK	Green	On	ADSL link is established
		Off	ADSL link is not established
		Blink	ADSL link is training
ADSL TX/RX	Green	On	ADSL Link is idle
		Off	ADSL Link is terminated
		Blink	ADSL link is active

Chapter 3 Web User Interface

This section describes the web user interface, which is accessed using any Internet browser, such as Microsoft Internet Explorer (version 5.0 and later).

3.1 Default Settings

The following are the default settings for the device.

- Local (LAN) access (**username:** root , **password:** 12345)
- Remote (WAN) access (**username:** support, **password:** support)
- User access (**username:** user, **password:** user)
- LAN IP address: 192.168.1.1
- WAN IP address: none
- Remote WAN access: only Ping (ICMP) enabled
- NAT and *Firewall: PPPoE/PPPoA enabled - MER/IPoA/Bridge disabled
- DHCP server on LAN interface: enabled
- Wireless Access: enabled
- SSID: Comtrend
- Wireless Authentication: Open (i.e. no authentication)

*If Firewall is not required, please untick selection box.

This device supports the following connection types.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

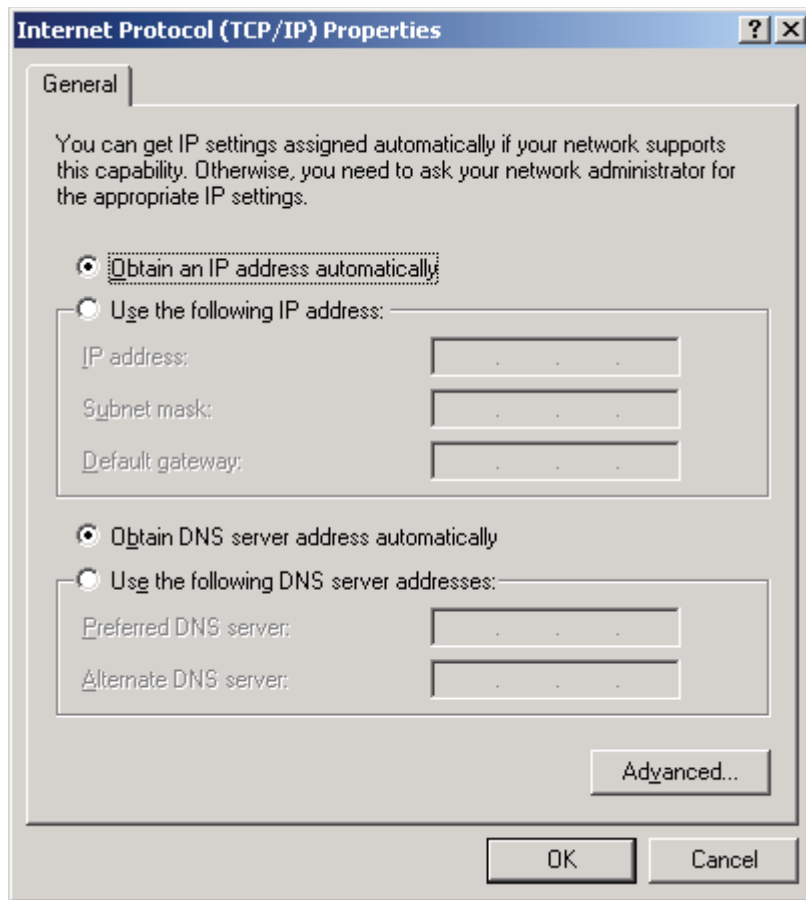
Technical Note:

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

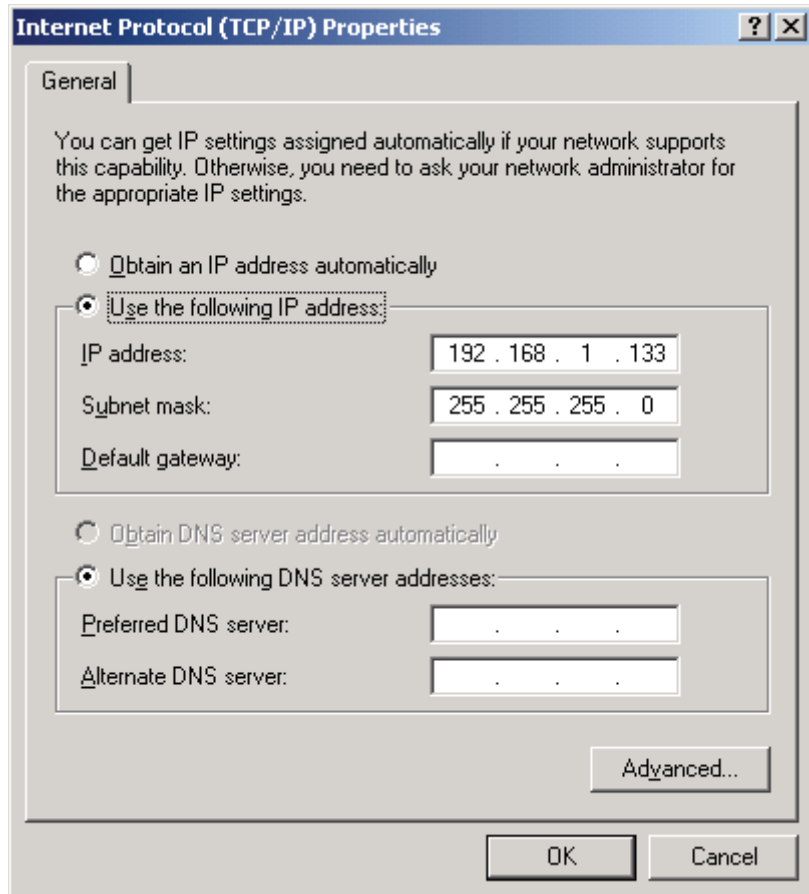
When the device powers up, the DHCP server (on the device) will start automatically. To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.



STATIC IP MODE

To configure the device manually, your PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x. The following assumes you are running Windows XP.

- 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. The screen should now display as below. Change the IP address to the domain of 192.168.1.x ($1 < x < 254$) with subnet mask of 255.255.255.0.



STEP 3: Click OK to submit the 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 [Device Info - WAN](#) screen and login with remote username and password.

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

Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm: DSL Router

User Name: root

Password: *****

Save this password in your password list

OK Cancel

NOTE: The login password can be changed later (see [section 9.6.3](#))

STEP 3: After successfully logging in, you will reach the **Quick Setup** screen.

GOMTREND ADSL Router

Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Select the check box below to enable DSL Auto-connect process.

DSL Auto-connect

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

NOTE: If a PVC connection already exists then this Quick Setup screen will be bypassed and the [Device Info](#) screen will display instead. In general, the selections available on the main menu (onscreen at left) are based upon configured connections and user account privileges.

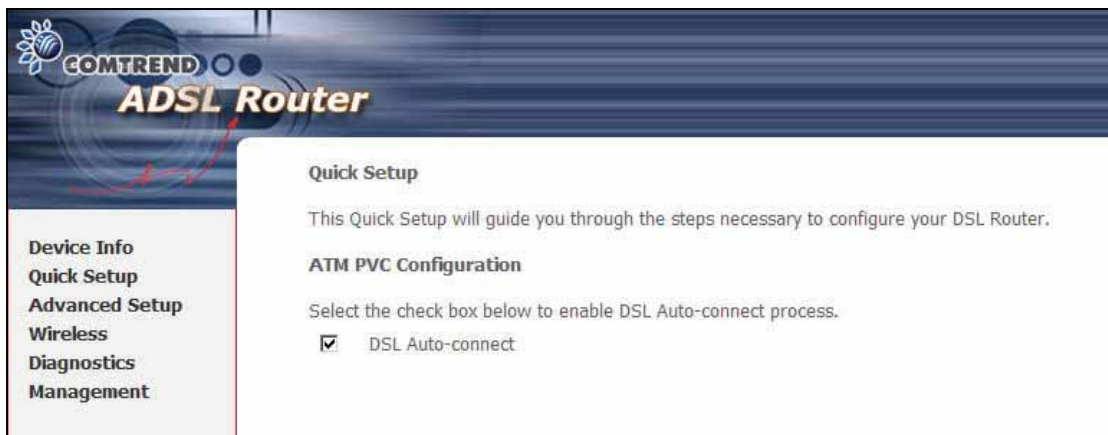
Chapter 4 Quick Setup

After login, the **Quick Setup** screen will appear. It is the default screen when no connections exist. This screen allows for the configuration of DSL settings and the IP configuration. It includes WAN, LAN and Wireless basic setup screens.

4.1 Auto Quick Setup

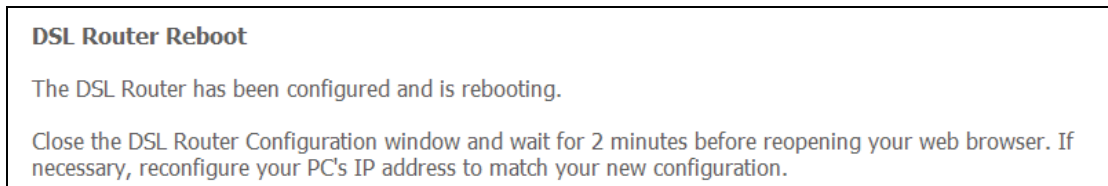
This function provides an automated process to quickly setup a WAN connection. The device will auto-detect the best PVC profile available, provided that the ADSL link is up. For manual setup, please go to [4.2 Manual Quick Setup](#).

STEP 1: Tick the **DSL Auto-connect** checkbox on the **Quick Setup** screen.



STEP 2: Click **Next** to start the setup process. Follow the onscreen prompts.

STEP 3: After setup is complete the device will reboot.

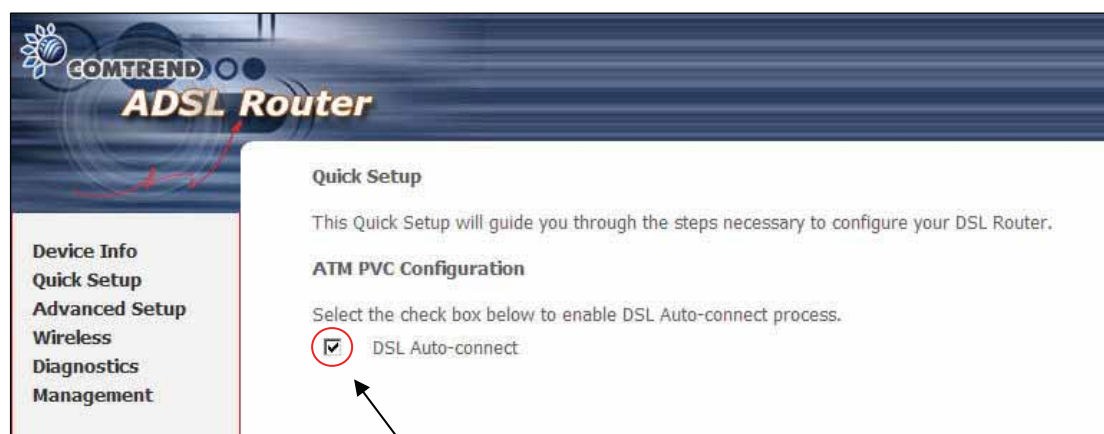


NOTE: After the device reboots, the [Device Info](#) screen should appear. If the browser does not refresh automatically, close it and restart. You will need to login again. If you encounter difficulty, be sure to check the IP configuration (see section [3.2 IP Configuration](#)).

4.2 Manual Quick Setup

To setup the router manually follow these instructions.

STEP 1: Select **Quick Setup** from the main menu and uncheck the **DSL Auto-connect** checkbox to begin the manual quick setup process.



Uncheck to begin the manual quick setup process and display the following screen.

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255]

VCI: [32-65535]

Enable Quality Of Service

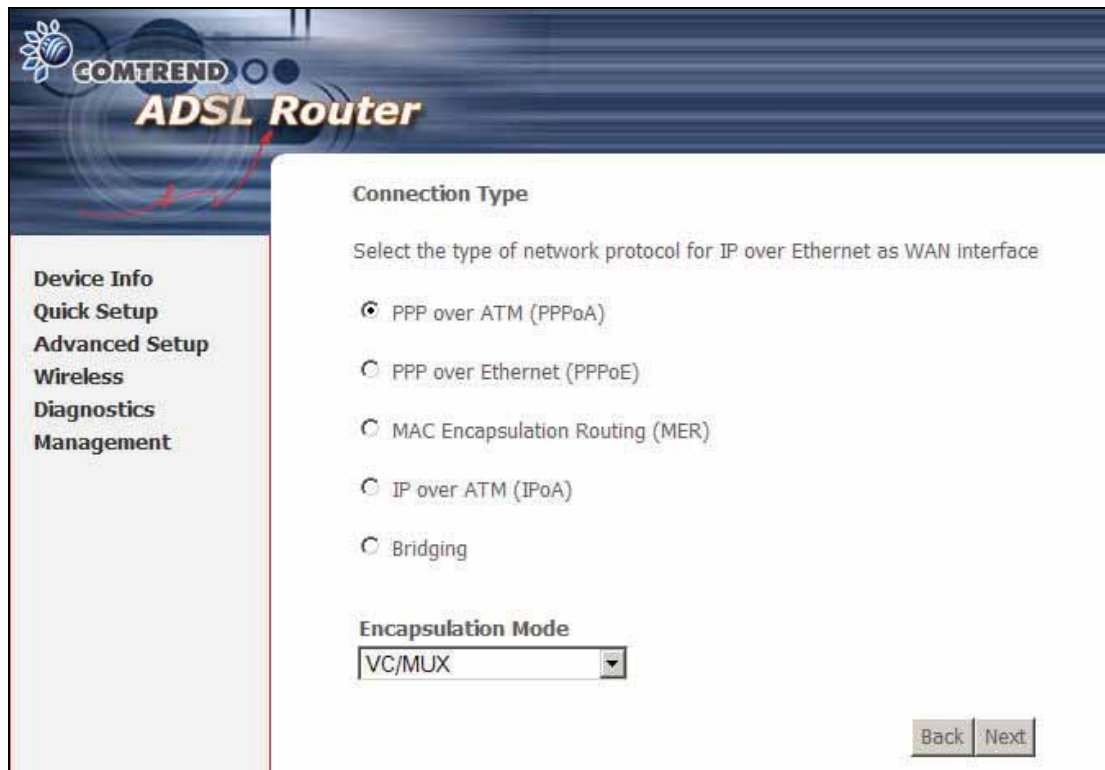
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

STEP 2: Adjust the VPI and VCI settings for the connection you wish to establish. Select **Enable Quality Of Service** if required.

Click **Next** to continue. **STEP 3:** On this screen, you can choose the connection type and select the appropriate encapsulation mode. The available options are shown.

- ◆ PPPoA- VC/MUX, LLC/ENCAPSULATION
- ◆ PPPoE- LLC/SNAP BRIDGING, VC/MUX
- ◆ MER- LLC/SNAP-BRIDGING, VC/MUX
- ◆ IPoA- LLC/SNAP-ROUTING, VC MUX
- ◆ Bridging- LLC/SNAP-BRIDGING, VC/MUX



Click **Next** to continue...

NOTE: The subsections that follow continue the ATM PVC setup procedure. Enter the appropriate settings for your service. Choosing different connection types will lead to a different sequence of setup screens.

4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

STEP 4: Select PPP over ATM (PPPoA) **or** PPP over Ethernet (PPPoE) and click **Next**. The following screen appears. Enter the Username and Password and select the connection options you wish. Review the descriptions below for more details. Click **Next** to continue.

PPP USERNAME / PPP PASSWORD

The PPP Username and the PPP password requirement are dependent on the particular requirements of the service provider. A maximum of 256 characters is allowed for the PPP user name and a maximum of 32 characters for PPP password.

PPPOE SERVICE NAME

PADI requests contain a service label for PPPoE connections. Some PPPoE servers (or BRAS) of ISP check this service label to make a connection.

ENABLE FULLCONE NAT

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 device can be configured to disconnect if there is no activity for a period of time. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 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, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN
- 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.
- NAT and firewall are disabled when this option is selected.
- 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.

ENABLE NAT

- If the LAN uses private IP addresses, this checkbox must be selected. The NAT submenu will be added to the Advanced Setup menu after reboot. This function consumes system resources and thus may impact performance.
- If the LAN uses public IP addresses, this checkbox must not be selected. The NAT submenu will be removed from the Advanced Setup menu after reboot.

ENABLE FIREWALL

To enable IP packet filtering, tick this checkbox . The Firewall menu will be added to the Advanced Setup menu after reboot. Disable this function when not required to improve performance.

USE STATIC IP 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. Don't forget to adjust the TCP/IP settings as described in section [3.2 IP Configuration](#).

Retry PPP password on authentication error

Tick the box to select this option.

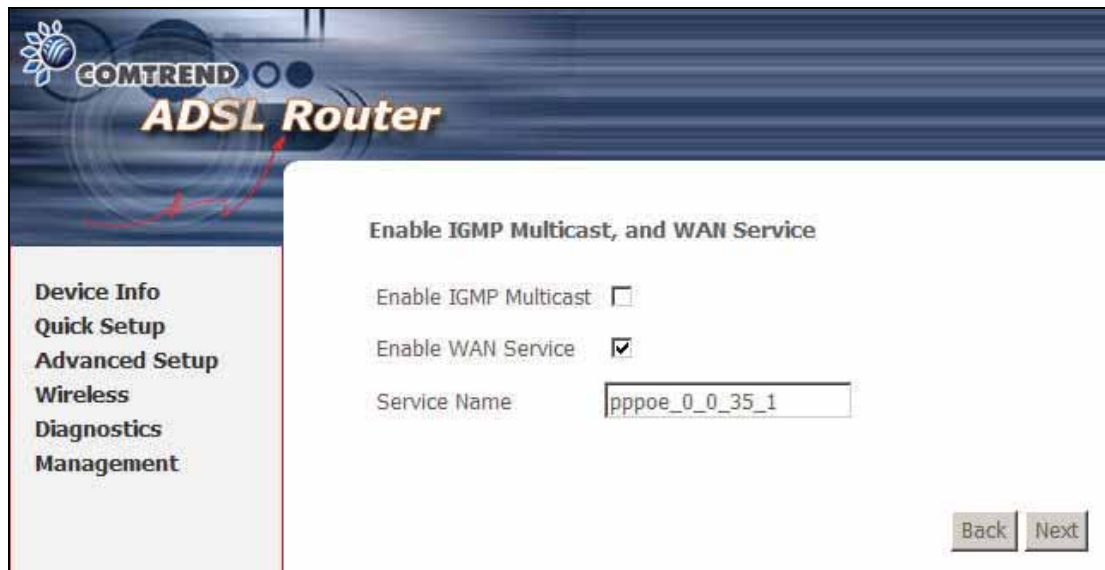
ENABLE PPP DEBUG MODE

More PPP connection information will be listed in the System Log. This is used for debugging. Please don't enable it for normal usage as it uses system resources.

FIXED MTU

Tick the checkbox and adjust the MTU value for WAN interface, PPPoE and PPPoA. The default values for MTU is 1492. The allowable range is from 0 to 9999. If a value is entered outside this range a dialog box will be displayed. If a value is entered outside this range a dialog box will pop up.

STEP 5: This screen allows the user to control IGMP Multicast and WAN Service.



ENABLE IGMP MULTICAST CHECKBOX

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

ENABLE WAN SERVICE CHECKBOX:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

SERVICE NAME

This is the WAN Service label.

STEP 6: After entering your settings, click **Next**. The following screen appears.

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses, Subnet Mask 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.

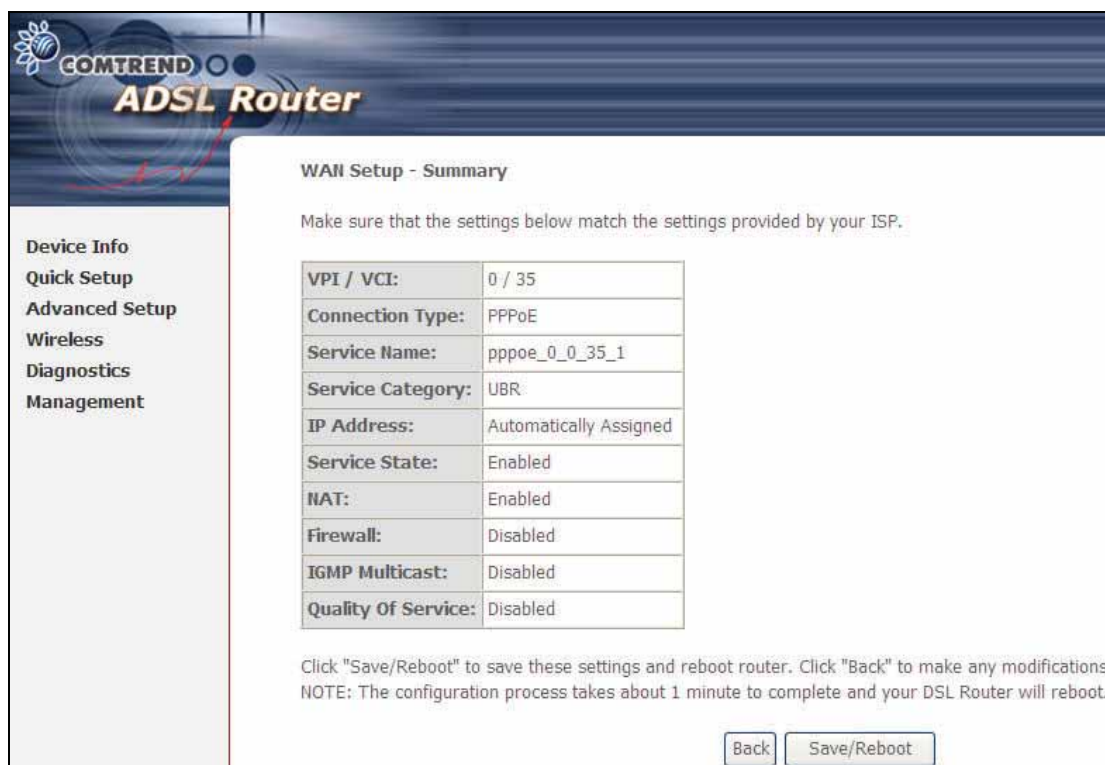
Please be aware that the private address range (e.g. 192.168.1.2 ~ 192.168.1.254) does not include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

To configure a second IP address for the LAN port, click the box shown below.

STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.



STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.



STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in subsection [3.3 Login Procedure](#).

4.2.2 MAC Encapsulation Routing (MER)

Step 4: Select MAC Encapsulation Routing (MER) and enter information provided to you by your ISP to configure the WAN IP settings. Detailed field descriptions are provided below. Click **Next** to continue.

The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'WAN IP Settings' and contains the following text: 'Enter information provided to you by your ISP to configure the WAN IP settings. Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address" field. The "Use WAN interface" is optional.'

The configuration options are as follows:

- Obtain an IP address automatically
- Use the following IP address:
 - WAN IPv4 Address:
 - WAN Subnet Mask:
- Obtain default gateway automatically
- Use the following default gateway:
 - Use IPv4 Address:
 - Use WAN Interface:
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
 - Primary DNS server:
 - Secondary DNS server:

At the bottom right, there are 'Back' and 'Next' buttons.

DHCP is enabled in MER mode when **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure the static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the **Use IPv4 address** field.

Step 5: This screen provides access to Network Address Translation (NAT), IGMP Multicast, and WAN Service settings. Enable each service by selecting its checkbox. When done, click **Next** to continue.



ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

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 the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service: Tick the checkbox to enable WAN service.

Service Name: This is the WAN Service label.

Step 6: Upon completion, click **Next**. The following screen appears.

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

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

- Disable DHCP Server
- Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

- Enable DHCP Server Relay

DHCP Server IP Address:

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

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses, Subnet Mask 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.


Please be aware that the private address range (e.g. 192.168.1.2 ~ 192.168.1.254) can never include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (not available if **NAT** enabled), and enter the DHCP Server IP Address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a second IP address for the LAN port, click the box shown below.

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

STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.



The screenshot shows the 'Wireless -- Setup' page of a Comtrend ADSL Router. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area has the title 'Wireless -- Setup'. Below the title, there is a checkbox for 'Enable Wireless' which is checked. A text prompt says 'Enter the wireless network name (also known as SSID):'. Below this, the 'SSID:' label is followed by a text input field containing the value 'Comtrend'. At the bottom right of the main content area, there are two buttons: 'Back' and 'Next'.

STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

COMTREND ADSL Router

WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	MER
Service Name:	mer_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in subsection [3.3 Login Procedure](#).

4.2.3 IP Over ATM

Step 4: Select IP over ATM (IPoA) and click **Next**. The following screen appears.

COMTREND ADSL Router

WAN IP Settings

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

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

Use the following default gateway:

Use IP Address:

Use WAN Interface:

Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

NOTE: Since DHCP is not supported over IPoA, users must manually enter the IP address or WAN interface for the default gateway and the DNS server addresses (primary and secondary), as provided by their ISP.

Step 5: Click **Next**. The following screen appears.



ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

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 the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service: Tick the checkbox to enable WAN service.

Service Name: This is the WAN Service label.

Step 6: Click **Next** to display the following screen.

COMTREND ADSL Router

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

Disable DHCP Server
 Enable DHCP Server

Start IP Address:
 End IP Address:
 Subnet Mask:
 Leased Time (hour):

Enable DHCP Server Relay
 DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses, Subnet Mask 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.

Please be aware that the private address range (e.g. 192.168.1.2 ~ 192.168.1.254) can never include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (not available if **NAT** enabled), and enter the DHCP Server IP Address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. To configure a second IP address for the LAN port, click the box shown below.

Configure the second IP Address and Subnet Mask for LAN interface

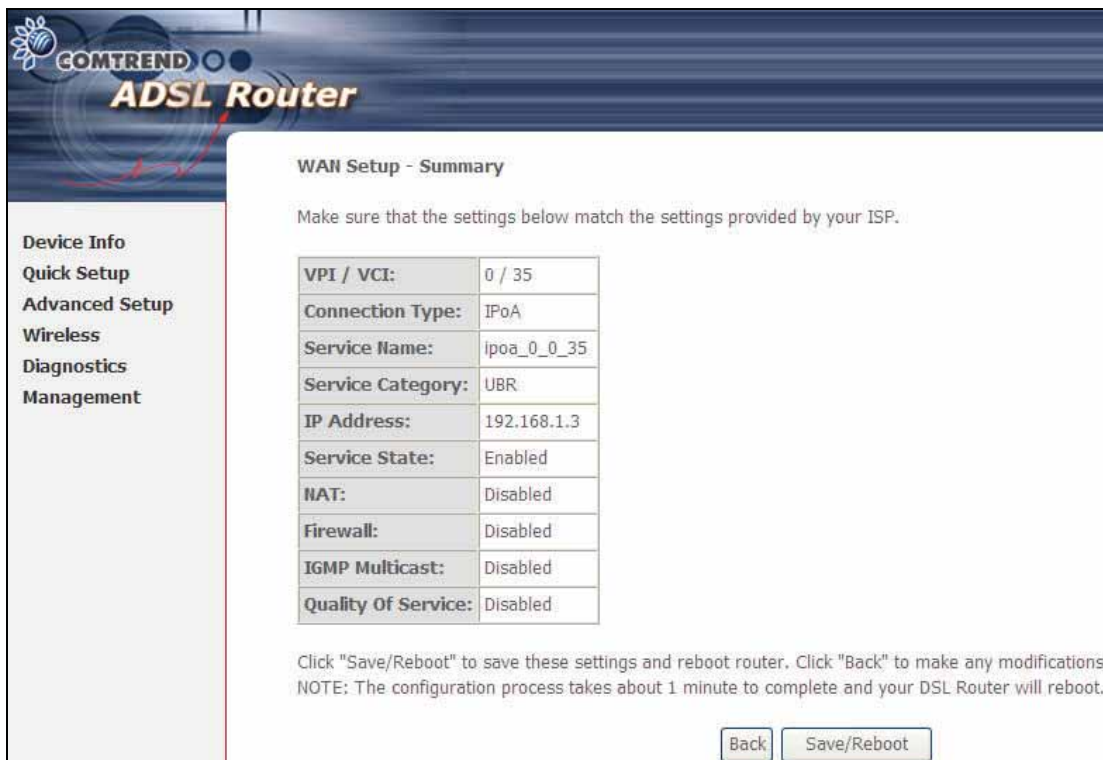
IP Address:

Subnet Mask:

STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.



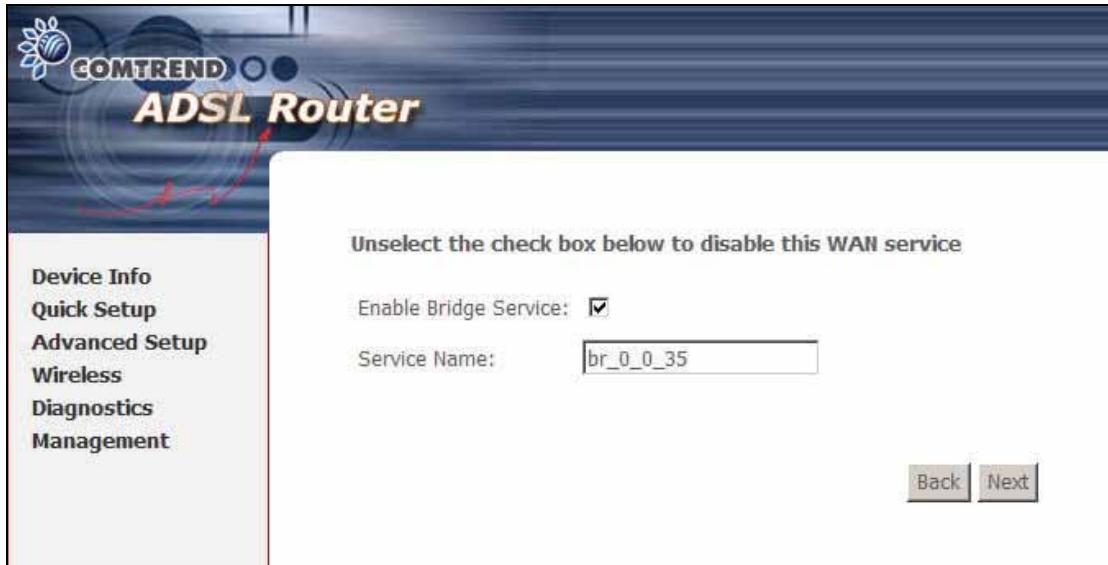
STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.



STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in subsection [3.3 Login Procedure](#).

4.2.4 Bridging

Step 4: Select Bridging and click **Next**. To enable bridging service, tick the **Enable Bridge Service** checkbox and enter a **Service Name**.



Step 5: Click the **Next** button to continue. On this screen, you may enter the IP address and Subnet Mask for the LAN interface. Click **Next**.



NOTE: The LAN IP interface in bridge mode is needed for local users to manage the device. In addition, there is no IP address for the WAN interface and therefore the device cannot be accessed remotely in this mode.

STEP 6: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.

COMTRENDS
ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

Wireless -- Setup

Enable Wireless

Enter the wireless network name (also known as SSID).
SSID:

Back Next

STEP 7: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

COMTRENDS
ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

STEP 8: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in subsection [3.3 Login Procedure](#).

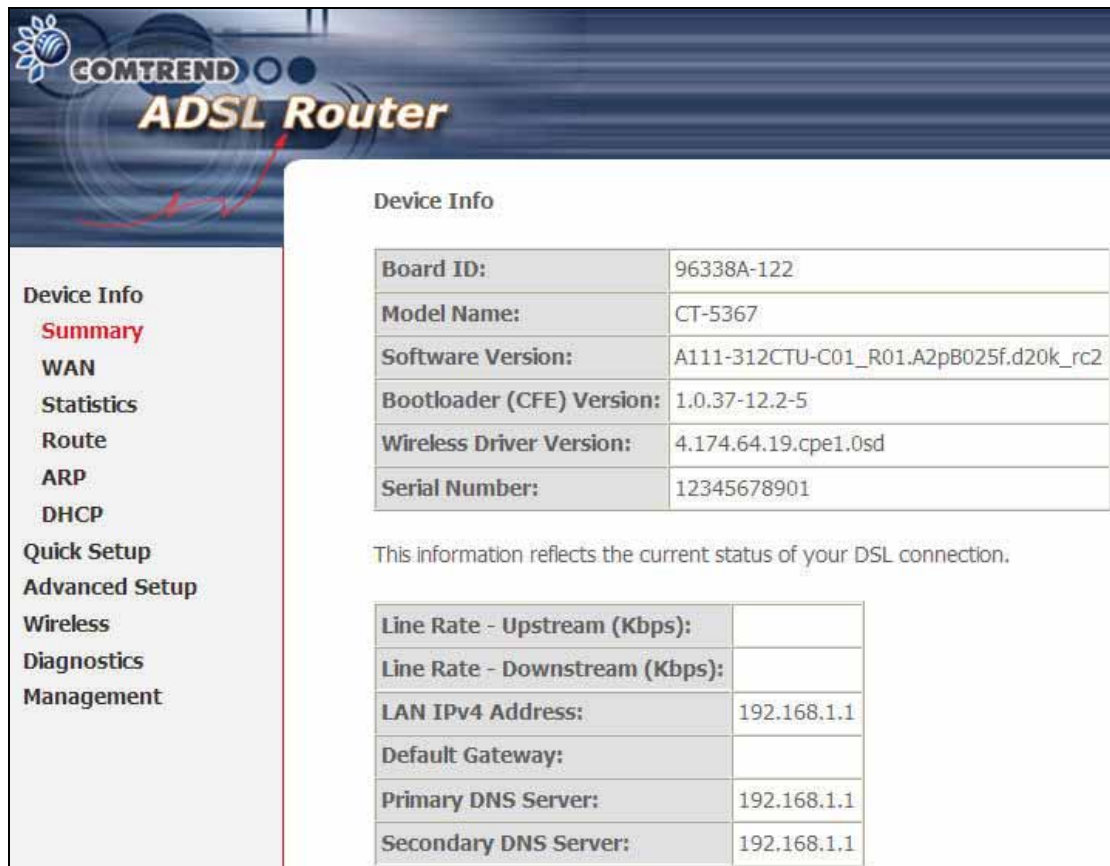
Chapter 5 Device Information

The web user interface is divided into two windowpanes, the main menu (at left) and the display screen (on the right). The main menu has the following options: Device Info, Advanced Setup, Wireless, Diagnostics, and Management. Selecting one of these options will open a submenu with more options.

NOTE: The menu items shown are based upon the configured connection and user account privileges (i.e. local or remote).

For example, in the Advanced Setup menu, 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 screenshot shows the COMTREND ADSL Router web interface. The left sidebar menu includes: Device Info (Summary, WAN, Statistics, Route, ARP, DHCP), Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area displays the 'Device Info' screen, which includes a table of device hardware and software versions, a note about the DSL connection status, and a table of IP configuration settings.

Device Info	
Board ID:	96338A-122
Model Name:	CT-5367
Software Version:	A111-312CTU-C01_R01.A2pB025f.d20k_rc2
Bootloader (CFE) Version:	1.0.37-12.2-5
Wireless Driver Version:	4.174.64.19.cpe1.0sd
Serial Number:	12345678901

This information reflects the current status of your DSL connection.

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

The Device Info Summary screen (shown above) provides summary information such as device hardware and software versions, data transmission (line rates) and the IP Configuration settings.

5.1 WAN

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

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Icmp	Nat	Firewall	QoS	State	Status	IPv4 Address
0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	ADSL Link Down	

Heading	Description
VPI/VCI	Shows the values of the ATM VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID status
Con. ID	Shows the connection ID number
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
Nat	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
QoS	Shows if IGMP IP QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IPv4 Address	Shows IPv4 address of the WAN interface

5.2 Statistics

The Statistics submenu provides detailed information for LAN and WAN interfaces.

NOTE: These statistics refresh every 15 seconds.

5.2.1 LAN Statistics

This screen shows statistics for the Ethernet interface on the LAN.

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	30572	250	0	0	181928	344	0	0
Wireless	0	0	0	0	23226	65	0	0

Heading	Description
Interface	Ethernet and Wireless interfaces
Received/Transmitted - Bytes	Rx/TX (receive/transmit) packets in bytes
- Pkts	Rx/TX (receive/transmit) packets
- Errs	Rx/TX (receive/transmit) packets with errors
- Drops	Rx/TX (receive/transmit) dropped packets

5.2.2 WAN Statistics

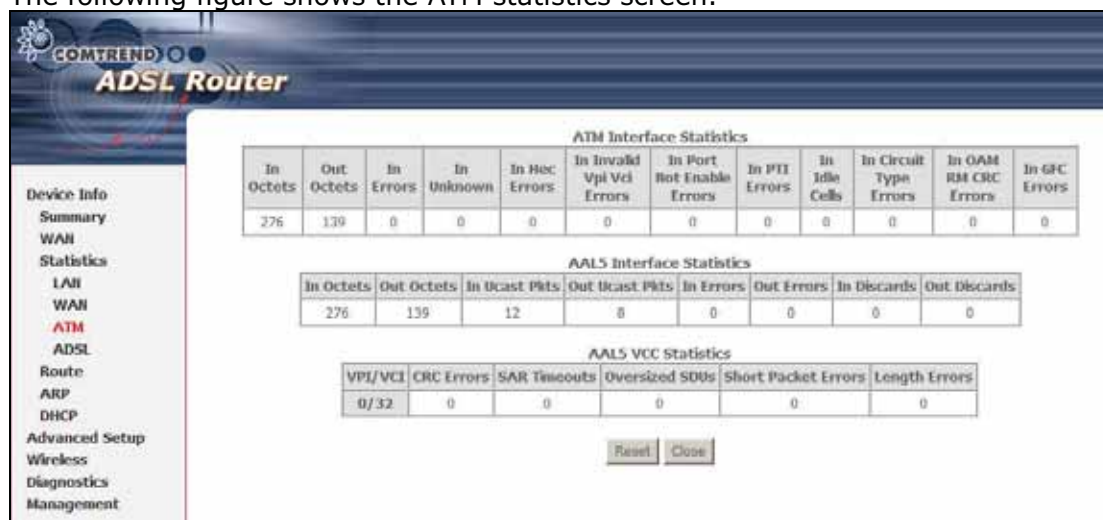
This screen shows statistics for interfaces on the WAN.

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa_0_0_35	0/0/32	PPPoA	ppp_0_0_32_1	148	7	0	0	58	4	0	0

Heading	Description
Service	WAN service label
VPI/VCI	ATM Virtual Path/Channel Identifiers
Protocol	Connection type (e.g. PPPoE, IPoA, Bridge)
Interface	Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.
Received/Transmitted	- Bytes - Pkts - Errs - Drops
	Rx/TX (receive/transmit) packets in bytes Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) packets with errors Rx/TX (receive/transmit) dropped packets

5.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

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

ATM AAL5 Layer Statistics over ADSL interface

Heading	Description
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of AAL5/AAL0 CPCS PDU octets transmitted
In Ucast Pkts	Number of received AAL5/AAL0 CPCS PDU passed to a higher-layer
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDU received from a higher layer for transmission
In Errors	Number of received AAL5/AAL0 CPCS PDU in error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDU that could not be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDU discarded due to an "input buffer overflow" condition.
Out Discards	This field is not currently used

ATM AAL5 Layer Statistics for each VCC over ADSL interface

Heading	Description
VPI/VCI	ATM Virtual Path/Channel Identifiers
CRC Errors	Number of PDUs received with CRC-32 errors
SAR Timeouts	Number of partially re-assembled PDUs that were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packet Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen in ADSL2+ mode.

COMTREND ADSL Router

Statistics -- ADSL

Mode:	ADSL2+	
Line Coding:	Trellis On	
Status:	No Defect	
Link Power State:	L0	
	Downstream	Upstream
SNR Margin (dB):	6.1	5.3
Attenuation (dB):	13.5	28.3
Output Power (dBm):	12.4	19.0
Attainable Rate (Kbps):	10888	0
Rate (Kbps):	10719	637
MSGc (number of bytes in overhead channel message):	51	16
B (number of bytes in Mux Data Frame):	190	19
M (number of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	2	3
R (number of check bytes in FEC Data Frame):	0	0
S (ratio of FEC over PMD Data Frame length):	0.5687	0.9877
L (number of bits in PMD Data Frame):	2687	162
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	6498	6564
Super Frame Errors:	4	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	4	0
OCD Errors:	1	0
LCD Errors:	0	0
Total Cells:	2667876	830136957
Data Cells:	17	301841
Bit Errors:	0	551949
Total ES:	4	251
Total SES:	0	13
Total UAS:	15	10068743

ADSL BER Test Reset Statistics

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

Heading	Description
Mode	T1.413, G.lite, G.DMT, ADSL2/2+ or Re-ADSL
Type	Channel type Interleave or Fast (not shown in all modes)
Line Coding	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, Annex L and Annex M
Status	Lists the status of the DSL link
Link Power State	Link output power state.

SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

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)

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	Max 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)

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

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

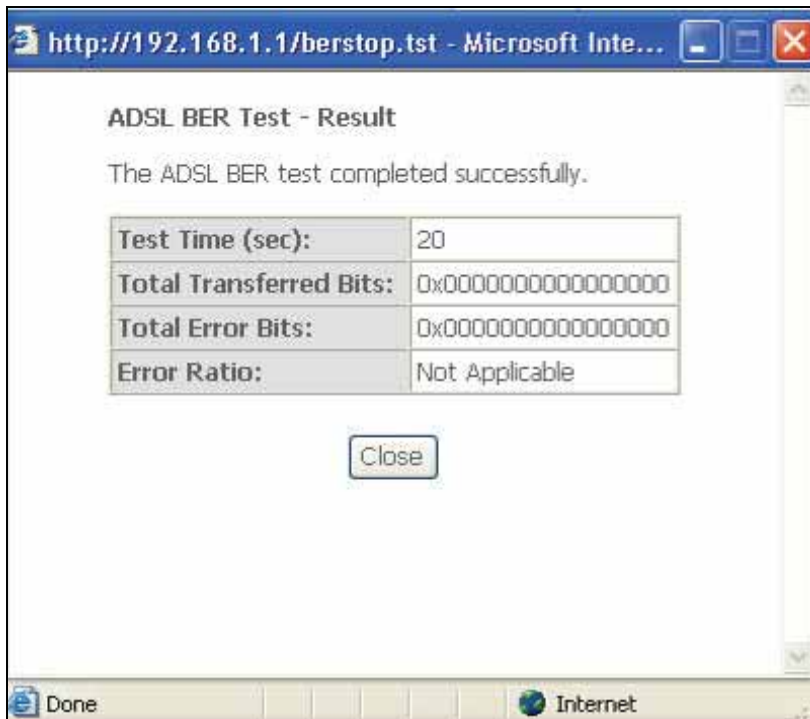
In ADSL2+ mode, the following section is inserted.

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

Within the ADSL Statistics window, a Bit Error Rate (BER) test can be started using the **ADSL BER Test** button. A small window will open when the button is pressed; it will appear as shown below. Click **Start** to start the test or **Close**.



If the test is successful, the pop-up window will display as follows.



5.3 Route

Choose Route to display the routes the device 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
172.16.114.254	0.0.0.0	255.255.255.255	UH	0	pppoa_0_0_35	ppp_0_0_32_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	172.16.114.254	0.0.0.0	UG	0	pppoa_0_0_35	ppp_0_0_32_1

Heading	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 name for WAN connection
Interface	Shows connection interfaces

5.4 ARP

Click ARP to display the ARP information.

The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP (highlighted in red), and DHCP. The main content area is titled "Device Info -- ARP" and displays a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:05:5D:A0:CD:E9	br0

Heading	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

5.5 DHCP

Click **DHCP** to display the DHCP information.

The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP, and DHCP (highlighted in red). The main content area is titled "Device Info -- DHCP Leases" and displays a table with the following data:

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

Heading	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

Chapter 6 Advanced Setup

This chapter explains the advanced setup screens in detail.

6.1 WAN

Follow the steps below to configure WAN interfaces.

- To **Add** a WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection. To remove a connection select its radio button under the **Remove** column in the table and click the **Remove** button under the table.
- To complete the **Add** or **Edit**, for a connection without VLAN Mux, proceed to **STEP 2** in section 4.2 [Manual Quick Setup](#) and on the opening screen do not choose the VLAN Mux option.
- To complete the **Add** or **Edit**, for a connection with VLAN Mux, proceed to [section 6.1.1](#) which provides detailed setup instructions.
- For advice regarding Multi-Service over PVC (MSP) see [section 6.1.2](#)
- Save/Reboot** activates the new settings by saving them and then rebooting



Heading	Description
VPI/VCI	VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
Igmp	Shows enable or disable IGMP proxy
Nat	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
QoS	Shows if IP QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Remove	To remove a connection select the radio button in this column and

	click the Remove button under the table.
Edit	Used to edit connections

6.1.1 VLAN Mux

VLAN Mux is a form of VLAN tagging that allows multiple protocols over a single connection. It is especially useful for VDSL2 connections in packet transfer mode.

Adding a new connection with VLAN Mux is accomplished by selecting the **VLAN Mux – Enable Multiple Protocols Over a Single PVC** check box (outlined in red below). Enter a value for **802.Q VLAN ID** in the box that appears below the checkbox. Click **Next** to continue to connection type selection.

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

VLAN Mux - Enable Multiple Protocols Over a Single PVC

802.1Q VLAN ID: [0-4095]

Service Category:

As shown below, you can choose from PPPoE, MER or Bridging connection types. Notice that PPPoA and IPoA are not shown. Select the connection type you wish to establish and then proceed according to the corresponding connection specific instructions found in Chapter 4.

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.

PPP over Ethernet (PPPoE)
 MAC Encapsulation Routing (MER)
 Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING ▼

Multiple PVCs can be added to connections sharing the same PORT/VPI/VCI values by repeating the procedure above, as long as the 802.1Q VLAN IDs differ. However, only one Bridge, one MER and four PPPoE connections can coexist on the same connection. The figure below shows an example of three protocols sharing the same connection.

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
 Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	Firewall	QoS	State	Remove	Edit
0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>
0/35	Off	2	UBR	br_0_0_35	nas_0_0_35_1	Bridge	N/A	N/A	N/A	Disabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>
0/35	2	3	UBR	br_0_0_35.2	ppp_0_0_35_3	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

6.1.2 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the VLAN Mux function, PPPoE, Bridge and MER protocols can coexist, while IPoA and PPPoA are not supported. This function supports remote management by bridge protocol in addition to multimedia applications over a single PVC.

Configuring MSP is a two-part process:

- Part 1** - Create multiple PVCs (One Bridge + multiple PPPoE / One MER)
- Part 2** - Use Interface Group to connect LAN / WAN interfaces

NOTE: The example below shows how to configure a Bridge / PPPoE MSP connection. Use the same process for Bridge / MER MSP connections.

If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections.

If a MSP connection is removed every other MSP connection should be removed to avoid Interface Group configuration problems.

PART 1 – CREATE MULTIPLE PVCs

On the Advanced Setup – WAN screen, create one PPPoE connection and one Bridge connection on the MSP supporting PVC. The screen will display as follows.

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	Firewall	QoS	State	Remove	Edit
0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/35	Off	2	UBR	br_0_0_35	nas_0_0_35_1	Bridge	N/A	N/A	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit

PART 2

Go to Advanced Setup – Interface Group (see [section 6.10](#)) and select the **Enable Virtual Ports** checkbox. The screen will display as follows.

Enable virtual ports on

Group Name	Remove	Edit	Interfaces
Default			Wireless(SSID1)
			nas_0_0_35_1
			ENET1
			ENET2
			ENET3
ENET4			

NOTE: Only hardware and bridge interfaces are listed. Bridge interfaces are shown as "nas_x_y_z" where x=port, y=vpi, and z=vci.

To continue, click the **Add** button at the bottom of the screen shown above. On the screen shown below, select the bridge connection and one Ethernet virtual port (ENET 1-4). Enter a group name, such as "MSP1", and click **Save/Apply**.

Group Name:

Grouped Interfaces

ENET4
nas_0_0_35_1

Available Interfaces

ENET1
ENET2
ENET3
Wireless(SSID1)

Automatically Add Clients With the following DHCP Vendor IDs

If successfully configured, the Interface Group screen will display as follows.

Interface Group -- A maximum 16 entries can be configured

Interface Group 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.

Enable virtual ports on

Group Name	Remove	Edit	Interfaces
Default			Wireless(SSID1)
			ENET1
			ENET2
			ENET3
MSP1	<input type="checkbox"/>	<input type="button" value="Edit"/>	nas_0_0_35_1 ENET4

-45-

6.2 LAN

This screen allows the user to configure the LAN Interface on the device.

The screenshot shows the 'Local Area Network (LAN) Setup' page of a COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Parental Control, Quality of Service, Routing, DNS, DSL, Interface Group, Certificate, Wireless, Diagnostics, and Management. The main content area is titled 'Local Area Network (LAN) Setup' and contains the following fields and options:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Enable UPnP
- Enable IGMP Snooping
 - Standard Mode
 - Blocking Mode
- Enhanced IGMP
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address: 192.168.1.2
 - End IP Address: 192.168.1.254
 - Leased Time (hour): 24
- Configure the second IP Address and Subnet Mask for LAN interface
- Ethernet Media Type**
 - Port 1: Auto
 - Port 2: Auto
 - Port 3: Auto
 - Port 4: Auto

At the bottom right are 'Save' and 'Save/Reboot' buttons.

NOTE: NAT is enabled above so **UPnP** is shown and **DHCP Server Relay** is hidden (see underlined notes below).

IP ADDRESS

Enter the IP address for the LAN port.

SUBNET MASK

Enter the subnet mask for the LAN port.

ENABLE UPNP

Tick the box to enable Universal Plug and Play.

This option is hidden when NAT disabled or if no PVC exists

ENABLE IGMP SNOOPING:

Enable by ticking the box.

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

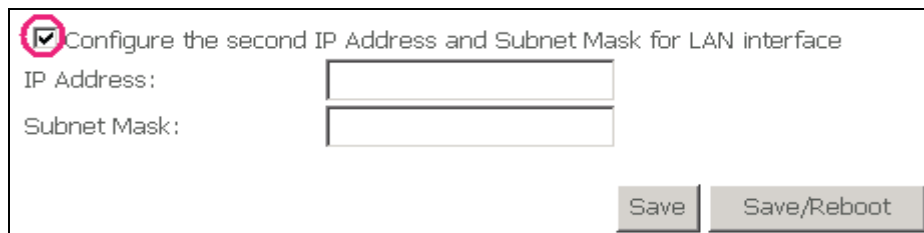
client subscriptions to any multicast group.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter starting and ending 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.

DHCP SERVER RELAY

Enable with checkbox and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. *This option is hidden if NAT is enabled*

Configure the second IP address by ticking the checkbox shown below.



Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

Save Save/Reboot

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

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

ETHERNET MEDIA TYPE

Select between Auto, 10_Half, 10_Full, 100_Half and 100_Full options.

NOTE: The **Save** button saves new settings to allow continued configuration while the **Save/Reboot** button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

6.3 NAT

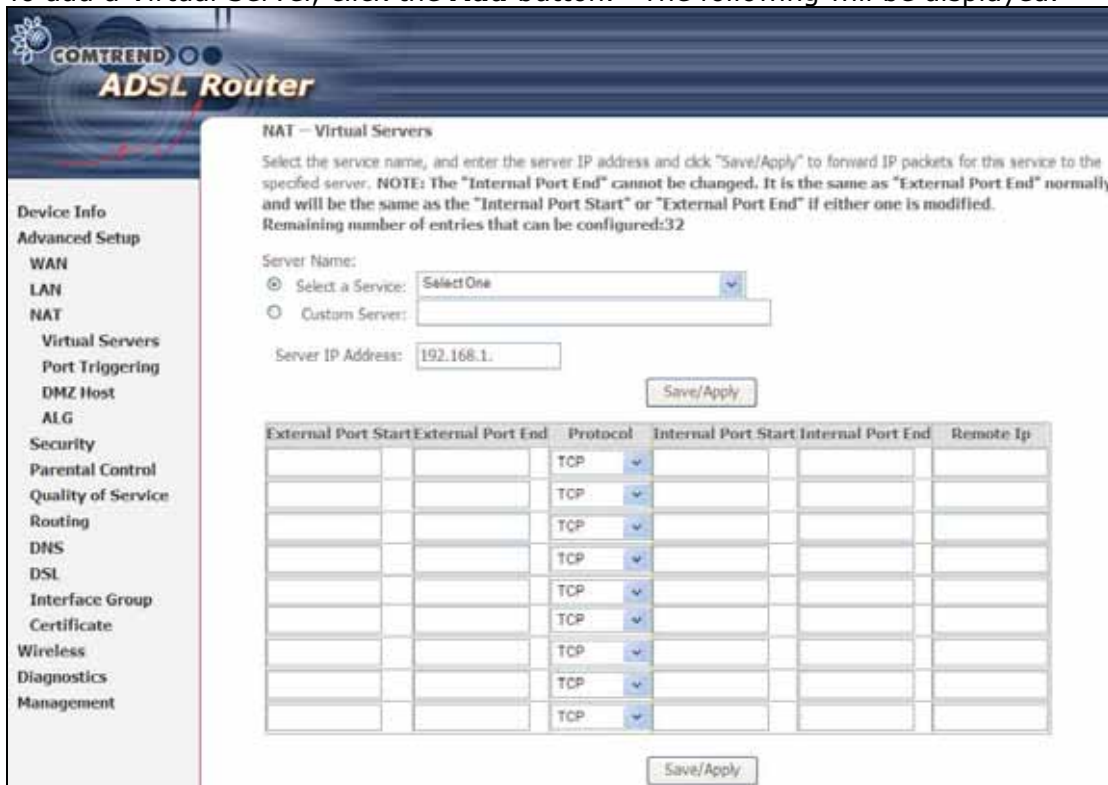
To display this option, NAT must be enabled in at least one PVC shown on the [Advanced WAN Setup](#) screen. *(NAT is not an available option in Bridge mode)*

6.3.1 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.



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

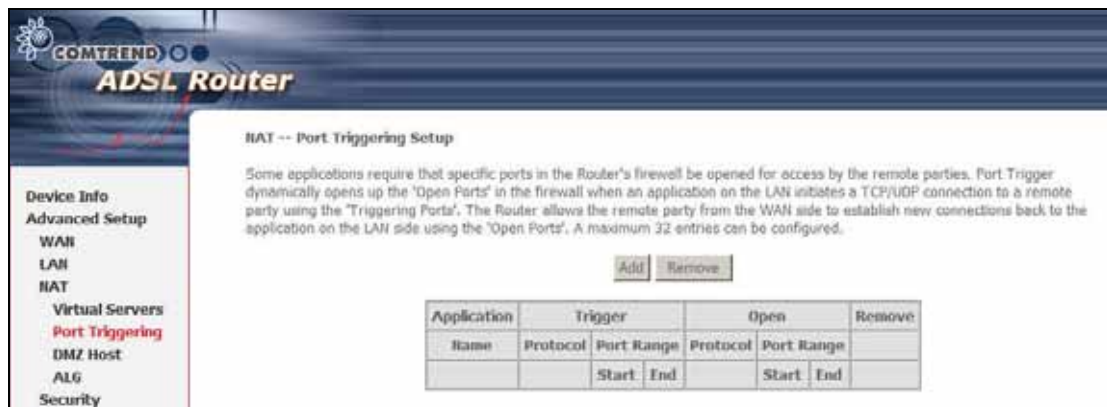


Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the 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	User can select from 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

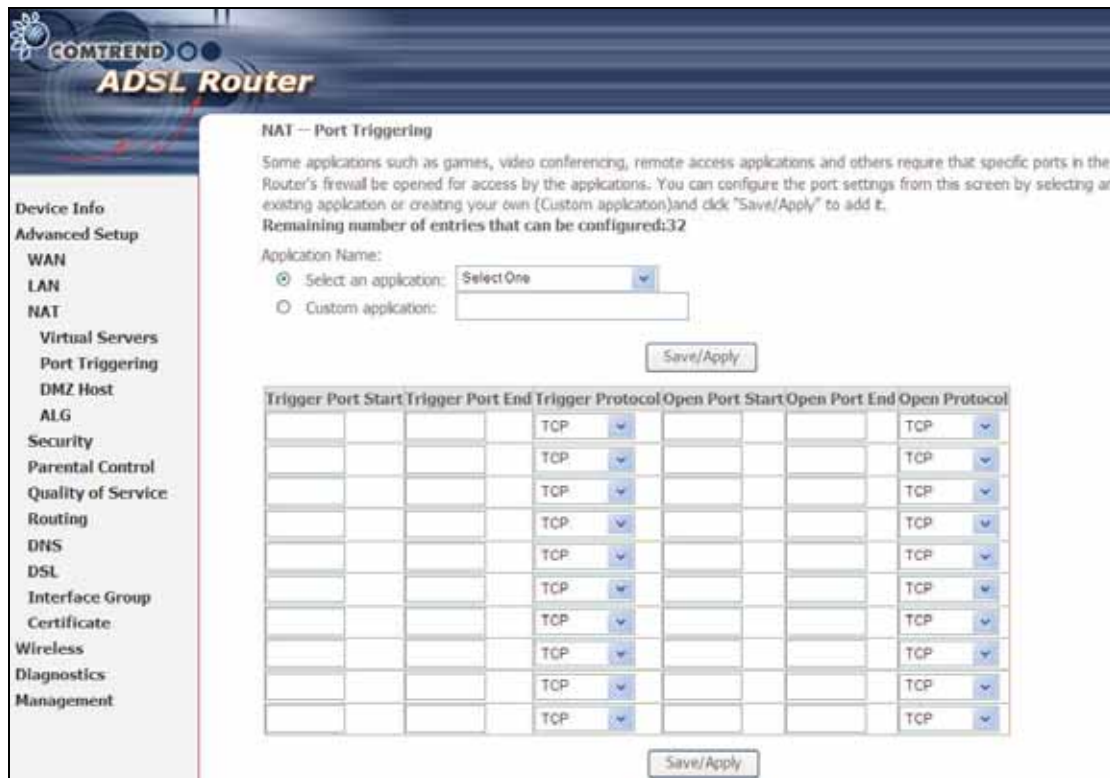
	Custom Server). When a service is selected, the port ranges are automatically configured.
Remote IP	The IP address of the remote host

6.3.2 Port Triggering

Some applications require that specific ports in the 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 of 32 entries can be configured.



To add a Trigger Port, click the **Add** button. The following screen will display.



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 trigger port end number (for custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	User can select from 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 open port end number (for custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	User can select from TCP, TCP/UDP, or UDP.

6.3.3 DMZ Host

The device 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.

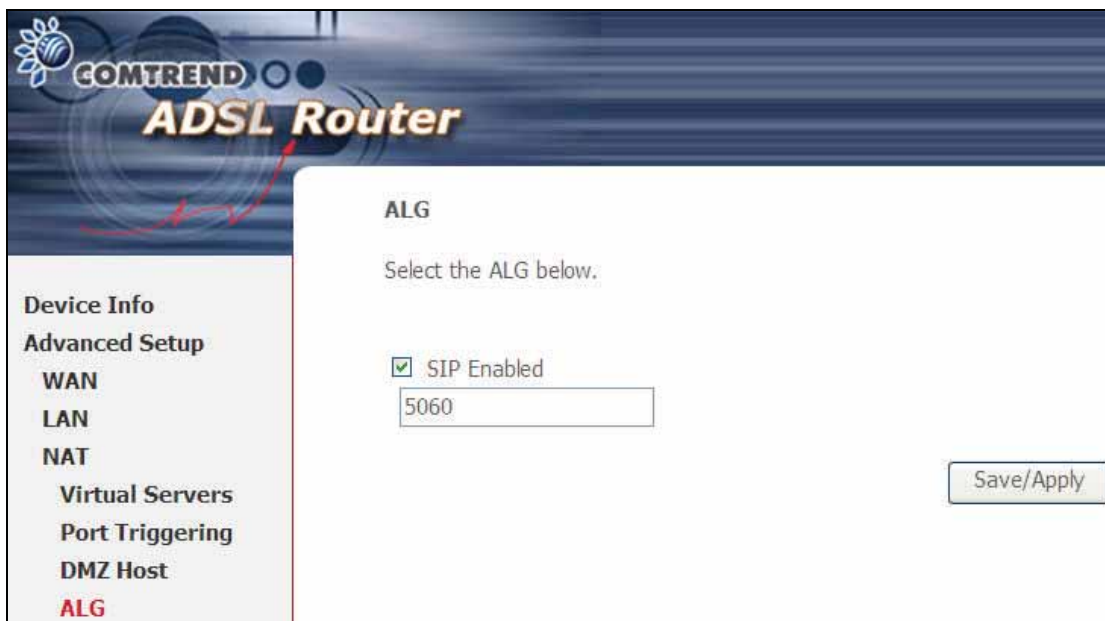
Clear the IP address field and click **Apply** to deactivate the DMZ host.



6.3.4 ALG

SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) devices to initiate communication. A SIP ALG (Application Layer Gateway) assists VoIP packet traffic from a SIP-compliant IP phone or VoIP gateway to passthrough a NAT enabled router.

To enable the SIP ALG select the **SIP Enabled** checkbox and click **Save/Apply**.



NOTE: ALG is only valid for SIP protocol running on UDP port 5060.

6.4 Security

To display this option, the Firewall checkbox must be enabled in at least one PVC shown on the [Advanced WAN Setup](#) screen.

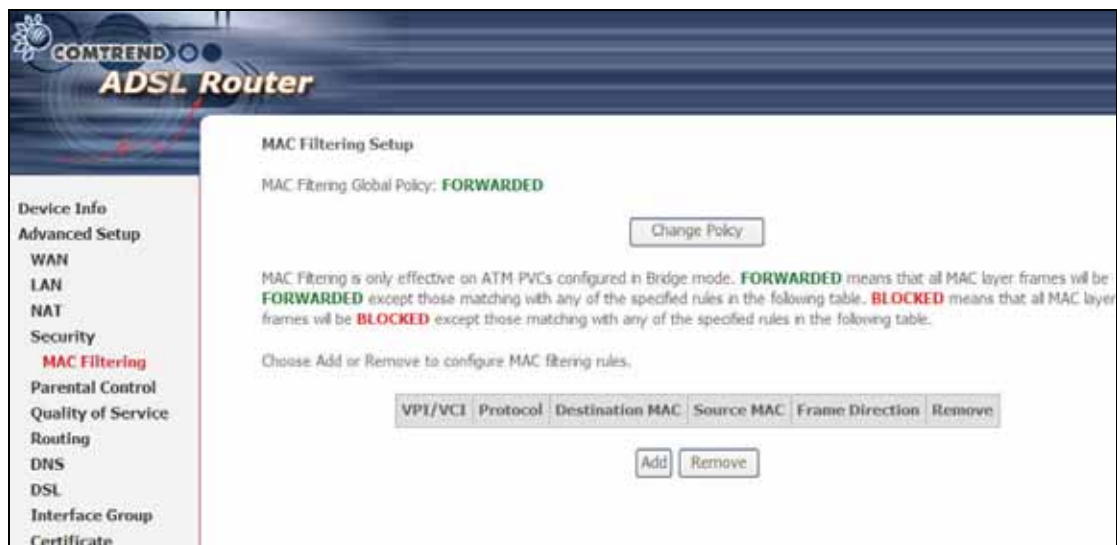
NOTE: For a more technical discussion of this topic, see [Appendix A: Security](#).

6.4.1 MAC Filtering

NOTE: This function is only available when in bridge mode. Other connection modes (e.g. PPPoE) use [IP Filtering](#) (pg. 53) which performs 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-5367 can be set according to the following procedure.

The **FORWARDED** policy means that all MAC layer frames will be **FORWARDED** except those matching the rules specified in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the rules specified in the following table. The default policy is **FORWARDED**. This can be changed by clicking the **Change Policy** button.



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.



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 filter to selected PVCs (bridge mode only). Filter rules are arranged according to PVC, as shown under the VPI/VCI heading on the previous screen.

6.4.2 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 of IP Filtering, [MAC Filtering](#) (pg. 52) performs a similar function.

OUTGOING IP FILTER

The default setting for Outgoing traffic is **ACCEPTED**. Under this condition, all outgoing IP packets that match the filter rules will be **BLOCKED**.



To add a filtering rule, click the **Add** button. The following screen will display.

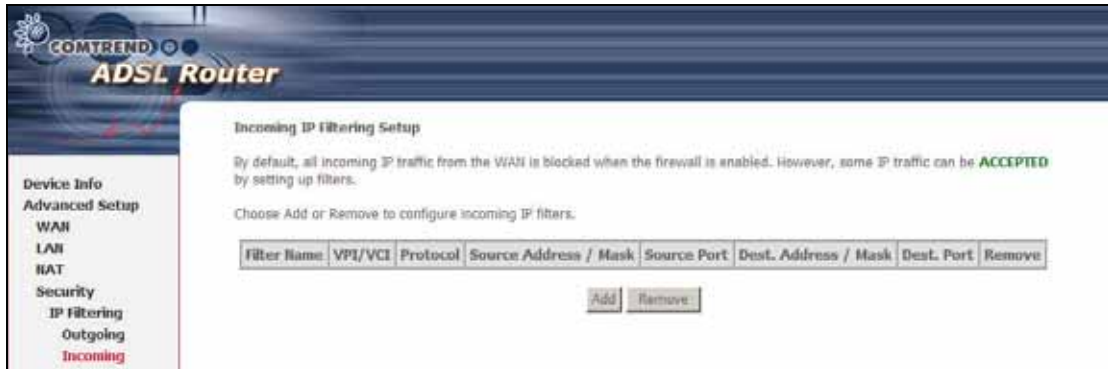


Click **Save/Apply** to save and activate the filter.

Field	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

The default setting for all Incoming traffic is **BLOCKED**. Under this condition, only those incoming IP packets that match the filter rules will be **ACCEPTED**.



To add a filtering rule, click the **Add** button. The following screen will display.



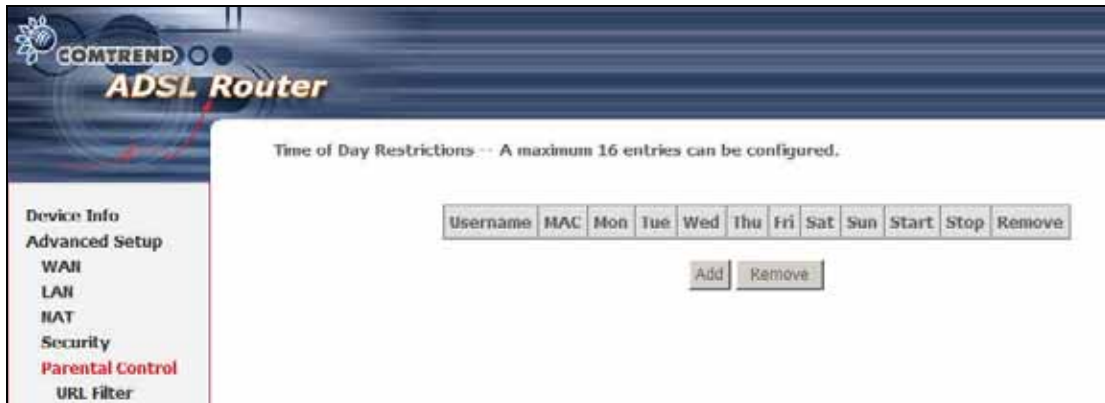
For detailed field descriptions, please reference the [Outgoing IP Filter](#) table.

Under WAN Interfaces, select the PVCs (routing mode with firewall only) where the filter rule will apply. You may select every PVC or just a subset. Filter rules are arranged by PVC as shown under the VPI/VCI heading on the previous screen.

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

6.5 Parental Control

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section [9.4 Internet Time](#), so that the scheduled times match your local time.



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

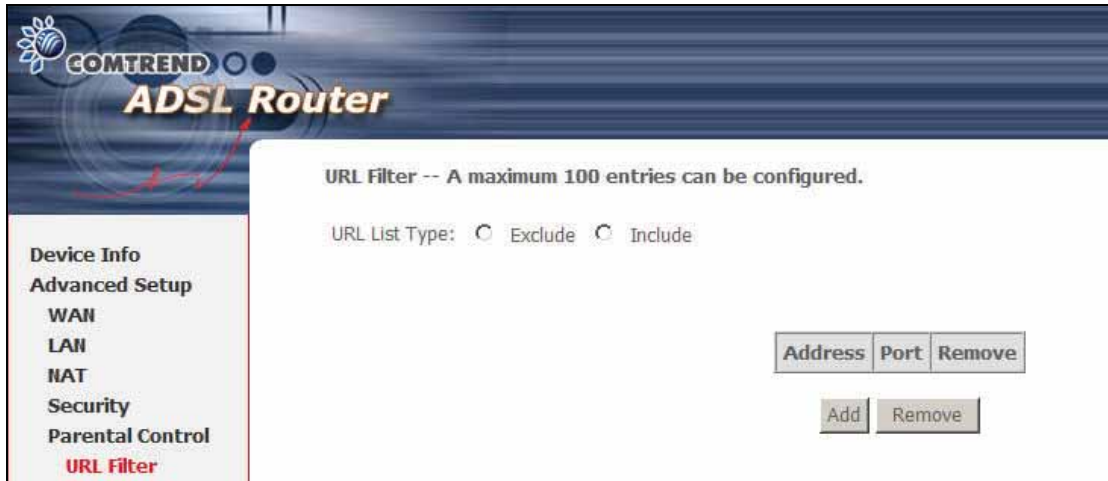


See below for field definitions. Select settings and click **Save/Apply**.

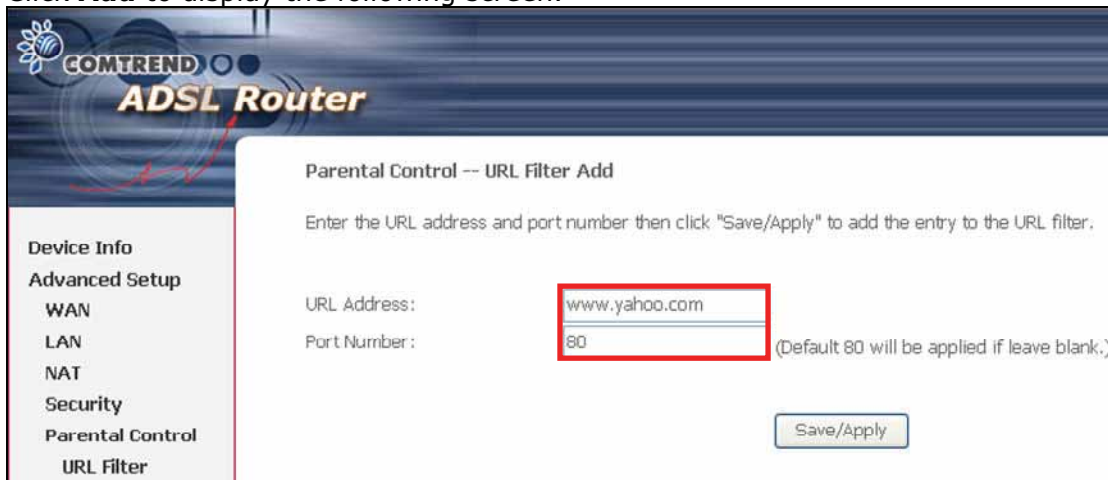
Field	Description
User Name	A user-defined label for this restriction.
Browser's MAC Address	MAC address of the PC running the browser.
Other MAC Address	MAC address of another LAN device.
Days of the Week	The days the restrictions apply.
Start Blocking Time	The time the restrictions start.
End Blocking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

6.5.1 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.



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



Enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter. The URL Address must begin with "www", as shown above.



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.

6.6 Quality of Service

NOTE: QoS must be enabled in at least one PVC to display this option.
(see [Advanced Setup - WAN](#) for detailed PVC setup instructions).

6.6.1 Queue Management Configuration

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.

To Enable QoS tick the checkbox and select a Default DSCP Mark.
Click **Save/Apply** to activate QoS.



6.6.2 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 Configuration -- A maximum 24 entries can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	8	8		

Buttons: Add, Remove, Save/Reboot

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

QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

Queue:

Queue Precedence:

Save/Apply

- Queue Configuration Status:** Enable/Disable the Queue entry.
- Queue:** Assign the entry to a specific network interface (QoS must be enabled).
- Queue Precedence:** Configure precedence for the Queue entry. Lower integer values for precedence imply higher priority for this entry relative to others.

6.6.3 QoS Classification

The network traffic classes are listed in this format:

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

MARK				TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Save/Apply"/>																	

Click **Add** to configure network traffic classes.

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 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Assign ATM Priority and/or DSCP Mark for the class

If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Physical LAN Port:

Protocol:

Differentiated Services Code Point (DSCP) Check:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

SET-2

802.1p Priority:

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition from either SET-1 or SET-2. All the conditions specified in the rule must be satisfied for it to take effect. Click **Save/Apply** to save and activate the rule.

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last or null are the only options.
Rule Status	Disable or enable the rule.
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.
Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Mark 802.1p if 802.1q is enabled	Select between 0-7. The lower the digit shows the higher the priority.
SET-1	
Physical LAN Port	Select between ENET (1-4), Wireless and Wireless_Guest.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Differentiated Services Code Point (DSCP) Check	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Static IP or DHCP ID drop-down box	Select IP Address, Vendor Class ID (DHCP Option 60), or User Class ID (DHCP Option 77)
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
UDP/TCP Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
UDP/TCP Destination Port (port or port:port)	Enter destination port number or port range.
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.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

6.7 Routing

This option allows for Default Gateway, Static Route, and RIP configuration.

NOTE: In bridge mode, the RIP screen is hidden while the Default Gateway and Static Route configuration screens are shown but ineffective.

6.7.1 Default Gateway

If the **ENABLE AUTOMATIC ASSIGNED DEFAULT GATEWAY** checkbox is selected, this device will accept the first received default gateway assignment from one of the enabled routing PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply** button to save it.

The screenshot shows the 'Routing -- Default Gateway' configuration page. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Parental Control, Quality of Service, Routing (Default Gateway, Static Route, RIP), DNS, DSL, Interface Group, Certificate, Wireless, Diagnostics, and Management. The main content area has the title 'Routing -- Default Gateway' and a descriptive paragraph: 'If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.' Below this is a note: 'NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.' There are three checkboxes: 'Enable Automatic Assigned Default Gateway' (unchecked), 'Use Default Gateway IP Address' (unchecked) with an empty text input field, and 'Use Interface' (unchecked) with a dropdown menu showing 'pppoe_0_0_35_1/ppp_0_0_35_1'. A 'Save/Apply' button is at the bottom right.

NOTE: After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.

6.7.2 Static Route

The Static Route screen lists the configured static routes.

The screenshot shows the 'Routing -- Static Route (A maximum 32 entries can be configured)' configuration page. The left navigation menu is the same as in the previous screenshot, with 'Static Route' highlighted in red. The main content area has the title 'Routing -- Static Route (A maximum 32 entries can be configured)'. Below the title is a table with five columns: 'Destination', 'Subnet Mask', 'Gateway', 'Interface', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

Clicking the **Add** button displays the following screen.



Enter Destination Network Address, Subnet Mask, Gateway IP Address, and/or WAN Interface. Then click **Save/Apply** to add the entry to the routing table.

6.7.3 RIP

To activate this option, select the **Enabled** radio button for **Global RIP Mode**. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the **Enabled** checkbox for the interface. Click the **Save/Apply** button to save the configuration and to start or stop RIP based on the Global RIP mode selected.



6.8 DNS

6.8.1 DNS Server

If the **Enable Automatic Assigned DNS** checkbox is selected, this device will accept the first received DNS assignment from one of the DHCP enabled PVC(s) – (PPPoA, PPPoE, or MER) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.



The screenshot shows the 'DNS Server Configuration' page of a COMTREND ADSL Router. The page has a dark blue header with the 'COMTREND ADSL Router' logo. On the left, there is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Parental Control, Quality of Service, Routing, DNS (DNS Server, Dynamic DNS), and Dynamic DNS. The main content area is titled 'DNS Server Configuration' and contains the following text: 'If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.' Below this text is a checkbox labeled 'Enable Automatic Assigned DNS'. Underneath are two input fields: 'Primary DNS server:' and 'Secondary DNS server:'. A 'Save' button is located at the bottom right of the configuration area.

NOTE: Click the **Save** button to save the new configuration. Remember, the device must be rebooted to make the new configuration effective.


6.8.2 Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of many domains, allowing the CT-5367 to be more easily accessed from various locations on the Internet.



The screenshot shows the 'Dynamic DNS' configuration page of a COMTREND ADSL Router. The page has a dark blue header with the 'COMTREND ADSL Router' logo. On the left, there is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Parental Control, Quality of Service, Routing, DNS (DNS Server, Dynamic DNS), and Dynamic DNS. The main content area is titled 'Dynamic DNS' and contains the following text: 'The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.' Below this text is a sub-header: 'Choose Add or Remove to configure Dynamic DNS.' Underneath is a table with five columns: 'Hostname', 'Username', 'Service', 'Interface', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

To add a dynamic DNS service, click the **Add** button and this screen will display.



COMTREND
ADSL Router

Add dynamic DDNS

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

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

Device Info
Advanced Setup
 WAN
 LAN
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DNS
 DNS Server
 Dynamic DNS
 DSL
 Interface Group
 Certificate

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

6.9 DSL

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

COMTREND ADSL Router

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Capability

- Bitswap Enable
- SRA Enable

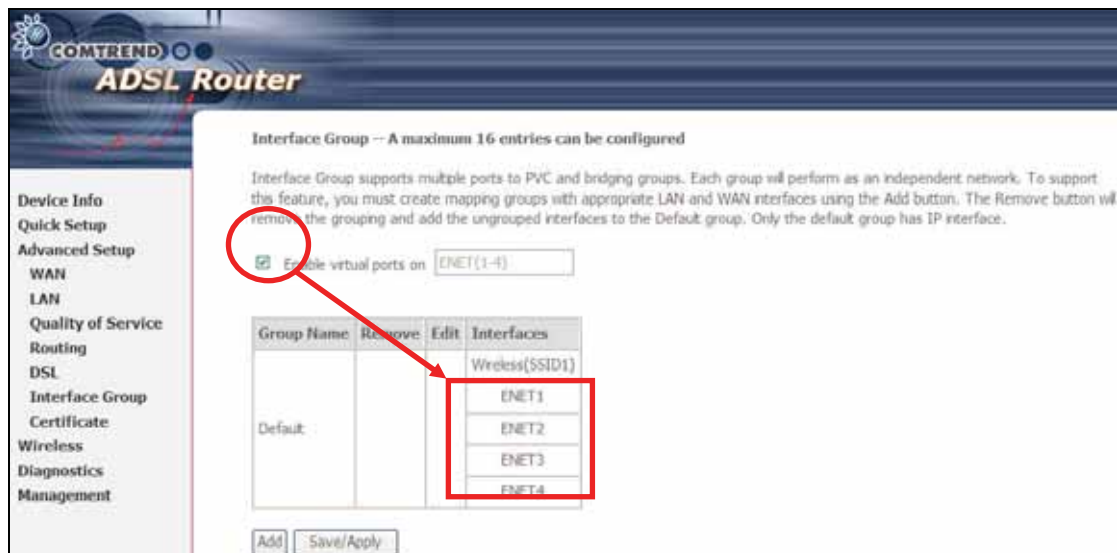
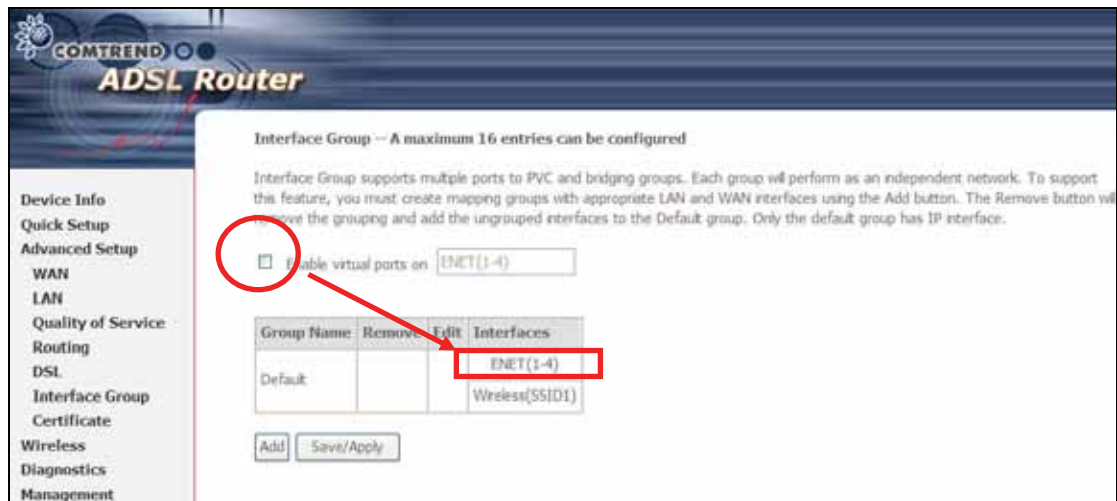
Apply

DSL Mode	Data Transmission Rate - Mbit/s (Megabits per second)
G.Dmt	Downstream: 12 Mbit/s Upstream: 1.3 Mbit/s
G.lite	Downstream: 4 Mbit/s Upstream: 0.5 Mbit/s
T1.413	Downstream: 8 Mbit/s Upstream: 1.0 Mbit/s
ADSL2	Downstream: 12 Mbit/s Upstream: 1.0 Mbit/s
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbit/s Upstream: 1.0 Mbit/s
AnnexM	Downstream: 24 Mbit/s Upstream: 3.5 Mbit/s
Options	Description
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)

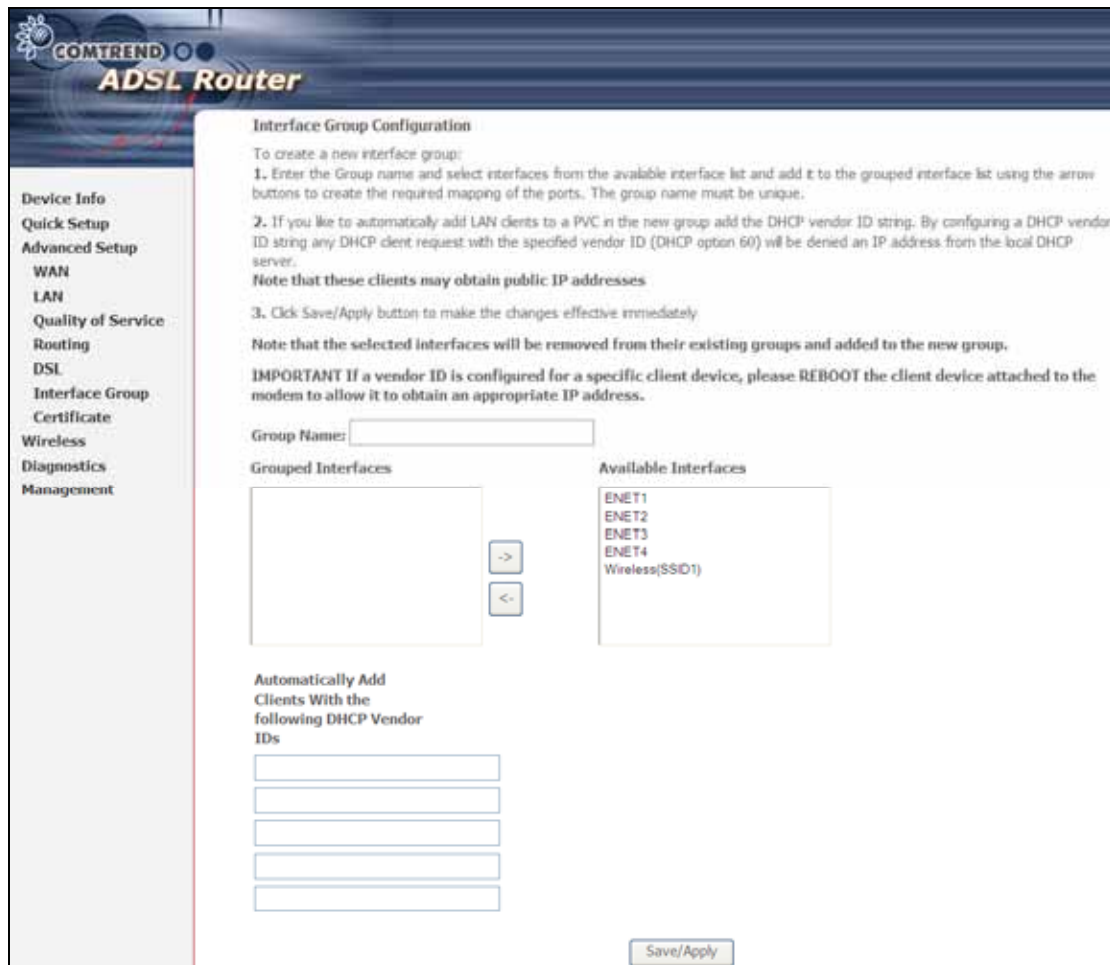
6.10 Interface Group

Interface Group supports multiple port 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.

As shown in these two figures, when you tick the **Enable virtual ports on**, the LAN interfaces, ENET(1-4) in the first figure, will separate into four virtual ports.



To add an Interface Group, click the **Add** button.



To create a group from the list, first enter the group name and then select from the available interfaces on the list.

Automatically Add Clients With the 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 is turned on when Interface Grouping is enabled.

There are four PVCs (0/33, 0/36, 0/37, 0/38); VPI/VCI 0/33 is for PPPoE and the others are for IP setup-box. The LAN interfaces are ETH1-4.

Interface Group configuration is:

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".

The CPE's DHCP server runs on "Default". In addition, the ISP's DHCP server is running on PVC 0/36. It is for setup-box use only. On the LAN side, the PC can get an IP address from the CPE's DHCP server and access Internet via PPPoE (0/33).

If the setup-box was connected with interface "ENET1" and sent a DHCP request with vendor id "Video", the CPE's DHCP server will forward this request to the ISP's DHCP server. The CPE will then change the Interface Grouping configuration automatically. The Interface Grouping configuration becomes:

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

6.11 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

6.11.1 Local



The screenshot shows the Comtrend ADSL Router web interface. The main heading is "Local Certificates". Below the heading, there is a text box that reads: "Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored." Below this text, there is a table with the following columns: "Name", "In Use", "Subject", "Type", and "Action". Below the table, there are two buttons: "Create Certificate Request" and "Import Certificate". On the left side of the interface, there is a navigation menu with the following items: "Device Info", "Quick Setup", "Advanced Setup", "WAN", "LAN", "Quality of Service", "Routing", "DSL", "Interface Group", "Certificate", "Local", "Trusted CA", "Wireless", "Diagnostics", and "Management".

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 for this information if necessary.

COMTREND
ADSL Router

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:

Device Info
Quick Setup
Advanced Setup
 WAN
 LAN
 Quality of Service
 Routing
 DSL
 Interface Group
 Certificate
 Local
 Trusted CA
 Wireless
 Diagnostics
 Management

Click **Apply** to generate a private key and a certificate-signing request.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, it is 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 private key provided by your vendor/ISP/ITSP.

The screenshot displays the 'Import certificate' configuration page on a COMTREND ADSL Router. The page is titled 'Import certificate' and includes the instruction: 'Enter certificate name, paste certificate content and private key.' The interface features a sidebar on the left with navigation options: Device Info, Quick Setup, Advanced Setup, WAN, LAN, Quality of Service, Routing, DSL, Interface Group, Certificate (selected), Local, Trusted CA, Wireless, Diagnostics, and Management. The main content area has three sections: 'Certificate Name' with a text input field; 'Certificate:' with a large text area containing the placeholder text '-----BEGIN CERTIFICATE-----', '<insert certificate here>', and '-----END CERTIFICATE-----'; and 'Private Key:' with another large text area containing the placeholder text '-----BEGIN RSA PRIVATE KEY-----', '<insert private key here>', and '-----END RSA PRIVATE KEY-----'. An 'Apply' button is located at the bottom right of the page.

6.11.2 Trusted CA

Certificate Authority (CA) is part of the X.509 authentication system. It is itself a certificate, attached with the owner information of the certificate authority; but its purpose is not encryption/decryption, instead it validates other certificates.



Click **Import Certificate** to paste the certificate content of your trusted CA. The 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.



Chapter 7 Wireless

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

7.1 Basic

The Basic option 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 **Save/Apply** to apply the selected wireless options.

Consult the table below for descriptions of these options.

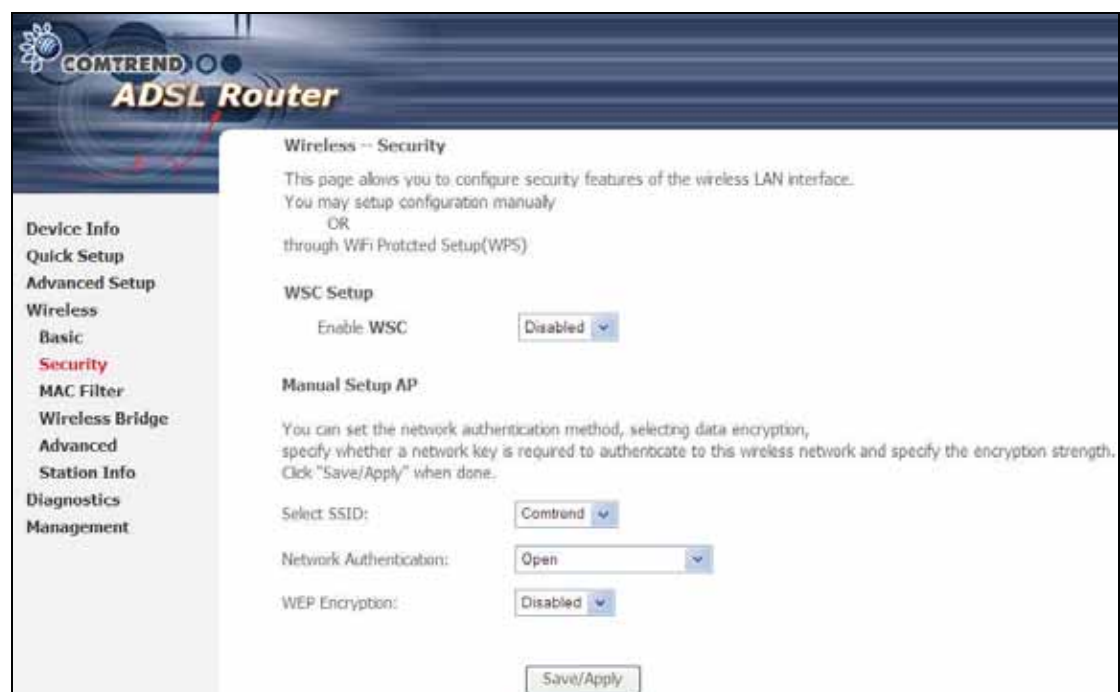
Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network → Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
Clients Isolation	<ol style="list-style-type: none"> Prevents clients PC from seeing one another in My Network Places or Network Neighborhood. Prevents one wireless client communicating with another wireless client.
Disable WMM	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for

Advertise	time-sensitive applications (e.g. VoIP, Video). <small>(wireless software version 3.10 and above)</small>
SSID	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. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium 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. Each county listed in the menu enforces specific regulations limiting 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.

7.2 Security

WIRELESS SECURITY

The wireless security screen (shown below) allows for configuration of wireless security settings according to WiFi Simple Configuration (WSC) or Manual Setup methods. The WSC method automatically configures security settings using Wi-Fi Protected Setup (WPS). In comparison, the Manual method requires the user to select and enter all these settings for every device on the WLAN.



Manual Setup AP settings are described in the table below.

Select SSID

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. 802.11 protocols support two types of network authentication services: open system and shared key.

Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

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.

Select SSID:	Comtrend
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:	
Network Key 2:	
Network Key 3:	
Network Key 4:	

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

Save/Apply

The settings for WPA authentication are shown below.

Select SSID:	Comtrend
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
<input type="button" value="Save/Apply"/>	

The settings for WPA-PSK authentication are shown below.

Select SSID:	Comtrend
Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	<input type="text"/> Click here to display
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP
WEP Encryption:	Disabled
<input type="button" value="Save/Apply"/>	

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.

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. FYI: Each key contains a 24-bit header (an initiation

vector) which enables parallel decoding of multiple streams of encrypted data.

7.2.1 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-5367 has both a WPS button on the rear panel and a virtual button accessed from the web user interface (WUI).

Devices with the WPS logo (shown here) support WPS. However, the WPS logo might not be present on your device. 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. WSC SETUP

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

A screenshot of the WSC Setup configuration page. It shows the text 'WSC Setup' at the top, followed by 'Enable WSC' and a dropdown menu currently set to 'Enabled'.

Step 2: Set the WSC AP Mode. **Configured** is used when the CT-5367 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the CT-5367.

A screenshot of the 'Set WSC AP Mode' configuration page. It shows the text 'Set WSC AP Mode' and a dropdown menu currently set to 'Configured'.

NOTE1: Your client may or may not have the ability to provide security settings to the CT-5367. If it does not, then you must set the WSC AP mode to Configured. Consult the device documentation to check its capabilities.

NOTE2: If you are running Windows Vista you can add an external registrar using the **StartAddER** button (Appendix E 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 "Save/Apply" when done.

Select SSID: Comtrend

Network Authentication: WPA2-PSK

WPA Pre-Shared Key: [Redacted]

WPA Group Rekey Interval: 0

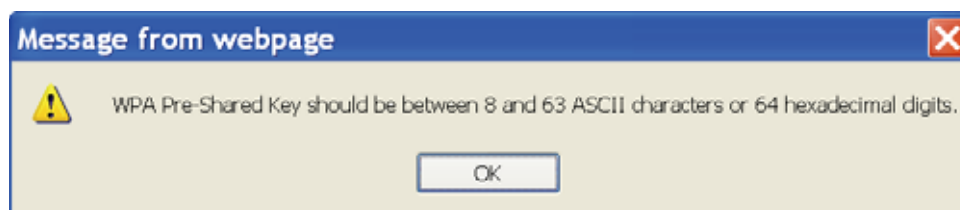
WPA Encryption: AES

WEP Encryption: Disabled

Save/Apply

Step 3

Step 4: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



Step 5: 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: 1st 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.

2nd 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)

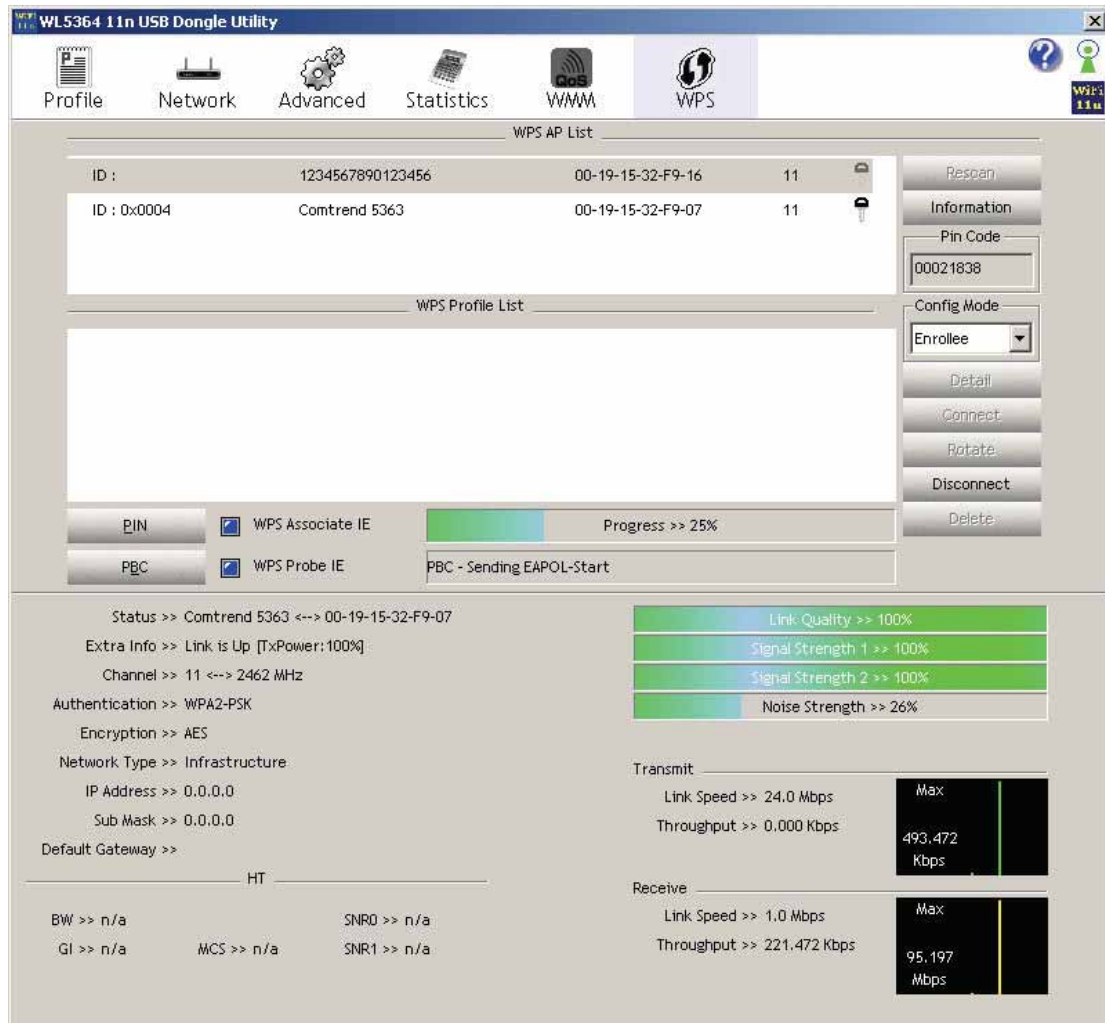
Push-Button PIN

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

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

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.



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

IIIB. WPS – PIN CONFIGURATION

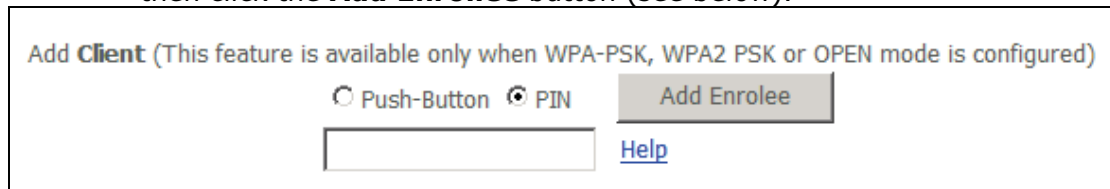
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific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

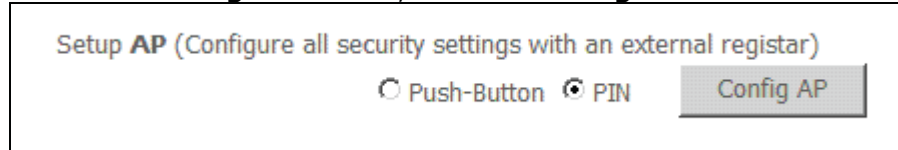
Step 6: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

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



The screenshot shows a configuration window titled "Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)". It contains two radio buttons: "Push-Button" (unselected) and "PIN" (selected). To the right of the radio buttons is a grey button labeled "Add Enrollee". Below the radio buttons is a text input field and a blue "Help" link.

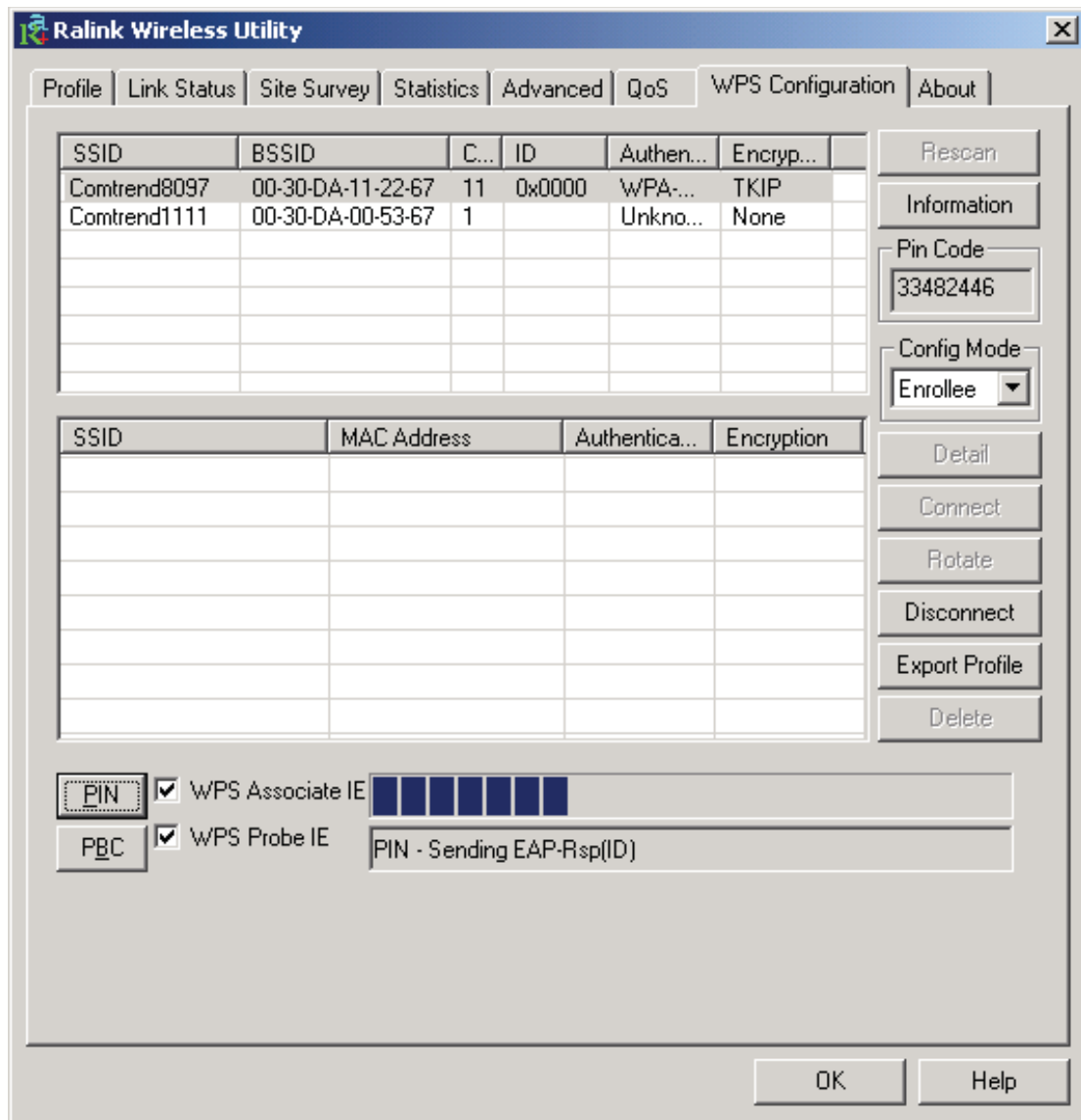
B - For **Unconfigured** mode, click the **Config AP** button.



The screenshot shows a configuration window titled "Setup AP (Configure all security settings with an external registrar)". It contains two radio buttons: "Push-Button" (unselected) and "PIN" (selected). To the right of the radio buttons is a grey button labeled "Config AP".

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 than the External Registrar function provided in Windows Vista.

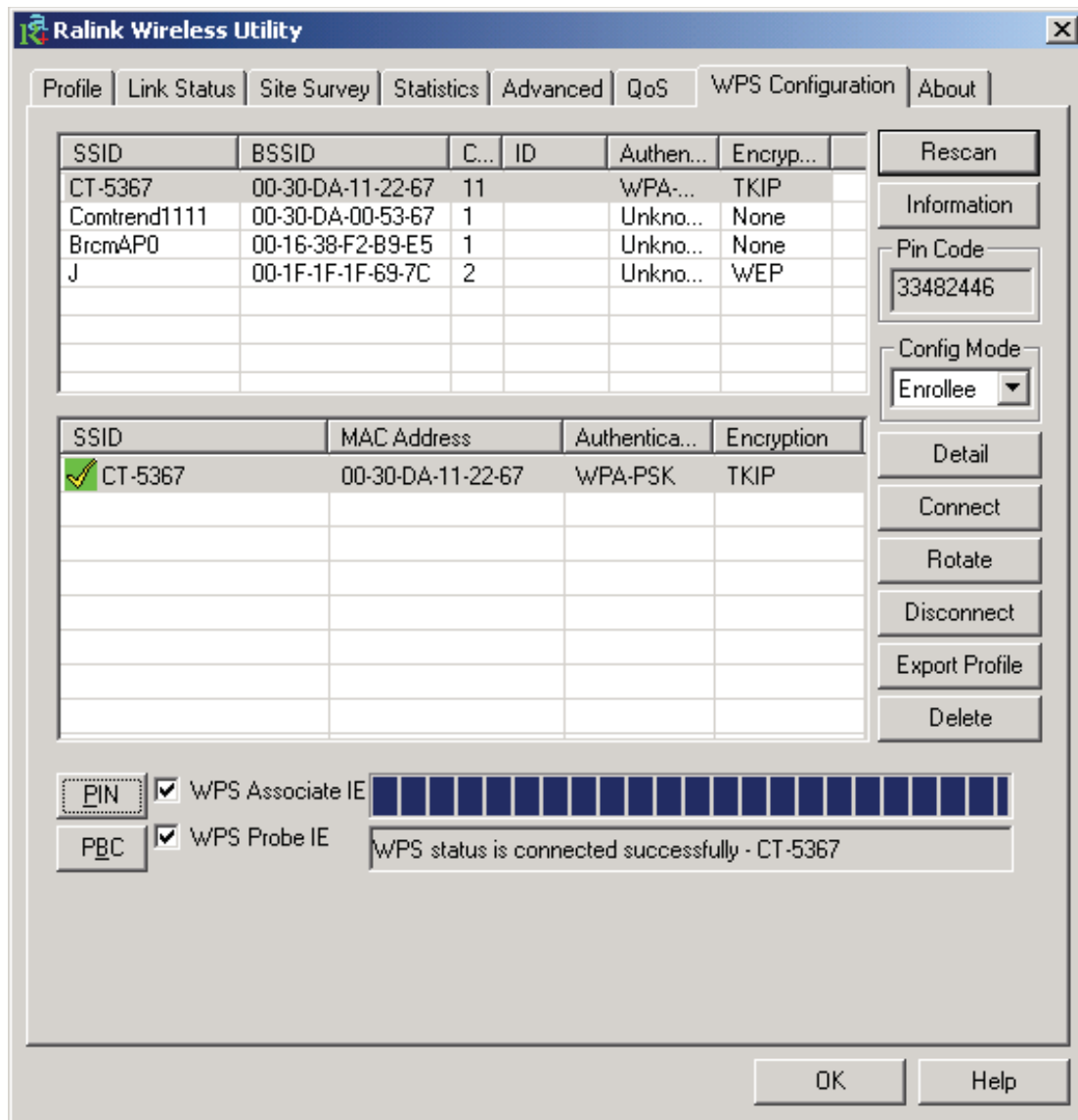
The figure below provides an example of a WPS client PIN function in-progress.



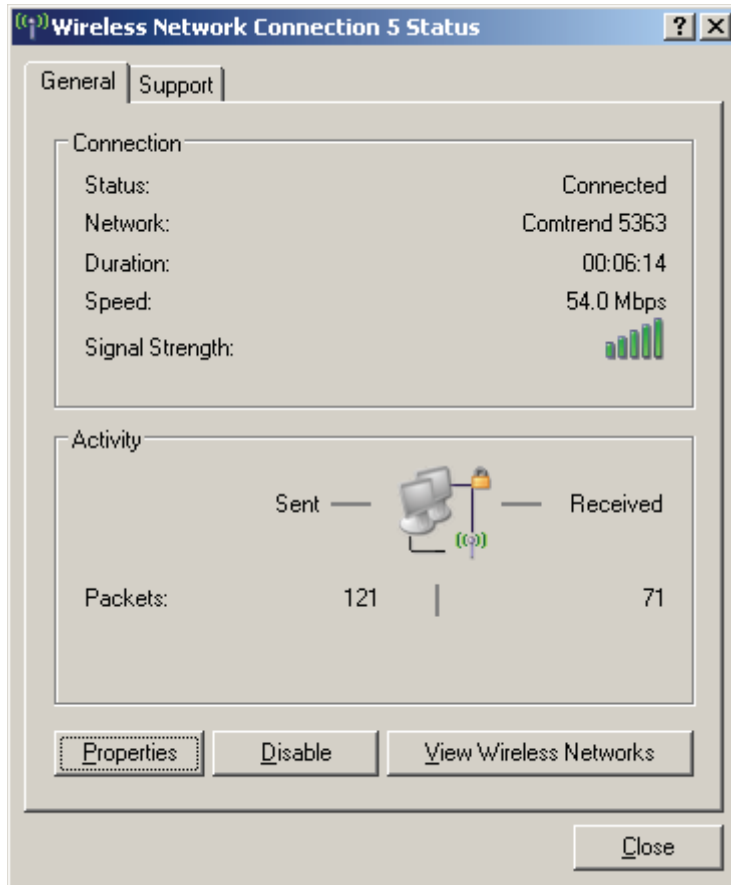
Now go to Step 8 (Part IV. Check Connection) to check the WPS connection.

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.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the new connection. It should look similar to the dialog-box shown below.



7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. 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. When MAC address filtering is enabled, it restricts the devices that can connect to your access point.

To add a MAC Address filter, click the **Add** button shown below.

To delete a filter, select it from the table below and click the **Remove** button.



Option	Description
MAC Restrict Mode	Disabled: MAC filter is disabled. Allow: Permits the listed addresses to connect to the access point (AP). Deny: Prevents the listed addresses from connecting to the AP.
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**.



7.4 Wireless Bridge

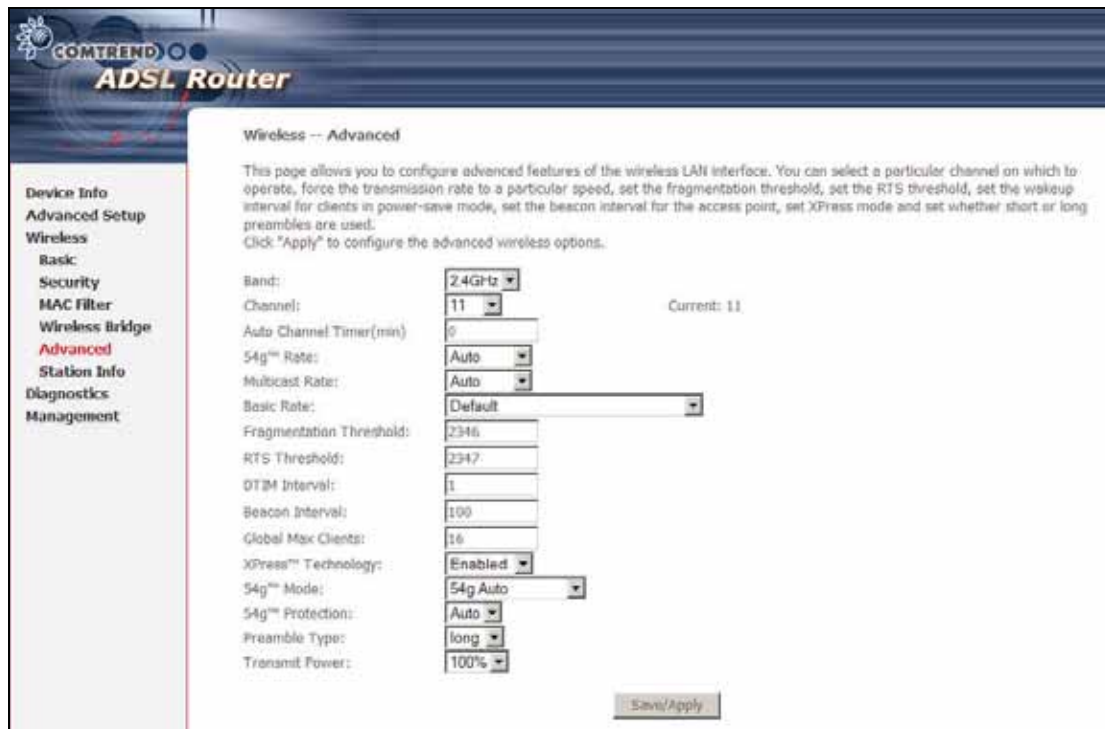
This screen allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will 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.



7.5 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 **Apply** to configure the advanced wireless options.



Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band.
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
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 multicast packet transmit rate.
Basic Rate	Setting basic transmit 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), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. 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). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Global Max Clients	The maximum number of clients allowed.
Xpress™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g™ Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.

7.6 Station Info

This screen shows authenticated wireless stations and their status.

COMTREND
ADSL Router

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

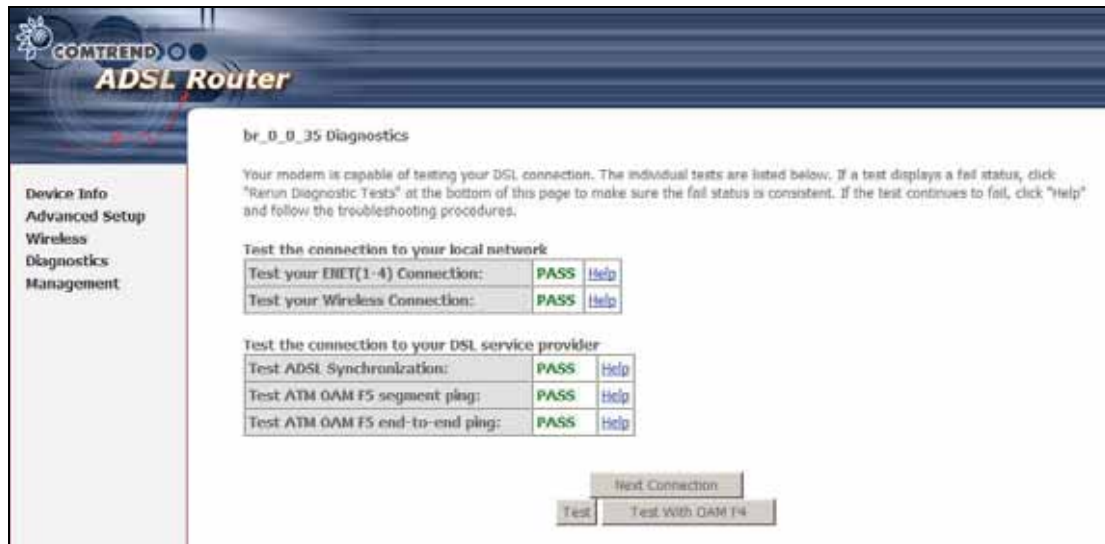
Refresh

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info

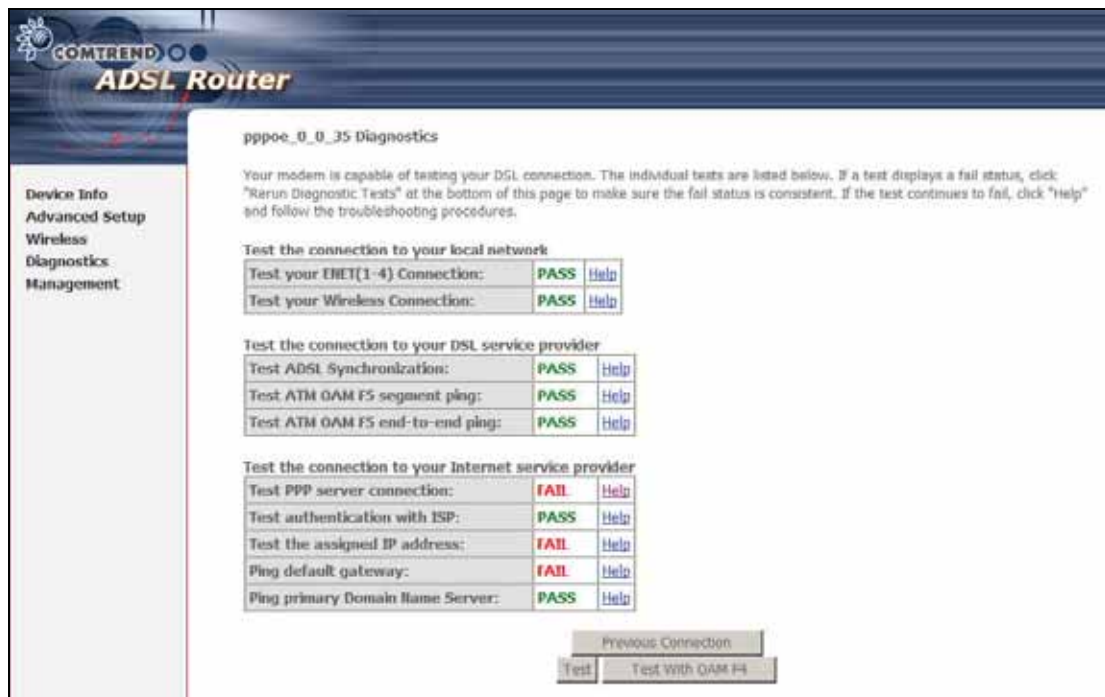
Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	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 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status, click **RERUN DIAGNOSTIC TESTS** at the bottom of the screen to retest and confirm the error. If the test continues to fail, click **HELP** and follow the troubleshooting procedures.



The figure above shows the Diagnostics screen in bridge mode.



The figure above shows the Diagnostics screen in PPPoE mode.

The table on the following page describes some basic diagnostics tests.

Test	Condition
ENET Connection	Pass: Indicates that the Ethernet interface on your computer is connected to the LAN port of this device. Fail: Indicates that the device does not detect the Ethernet interface on your computer.
Wireless connection	Pass: Indicates the wireless card on the device is ON. Down: Indicates that the wireless card is OFF.
ADSL Synchronization	Pass: Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid ADSL LED on the device also indicates the detection of a DSL signal from the telephone company Fail: Indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The ADSL LED will turn off.
Ping Default Gateway	Pass: Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. Fail: Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the device can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

NOTE: This table describes the basic test set (i.e. no PVC configured). For help with other tests click on the [Help](#) link next to each test condition.

Chapter 9 Management

The Management menu has the following maintenance functions and processes:

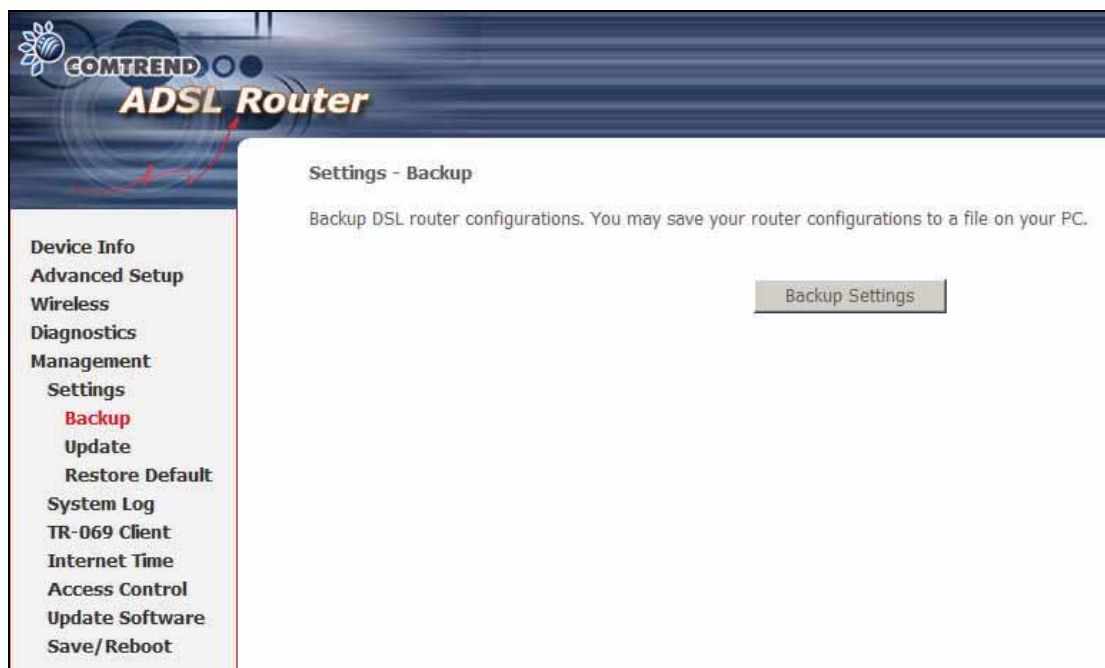
- 9.1 Settings
- 9.2 System Log
- 9.3 TR-069 Client
- 9.4 Internet Time
- 9.5 Access Control
- 9.6 Update Software
- 9.7 Save and Reboot

9.1 Settings

The Settings screen allows for the backup, retrieval, and restoration of settings.

9.1.1 Backup

Select **Backup** from the **Settings** submenu to access the screen shown below. Click the **Backup Settings** button to save the current configuration settings. You will be prompted to define the location of a backup file to save to your PC.



9.1.2 Update Settings

Select **Update** from the **Settings** submenu to access the screen shown below. Enter a previously saved configuration backup file in the **Settings File Name** field and click the **Update Settings** button to load it. If you forget the filename and path, you can search your PC by clicking on the **Browse** button.



The screenshot shows the COMTREND ADSL Router web interface. The header includes the COMTREND logo and 'ADSL Router'. A left sidebar contains a menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings (highlighted), Backup, Update (highlighted in red), Restore Default, System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled 'Tools -- Update Settings' and contains the text: 'Update DSL router settings. You may update your router settings using your saved files.' Below this is a form with 'Settings File Name:' followed by an empty text input field and a 'Browse...' button. A 'Update Settings' button is located to the right of the input field.

9.1.3 Restore Default

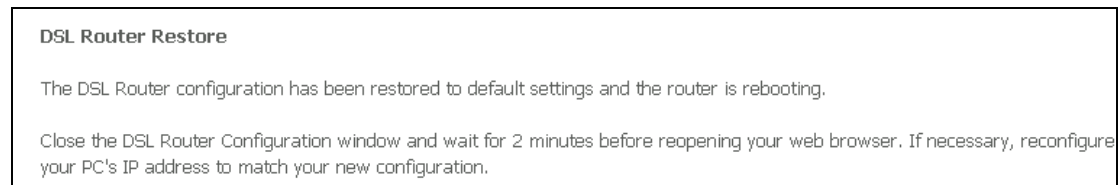
Select **Restore Default** from the **Settings** submenu to access the screen shown below. Click the **Restore Default Settings** button to restore the device to the default firmware settings. Restoring system settings require a device reboot.



The screenshot shows the COMTREND ADSL Router web interface. The header includes the COMTREND logo and 'ADSL Router'. A left sidebar contains a menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, Backup, Update, Restore Default (highlighted in red), System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled 'Tools -- Restore Default Settings' and contains the text: 'Restore DSL router settings to the factory defaults.' A 'Restore Default Settings' button is located on the right side of the main content area.

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

After the Restore Default Configuration button is selected, the following screen appears. Close the device Configuration window and wait for 2 minutes before reopening the browser. If necessary, reconfigure your PC IP address to match your new configuration (see section 3.2 IP Configuration for details).



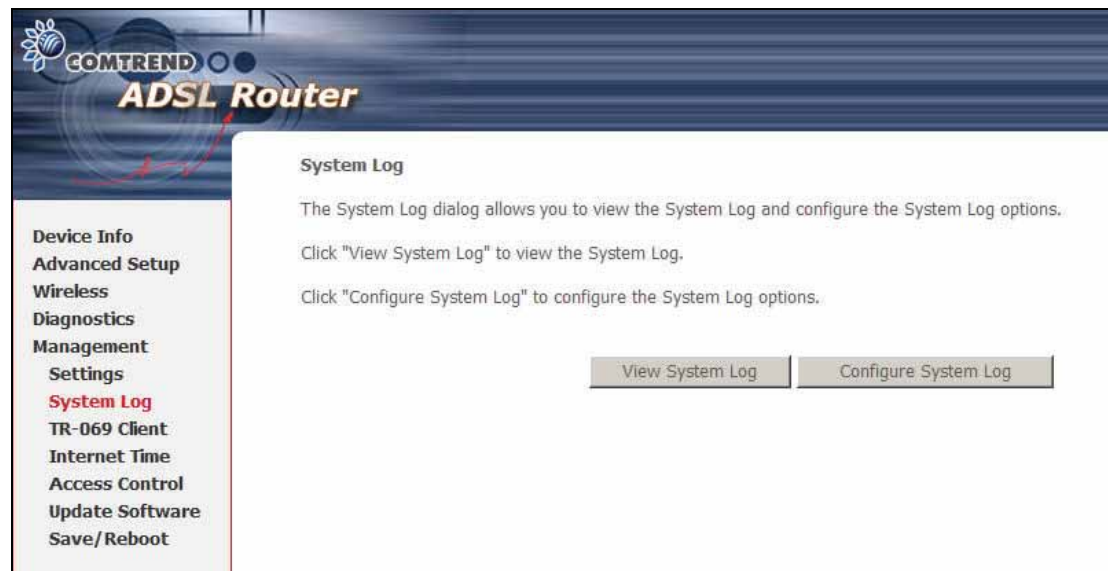
After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

NOTE: The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

9.2 System Log

The **System Log** option under **Management** allows for the viewing of system events and configuration of related options. The default setting for the System Log is enabled. Follow the steps below to enable and view the System Log.

STEP 1: Click Configure System Log to begin.



Step 2: Select the system log options (see table below) and click **Save/Apply**.



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

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.

9.3 TR-069 Client

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

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" to configure the TR-069 client options.

Inform: Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Display SOAP messages on serial console: Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
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.

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	
Authentication	Enable/Disable using the checkbox.
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.
Get RPC Methods	Click this button to force 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.

9.4 Internet Time

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet timeservers, tick the corresponding box displayed on this screen shown below.

FIRST NTP TIMESERVER: Select the required server.

SECOND NTP TIMESERVER: Select second timeserver, if required.

TIME ZONE OFFSET: Select the local time zone.

Configure these options and then click **Save/Apply** to activate.

NOTE: Internet Time must be activated to use [Parental Control](#) (page 55). 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.

9.5 Access Control

The Access Control option under the Management menu bar configures access related parameters in three areas: Services, IP Addresses, and Passwords. Use Access Control to control local and remote management settings for the device.

9.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These access services are available: FTP, HTTP, ICMP, SSH, TELNET and TFTP. Enable a service by ticking its checkbox. Click **Save/Apply** to activate.

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Save/Apply

NOTES: The WAN column is present if the WAN interface is active. Only the LAN side will be displayed if the WAN interface is not configured.

[Appendix D: SSH Client](#) contains a quick introduction to SSH clients.

9.5.2 IP Addresses

The IP Addresses option limits local access by IP address. When the **Access Control Mode** is enabled, only the IP addresses listed here can access the device. Before enabling **Access Control Mode**, add IP addresses with the **ADD** button.



On this screen, enter the IP address to which you wish to give access privileges.

Click **Save/Apply** to continue.



9.5.3 Passwords

The Passwords option configures the user account access passwords for the device. Access to the device is limited to the following three user accounts:

- **root** is to be used for local (LAN) management.
- **support** is to be used for remote (WAN) management.
- **user** is to be used to view information and update device firmware.

NOTE: Default passwords for these three user accounts can be found in section [3.1 Default Settings](#)

Use the fields in the screen below to select a username and change its password. Passwords must be 16 characters or less. Click **Save/Apply** to continue.

The screenshot shows the 'Access Control -- Passwords' page in the COMTREND ADSL Router web interface. The left sidebar contains a navigation menu with items like 'Device Info', 'Advanced Setup', 'Wireless', 'Diagnostics', 'Management', 'Settings', 'System Log', 'TR-069 Client', 'Internet Time', 'Access Control', 'Services', 'IP Addresses', 'Passwords', 'Update Software', and 'Save/Reboot'. The main content area is titled 'Access Control -- Passwords' and contains the following text: 'Access to your DSL router is controlled through three user accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of your DSL Router. The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software. Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.' Below this text are four input fields: 'Username:' (a dropdown menu), 'Old Password:', 'New Password:', and 'Confirm Password:'. A 'Save/Apply' button is located at the bottom right of the form area.

9.6 Update Software

The **Update Software** screen allows for firmware updates. Manual device upgrades from a locally stored file can be performed using the following screen.

The screenshot shows the 'Tools -- Update Software' page in the COMTREND ADSL Router web interface. The left sidebar is the same as in the previous screenshot, but 'Update Software' is highlighted in red. The main content area is titled 'Tools -- Update Software' and contains the following text: '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 DSL Router will reboot.' Below this text is a 'Software File Name:' label followed by an input field and a 'Browse...' button. An 'Update Software' button is located at the bottom right of the form area.

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 1: 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** at the top of the **Device Info** Summary screen (see graphic below) with the firmware version installed, to confirm the installation was successful.

Device Info	
Board ID:	96338A-122
Software Version:	A111-312CTL-C01_R02
Bootloader (CFE) Version:	1.0.37-12.1-1
Wireless Driver Version:	4.170.16.0.cpe2.1sd
ADSL Version:	A2pB023k.d20k_rc2

9.7 Save and Reboot

This function saves the current configuration settings and reboots the device.



NOTE: You may need to reconfigure the TCP/IP settings after rebooting. For example, if the DHCP server is disabled Static IP settings must be configured. See section [3.2 IP Configuration](#) for detailed instructions.

NOTE: If you lose all access to the web user interface (WUI), you may need to close the browser, wait for two minutes, and then restart the WUI. If this does not work, then press the reset button on the rear panel of the device for 5-7 seconds to restore to default settings.

Appendix A: Security

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 Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

FILTER NAME: User defined Filter Name.

PROTOCOL: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

SOURCE IP ADDRESS/SOURCE SUBNET MASK: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

SOURCE PORT: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

DESTINATION IP ADDRESS/DESTINATION SUBNET MASK: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

DESTINATION PORT: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be dropped.

EXAMPLE 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Destination Address	: NA
Destination Subnet Mask	: NA
Destination Port	: NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 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 Address : 192.168.1.45
Source Subnet Mask : 255.255.255.0
Source Port : 5060:6060
Destination Address : 172.16.13.4
Destination Subnet Mask : 255.255.255.0
Destination Port : 6060:7070

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

INCOMING IP FILTERING:

Helps in setting rules to ACCEPT 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, particular packet types coming from the WAN can be Accepted.

FILTER NAME: User defined Filter Name.

PROTOCOL: Can take on any values from TCP/UDP, TCP, UDP or ICMP

SOURCE IP ADDRESS/SOURCE SUBNET MASK: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

SOURCE PORT: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

DESTINATION IP ADDRESS/DESTINATION SUBNET MASK: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

DESTINATION PORT: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers (portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by user.

EXAMPLE 1:

Filter Name : In_Filter1
Protocol : TCP
Source Address : 210.168.219.45
Source Subnet Mask : 255.255.0.0
Source Port : 80
Destination Address : NA
Destination Submask : NA
Destination Port : NA
Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having 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
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Destination Address	: 192.168.1.45
Destination Subnet Mask	: 255.255.255.0
Destination Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 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 FILTERING: These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup - Security - MAC Filtering.

GLOBAL POLICY: When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

PROTOCOL TYPE: Either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

DESTINATION MAC ADDRESS: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

SOURCE MAC ADDRESS: Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

FRAME DIRECTION: (User must select interface on which this rule is applied)

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

EXAMPLE 1:

Global Policy: Forwarded
Protocol Type: PPPoE
Destination MAC Address: 00:12:34:56:78:90
Source MAC Address: NA
Frame Direction: LAN => WAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address on the br_0_34 WAN interface. All other frames on this interface are forwarded.

EXAMPLE 2:

Global Policy: Blocked
Protocol Type: PPPoE
Destination MAC Addr: 00:12:34:56:78:90
Source MAC Addr: 00:34:12:78:90:56
Frame Direction: WAN => LAN
WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56 on the br_0_34 WAN interface. 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 device, as per chosen days of the week and the chosen times.

USER NAME: Name of the Filter.

BROWSER MAC ADDRESS: Displays MAC address of the LAN device on which the browser is running.

OTHER MAC ADDRESS: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

DAYS OF THE WEEK: Days of the week, when the restrictions are applied.

START BLOCKING TIME: The time when restrictions on the LAN device begin.

END BLOCKING TIME: The time when LAN device restrictions are lifted.

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

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and time, this device will have access to the outside Network.

Appendix B: Pin Assignments

Line Port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

LAN Port (RJ45)

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

Appendix C: Specifications

REAR PANEL

RJ-11 X1 for ADSL2+, RJ-45 X 4 for LAN, WPS Button X 1, Wi-Fi Button X 1
Reset Button X 1, Power Jack X 1, Power button X 1, Wi-Fi Antenna x 1

WAN

Standard ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2
G.992.5 (ADSL2+) Downstream: 24 Mbps Upstream: 1.3 Mbps
G.992.3 (ADSL2) Downstream: 12 Mbps Upstream: 1.3 Mbps
G.DMT Downstream: 8 Mbps Upstream: 0.8 Mbps
AnnexM

LAN

StandardIEEE 802.3, IEEE 802.3u
10/100 BaseTAuto-sense
MDI/MDX support.....Yes

WIRELESS

StandardIEEE 802.11g – backward compatible with 802.11b
Encryption.....64/128-bit WEP
Channels.....11 (US, Canada), 13 (Europe), 14 (Japan)
Data Rate.....Up to 54Mbps
WPA/WPA2Yes
IEEE 802.1xYes
WPSYes
MAC FilteringYes
Afterburner mode/Turbo mode Optional

ATM ATTRIBUTES

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC
1577 (IPoA), Annex M
Support PVCs16
AAL typeAAL5
ATM service classUBR/CBR/VBR
ATM UNI supportUNI3.1/4.0
OAM F4/F5Yes

MANAGEMENT

Telnet, Web-based management, Configuration backup and restoration, Software
upgrade via HTTP, TFTP, or FTP server, Supports TR-069/TR-098/TR-111 for
Remote Management

SECURITY FUNCTIONS

PAP, CHAP,
Packet and MAC address filtering,
Access control and SSH
Four level login including local admin, local user and remote technical support
access and user for WiFi access

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,
DHCP Server/Client/Relay,
DNS Relay, Dynamic DNS,
ARP, RARP, SNTP

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
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

SIP, H.323, YAHOO MESSENGER, ICQ, REALPLAYER, NET2PHONE, NETMEETING,
MSN, X-BOX, MICROSOFT DIRECTX GAMES AND ETC POWER SUPPLY

External power adapter.....110 - 240 Vac Output:18V/0.5A

ENVIRONMENT CONDITION

Operating temperature0 ~ 50 degrees Celsius
Relative humidity5 ~ 95% (non-condensing)

KIT WEIGHT

1 X (CT-5367, RJ11 and RJ45 cables, power adapter, CD-ROM) = 1.0 kg

DIMENSIONS 158 MM (W) X 40 MM (H) X 136 MM (D)

CERTIFICATIONS CE, FCC PART 15, FCC PART 68

NOTE: Specifications are subject to change without notice.

Appendix D: SSH Client

Linux OS comes with a ssh client. Microsoft Windows does not have ssh client but there is a public domain one called "putty" that you can download here:

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

To access the router using Linux ssh client:

From LAN: Use the router WEB UI to enable SSH access from LAN.

(default is enabled)

type: `ssh -l root 192.168.1.1`

From WAN: Use WEB UI to enable SSH access from WAN.

type: `ssh -l support router-WAN-ip-address`

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

From LAN: Use the router WEB UI to enable SSH access from LAN

(default is enabled)

type: `putty -ssh -l admin 192.168.1.1`

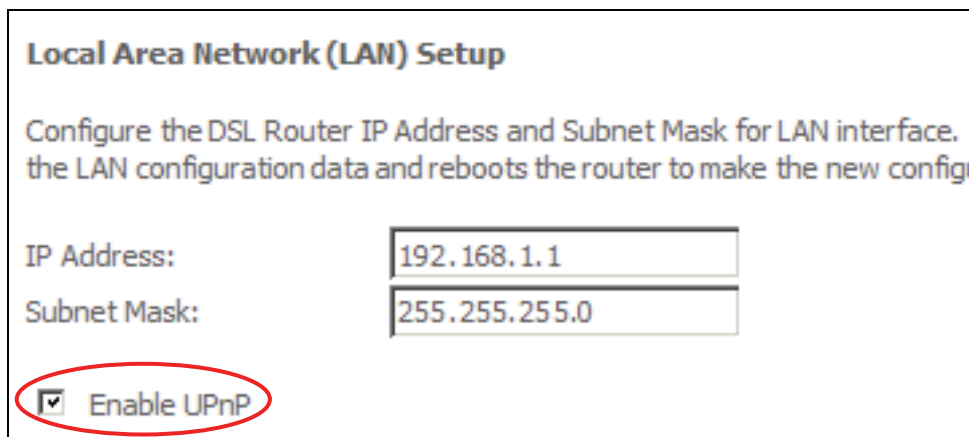
From WAN: In the router, use WEB UI to enable SSH access from WAN.

type: `putty -ssh -l support router-WAN-ip-address`

Appendix E: WSC External Registrar

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

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



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save the LAN configuration data and reboots the router to make the new configuration.

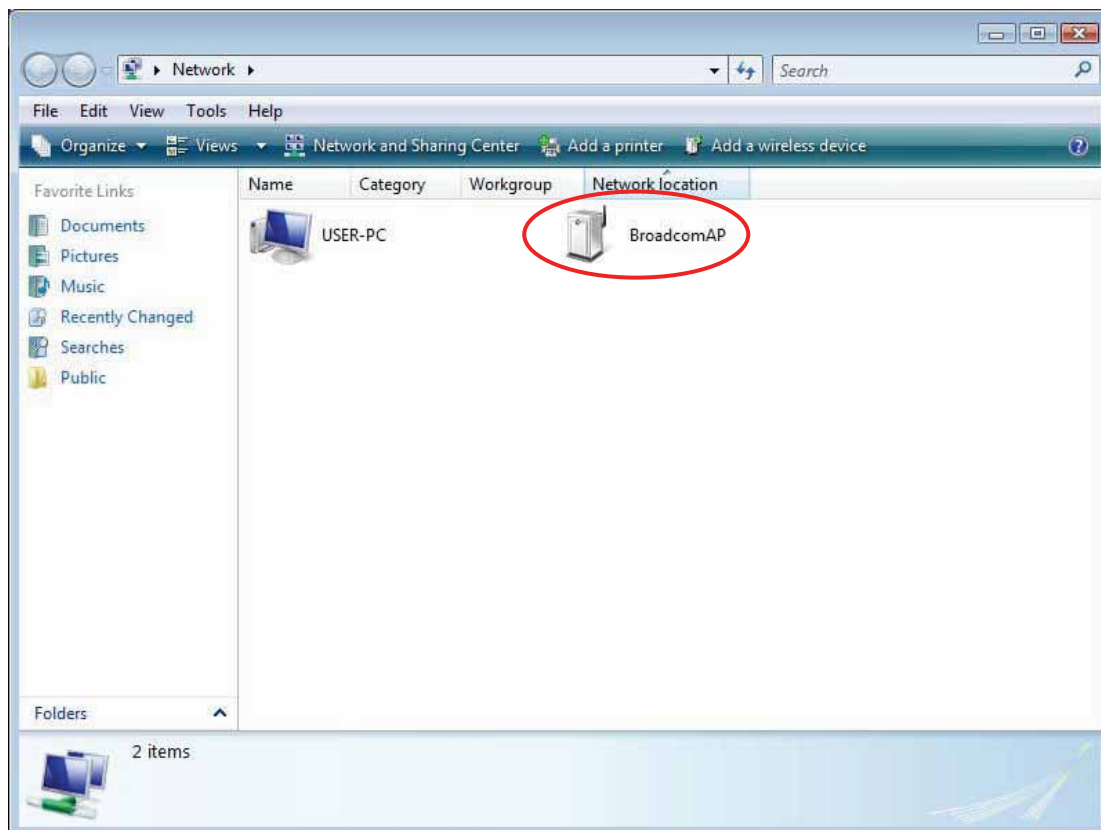
IP Address:

Subnet Mask:

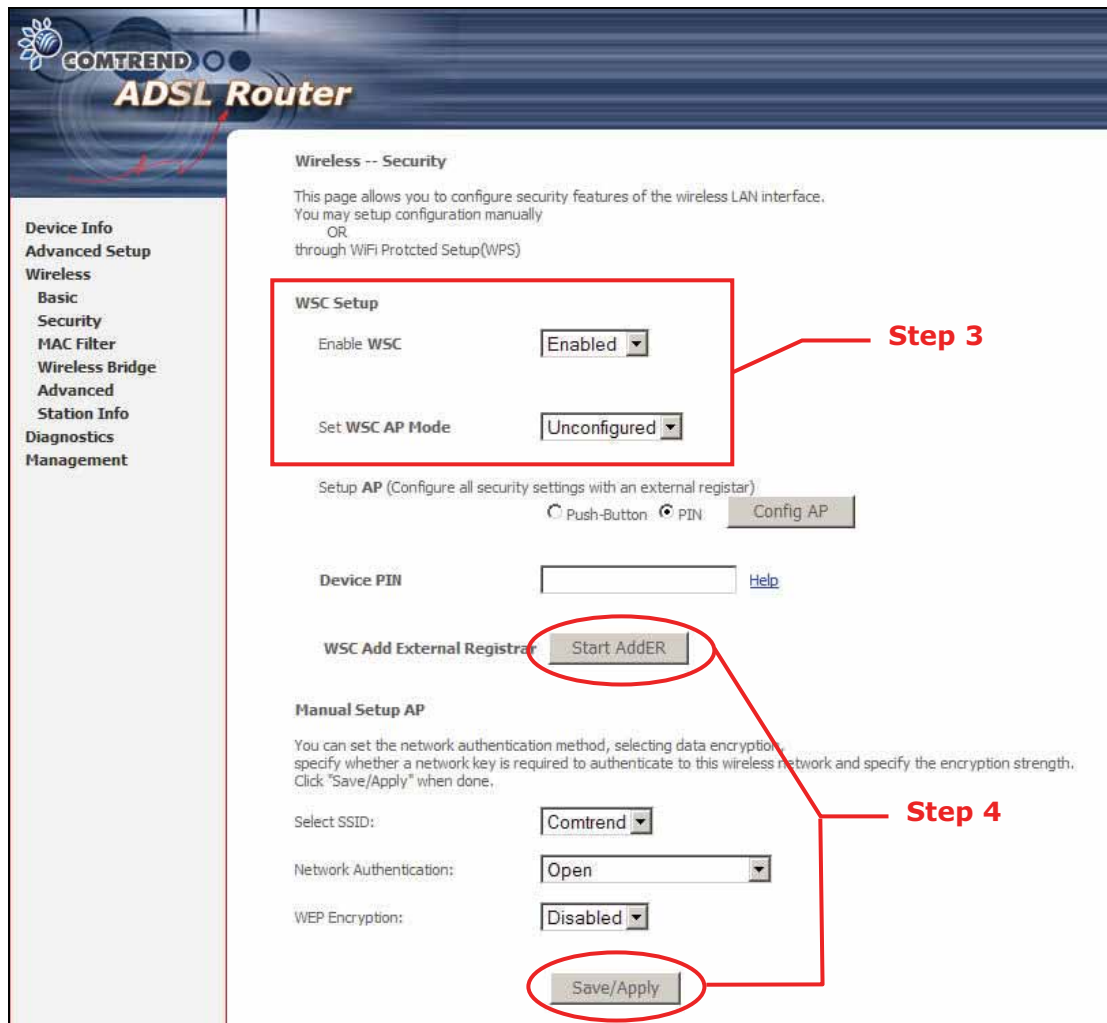
Enable UPnP

NOTE: A PVC must exist to see this option.

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

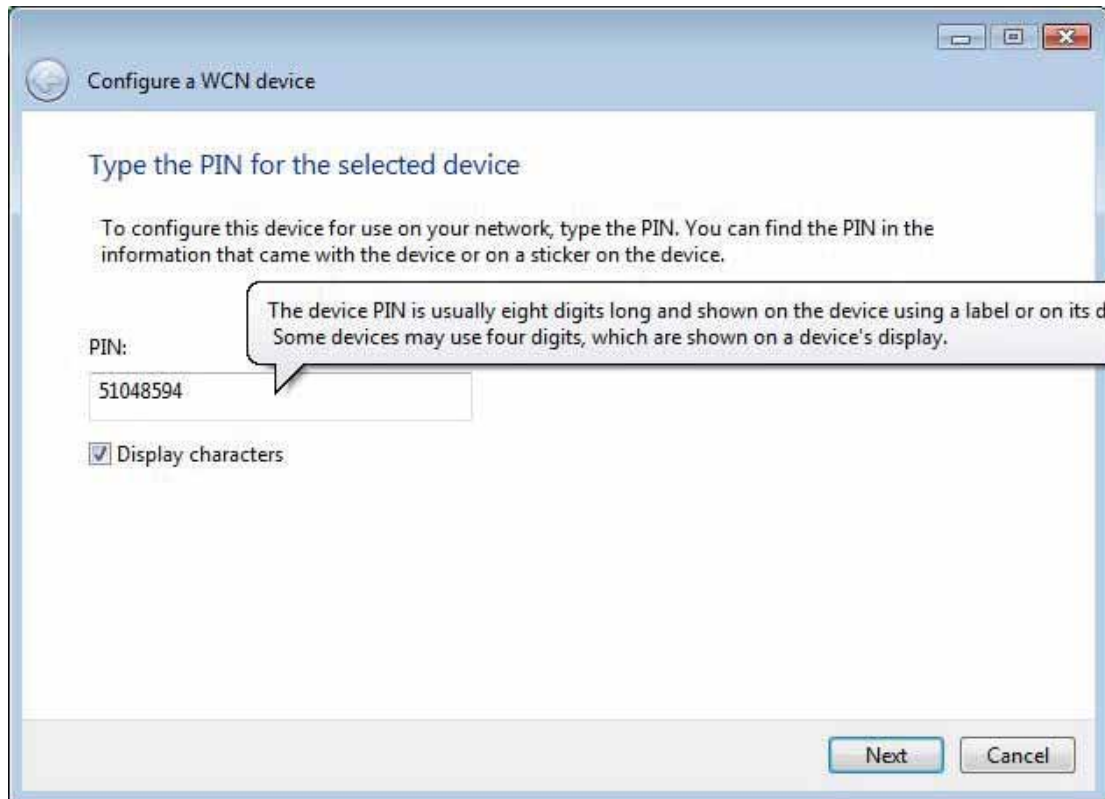


Step 3: On the Wireless → Security screen, enable WSC by selecting **Enabled** from the drop down list box and set the WSC AP Mode to Unconfigured.

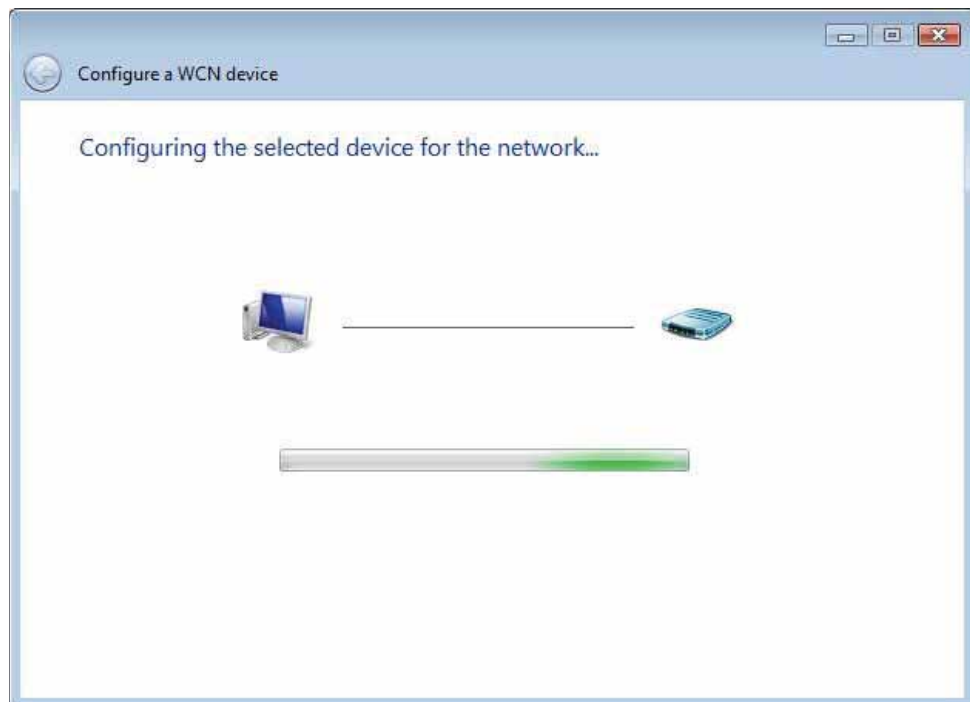


Step 4: Click the **Save/Apply** button at the bottom of the screen. The screen will go blank while the router applies the new Wireless settings. When the screen returns, press the **Start AddER** button, as shown above.

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**.



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



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