COMTREND CORPORATION

CT-5364A

802.11n ADSL2+ Router

User Manual

Version A2.0, May 17, 2010

261091-007

Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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

WARNING

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

FCC Compliance

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:
The equipment has been tested and found to comply with the limits for a Class 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.

The user should not modify or change this equipment without written approval form Comtrend Corporation .Modification could void authority to use this equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. No change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

Copyright

NOTE: This document is subject to change without notice.

Protect Our Environment

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

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

Table of Contents

Chapter 1 Introduction

The CT-5364A 802.11n ADSL2+ Router provides wired and wireless access for high-bandwidth applications in the home or office. It includes one ADSL port and five 10/100 ase-T Fast Ethernet ports, with one Ethernet port assigned to the Ethernet WAN and the other four supporting LAN traffic. An added US host port supports printers. The front and back panels are TR-068 compliant, with colored panels and LED indicators that make for easy setup and use.

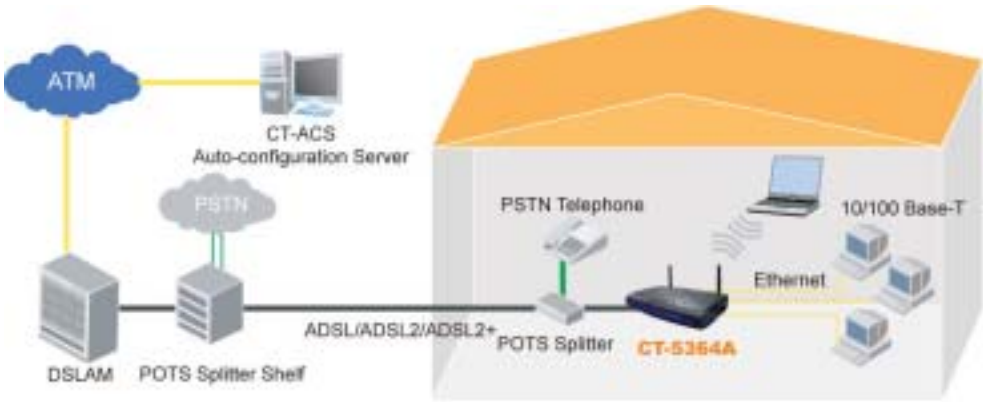
An integrated 802.11n (2x2 MIMO) WLAN Access Point supports faster connections (up to 270Mbps) and increased range compared with 802.11b or 802.11g protocols, without sacrificing compatibility with these older standards. A WPS (Wi-Fi Protected Setup) button is included for easy and secure wireless network setup. Security features include 64/128 bit WEP and WPA/WPA2 encryption, firewall and VPN.

1.1 Features

- Printer Server through US host
- Ethernet WAN or ADSL access
- Auto PVC configuration, up to 16 VCs
- DHCP Client/Server/Relay
- Dynamic IP assignment
- Static and RIP v1/v2 routing
- DNS Proxy/Relay
- Per-VC packet level QoS
- IP/TCP/UDP QoS
- NAT/PAT
- IP/MAC address filtering
- Parental Control
- UPnP
- IGMP Proxy
- WMM
- Integrated 802.11n AP
- 2x2 MIMO wireless antennas
- 802.11b/g backward-compatible
- Wireless Distribution System (WDS)
- Wi-Fi Protected Setup (WPS)
- Strong wireless security encryption
- WPA/WPA2 and 802.1x
- Supports remote administration
- TR-069/TR-098/TR-111 protocols
- Configuration backup and restoration
- Automatic firmware upgrade
- FTP/TFTP server
- RADIUS client
- Web-based management
- Embedded SNMP agent
- TR-068 compliant color connectors

1.2 Application

The following diagram depicts the application of the CT-5364A.



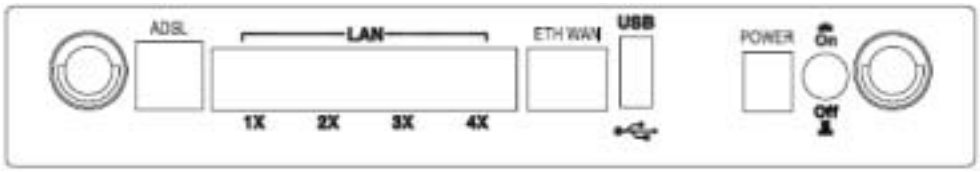
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



ADSL PORT
Connect the ADSL line to the ADSL port with a RJ-11 (telephone) cable.

LAN PORTS
Use RJ-45 cable to connect up to four network devices. These ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

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

USB HOST PORT
The high-speed US 2.0 host connection connects compatible US devices. This firmware release supports most printers.

- Consult Appendix E for generic printer setup.

POWER ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected (see section 2.2 LED Indicators) then the CT-5364A is ready for use.

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.
Caution 2:	efore servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

SIDE PANEL

The figure below shows the right-side panel of the device.

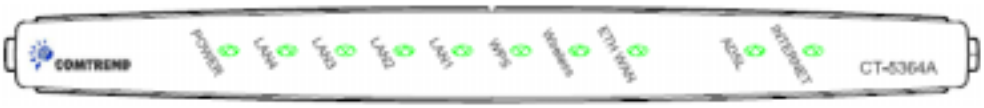
WPS BUTTON
Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode. When WPS is available the WPS LED will be ON.

Reset Button
Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 LED Indicators for details).

NOTE:	If pressed down for more than 20 seconds, the CT-5364A will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

2.2 LED Indicators

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



LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
LAN 4X-1X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		link	Data transmitting or receiving over LAN.
WPS	Green	On	WPS enabled.
		Off	WPS disenabled.
		link	The router is searching for WPS clients.
Wireless	Green	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		link	Data transmitting or receiving over WLAN.
ETH WAN	Green	On	An Ethernet WAN Link is established.
		Off	An Ethernet WAN Link is not established.
		link	Data transmitting or receiving over Ethernet WAN.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		link	The ADSL link is training.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
		Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		link	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

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

- Remote WAN access: **enabled**
- Remote (WAN) access (username: **support**, password: **support**)

- WLAN access: **enabled**
- Service Set Identifier (SSID): Comtrend_xxxx,
  where xxxx are the last-four digits of the MAC address of the wireless interface.

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the CT-5364A powers up, the onboard DHCP server will switch on.
The DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

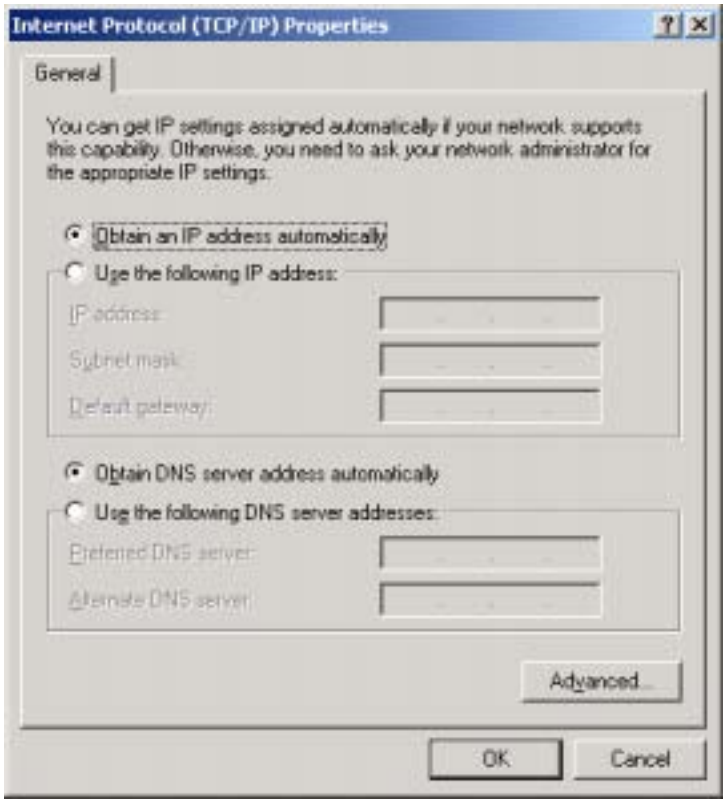
To obtain an IP address from the DCHP server, follow the steps provided below.

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

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

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

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



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

If you experience difficulty with DHCP mode, you can try static IP mode instead, as described on the next page.

STATIC IP MODE

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

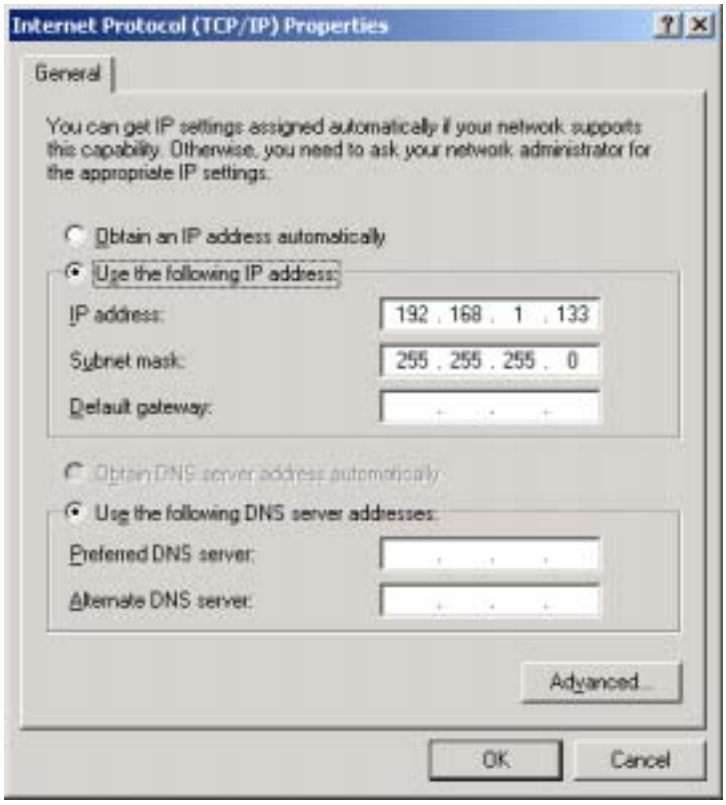
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



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

3.3 Login Procedure

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

NOTE:	The default settings can be found in section 3.1.

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 Quick Setup

After login, the **Quick Setup** screen will appear as shown.

NOTE:	The selections available on the main menu are based upon the configured connection type and user account privileges.

The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.

NOTE:	Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

3.4 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

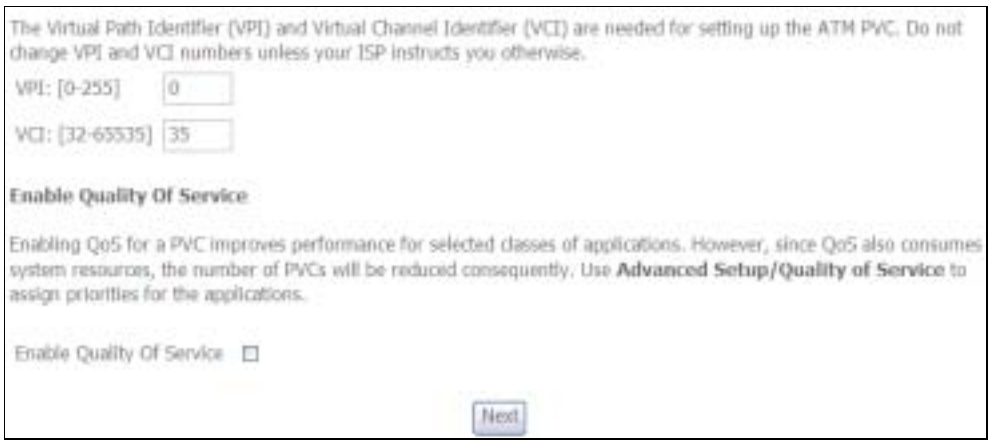
STEP 1: Select **Quick Setup** to display this screen.

STEP 2: Click **Next** to start the setup process. Follow the online instructions to complete the settings. This procedure will skip some processes such as the PVC index and encapsulation mode selection.

STEP 3: After the settings are complete, you can use the ADSL service.

3.5 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.

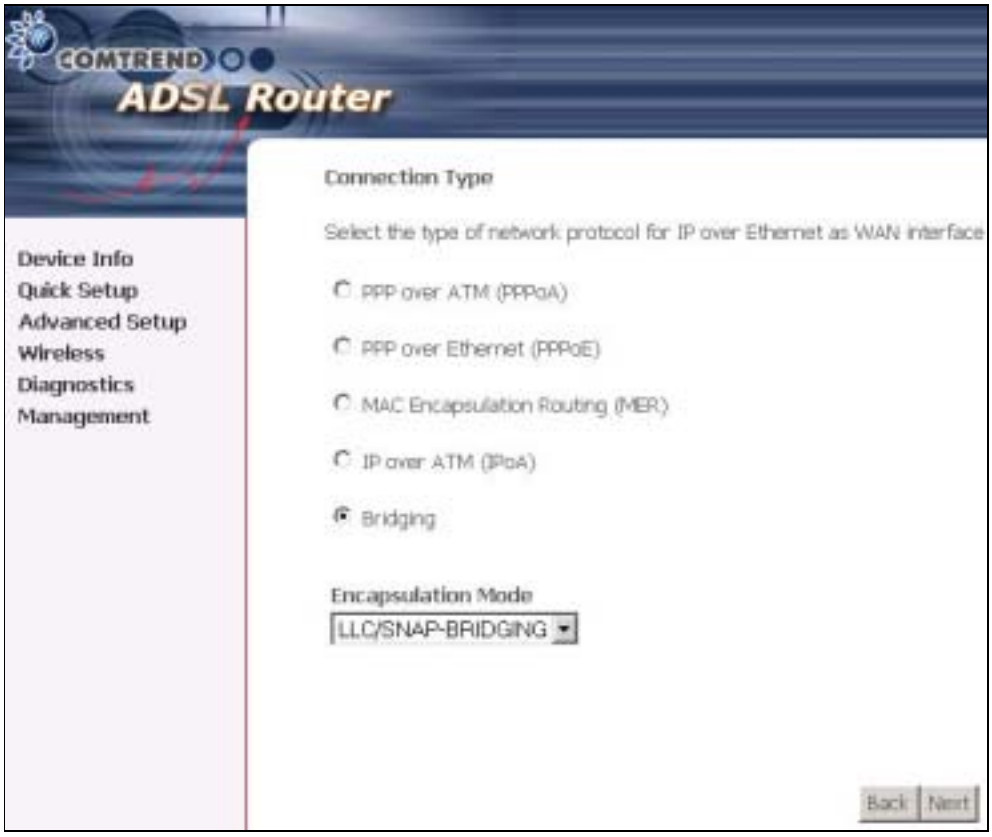


STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click **Next**.

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

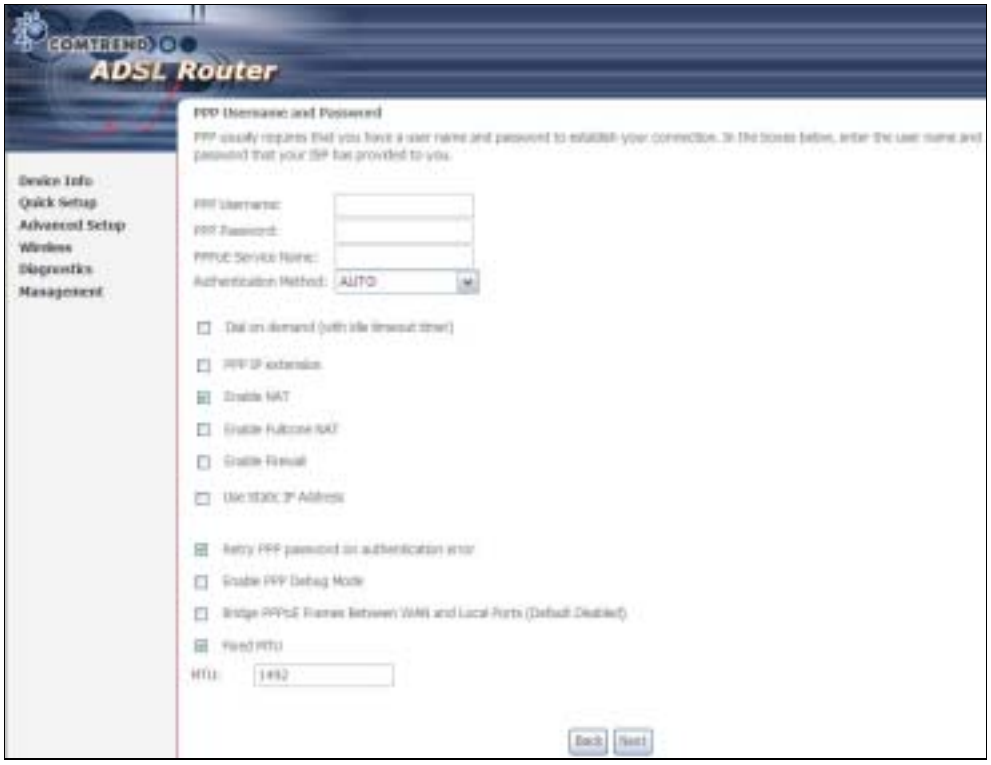
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP RIDGING, VC/MUX
- MER- LLC/SNAP- RIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX



NOTE:	Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

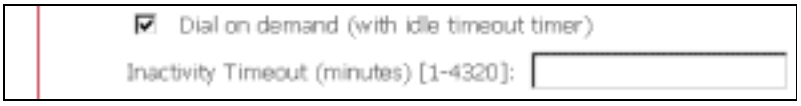


PPP Username/PPP Password: The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, 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.
- 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 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: 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.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address.

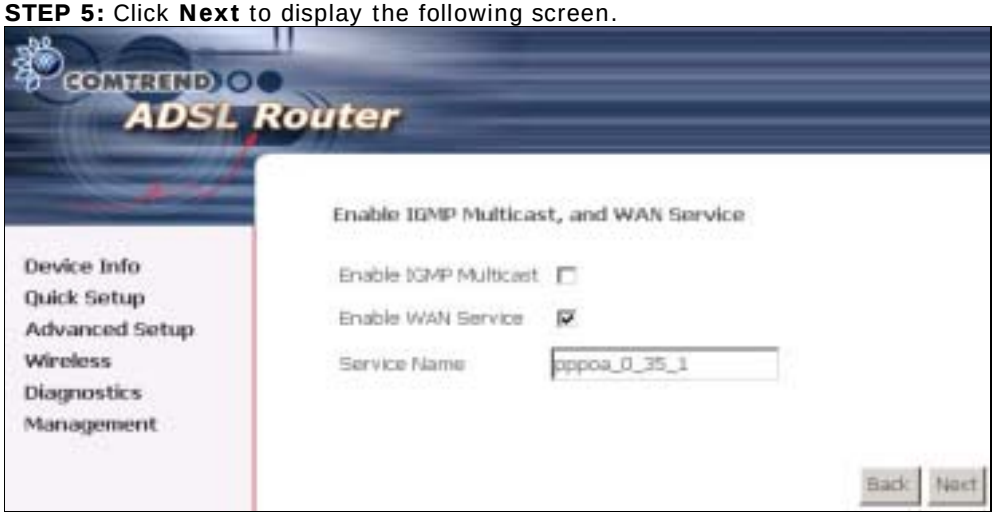
Retry PPP password on authentication error
Tick the box to select.

Enable PPP Debug Mode
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports
If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU
Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click **Next** to display the following screen.



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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

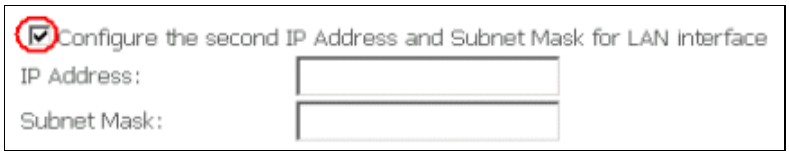
STEP 6: After entering your settings, select **Next**. The following screen appears.

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 and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

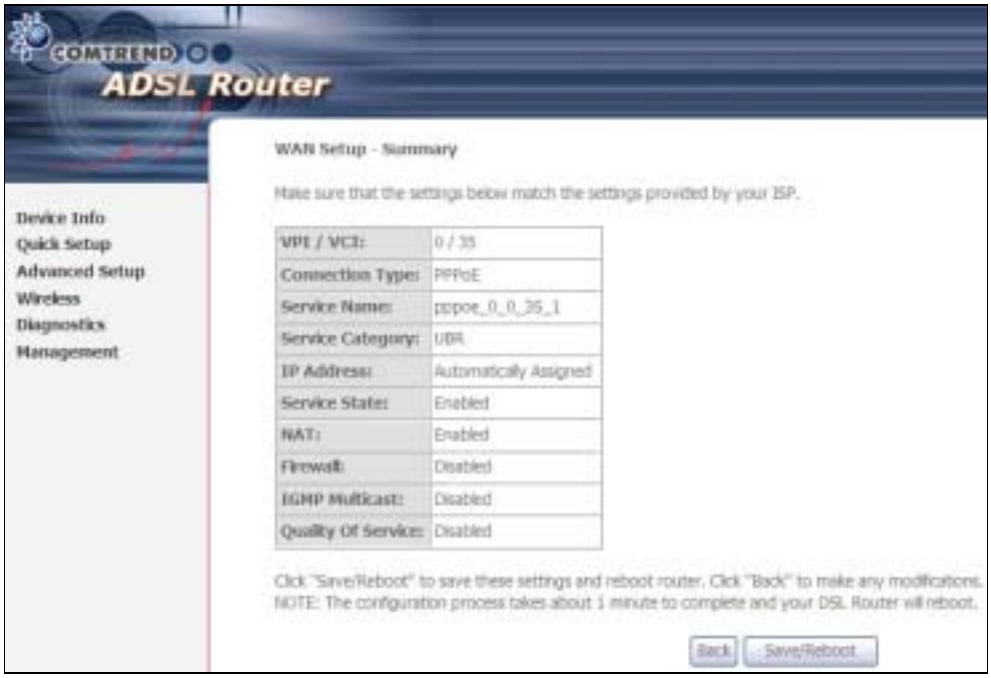
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

3.5.2 MAC Encapsulation Routing (MER)

Step 4: Select the MAC Encapsulation Routing (MER) radio button and click **Next**.

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

NOTE:	DHCP can be enabled for PVC in MER mode 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. Your ISP should provide the values to be entered in these fields.

Step 5: Click **Next** to display the following screen.

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.

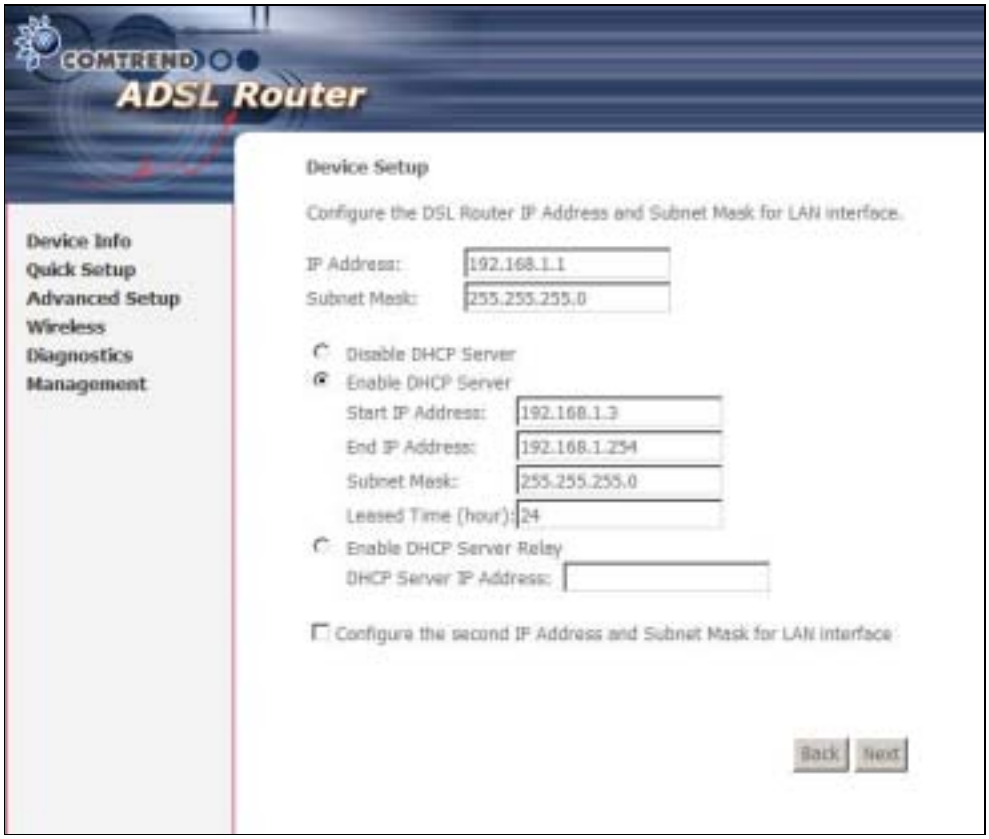
Enable Firewall
If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

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

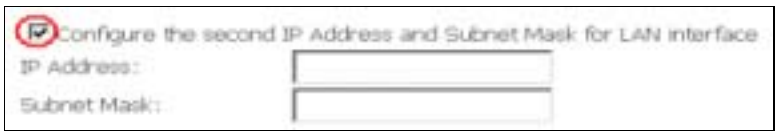


The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

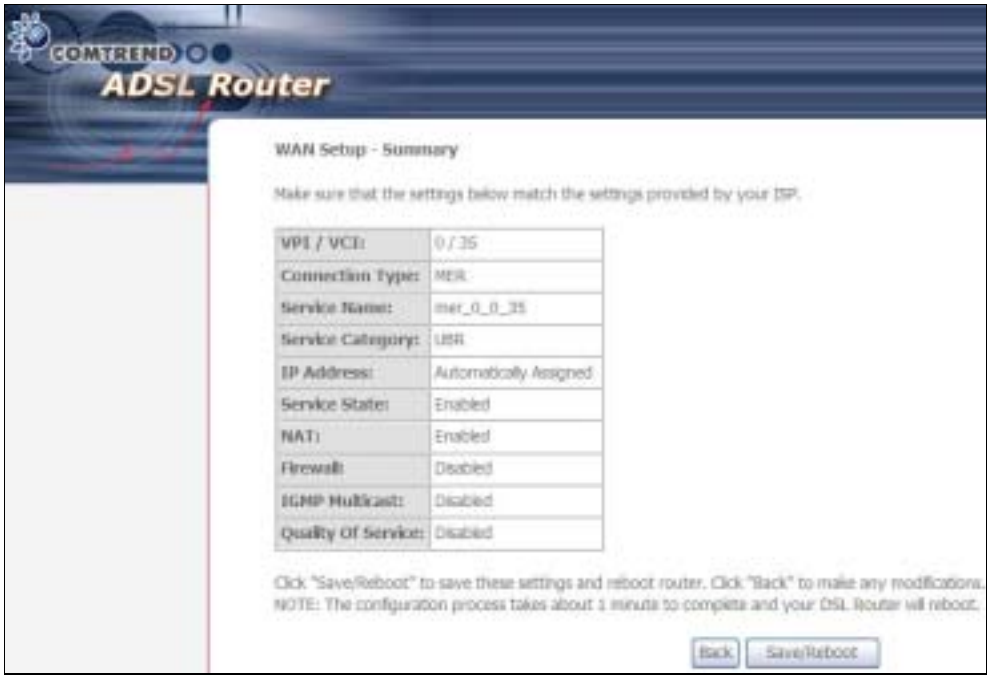
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

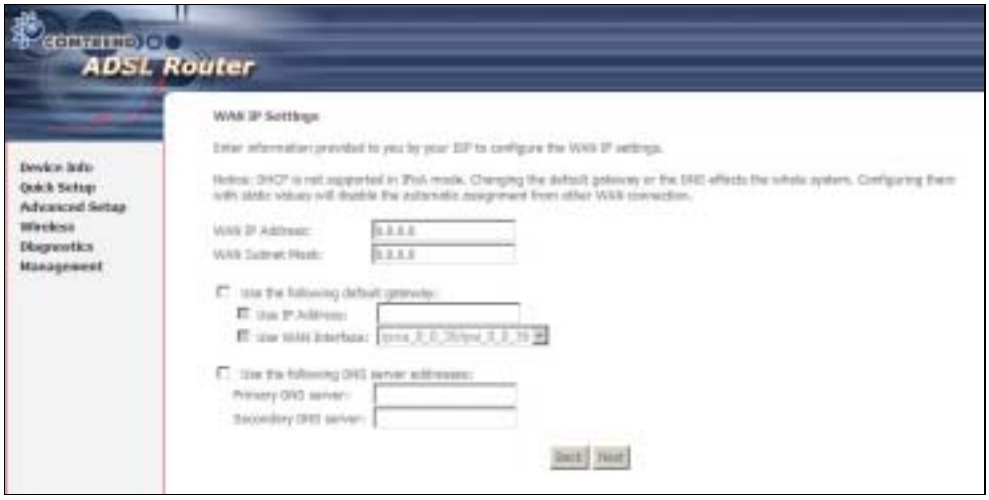
Click **Next** to display the final setup screen.



Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

3.5.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.



NOTE:	DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by their ISP.

Step 5: Click **Next** to display the following screen.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

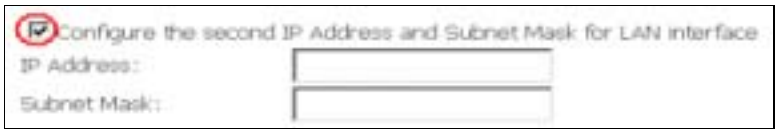
Step 6: Click **Next** to display the following screen.

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 and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.

Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

3.5.4 Bridging

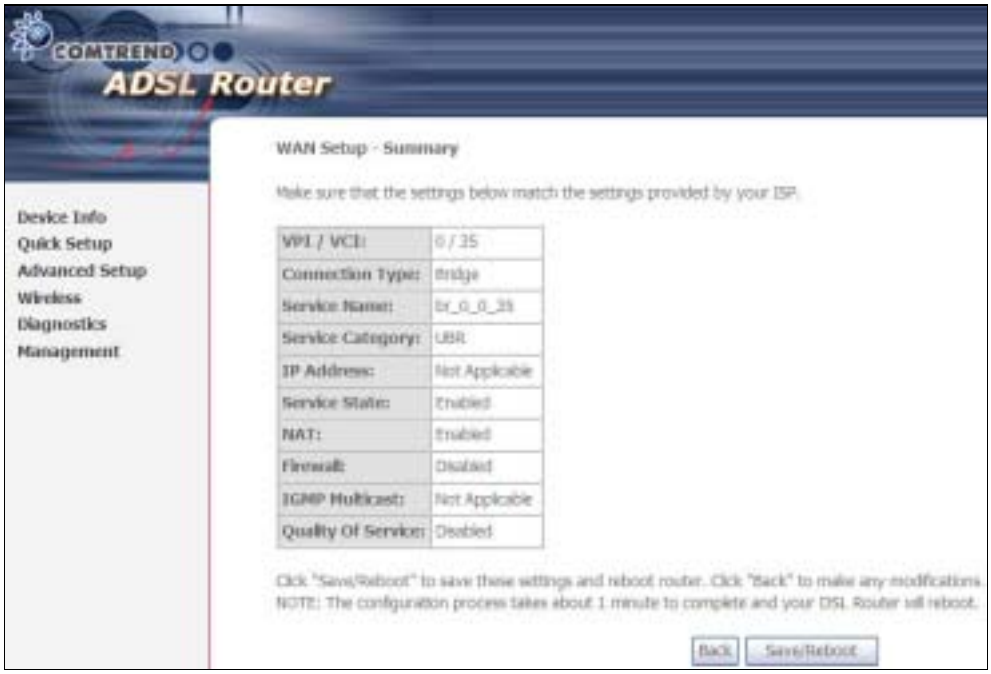
Step 4: Select the ridging radio button and click **Next**. The following screen appears. Select **Enable Bridge Service** and click **Next**.

Step 5: On this screen, you can change the LAN IP address of the router.

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

Device Information screen and login with remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter the default

username and password, as defined in section 3.1 Default Settings.

Click **OK** to continue.

NOTE:	The login password can be changed later (see section 0).

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

Chapter 4 Quick Setup

After login, the **Quick Setup** screen will appear as shown.

NOTE:	The selections available on the main menu are based upon the configured connection type and user account privileges.

The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.

NOTE:	Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

4.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

STEP 1: Select **Quick Setup** to display this screen.

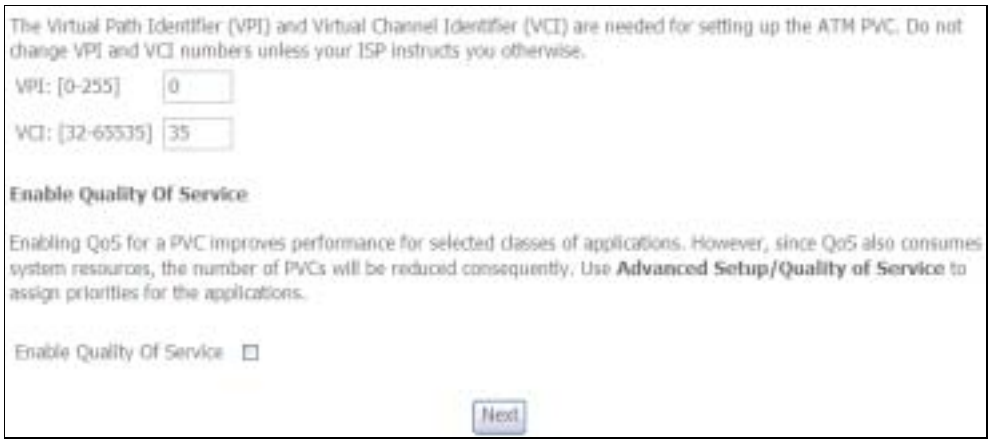
STEP 2: Click **Next** to start the setup process. Follow the online instructions to complete the settings. This procedure will skip some processes such as the PVC index and encapsulation mode selection.

STEP 3: After the settings are complete, you can use the ADSL service.

4.2 Manual Quick Setup

STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.

Untick this checkbox to enable manual setup and display the following screen.

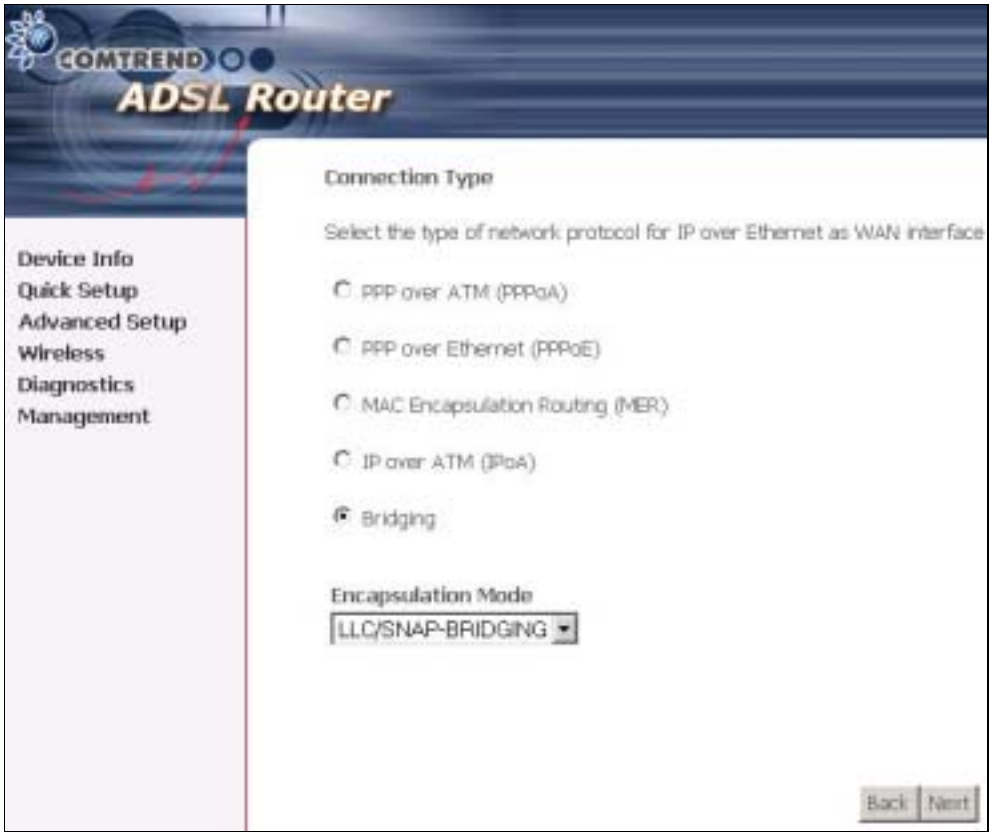


STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click **Next**.

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

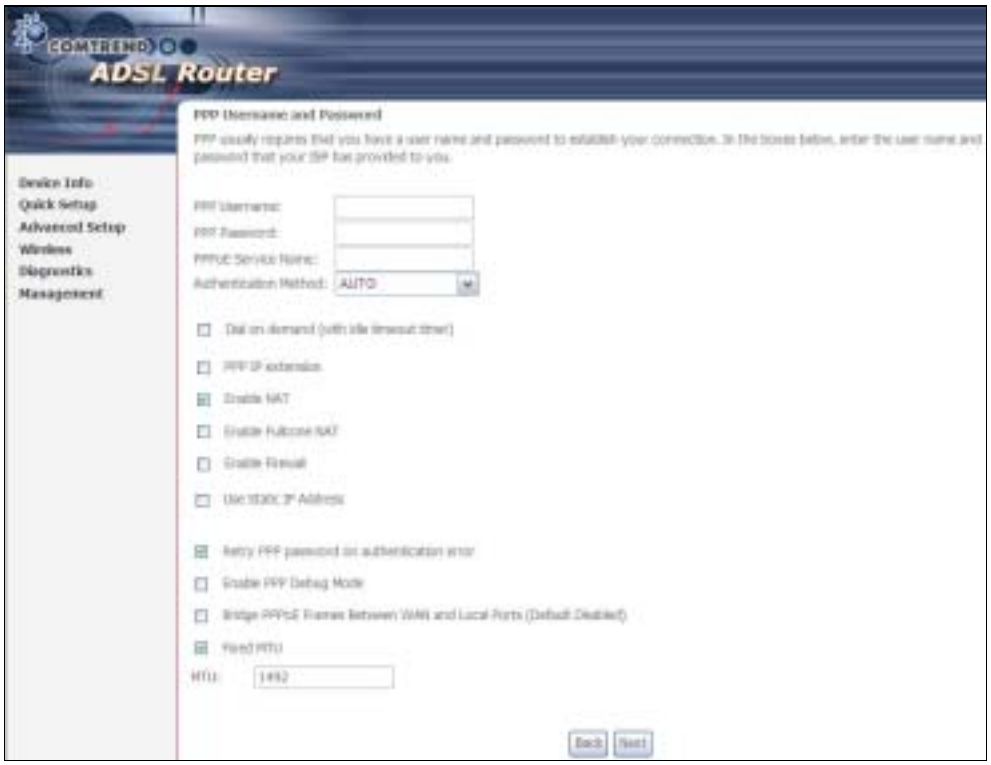
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP RIDGING, VC/MUX
- MER- LLC/SNAP- RIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX



NOTE:	Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

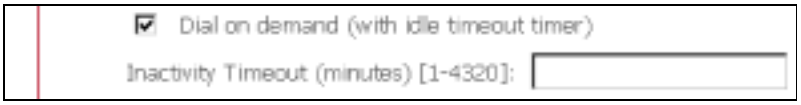


PPP Username/PPP Password: The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, 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.
- 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 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: 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.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address.

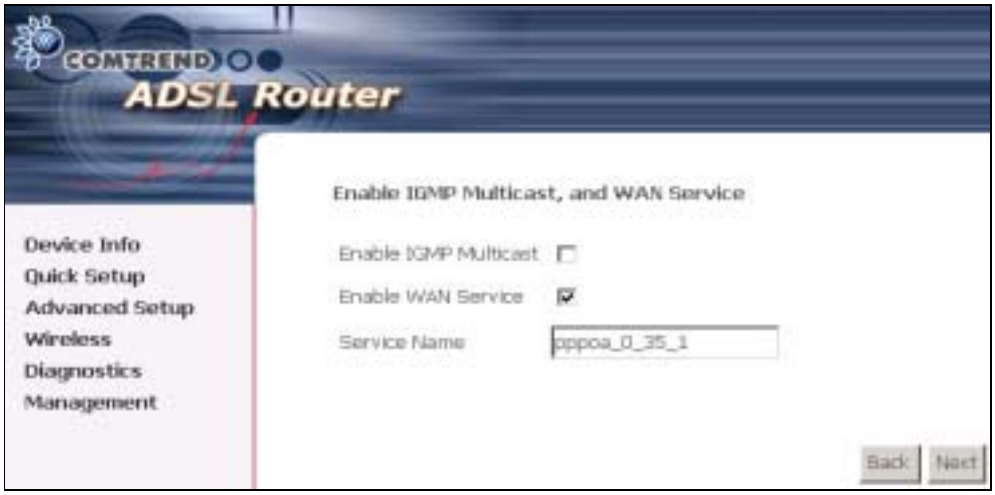
Retry PPP password on authentication error
Tick the box to select.

Enable PPP Debug Mode
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports
If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU
Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click **Next** to display the following screen.



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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

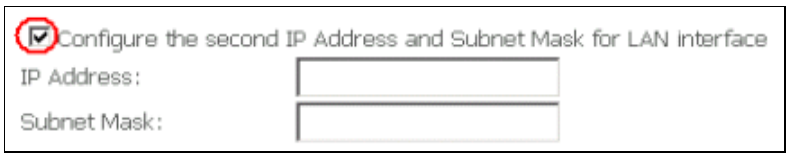
STEP 6: After entering your settings, select **Next**. The following screen appears.

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 and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

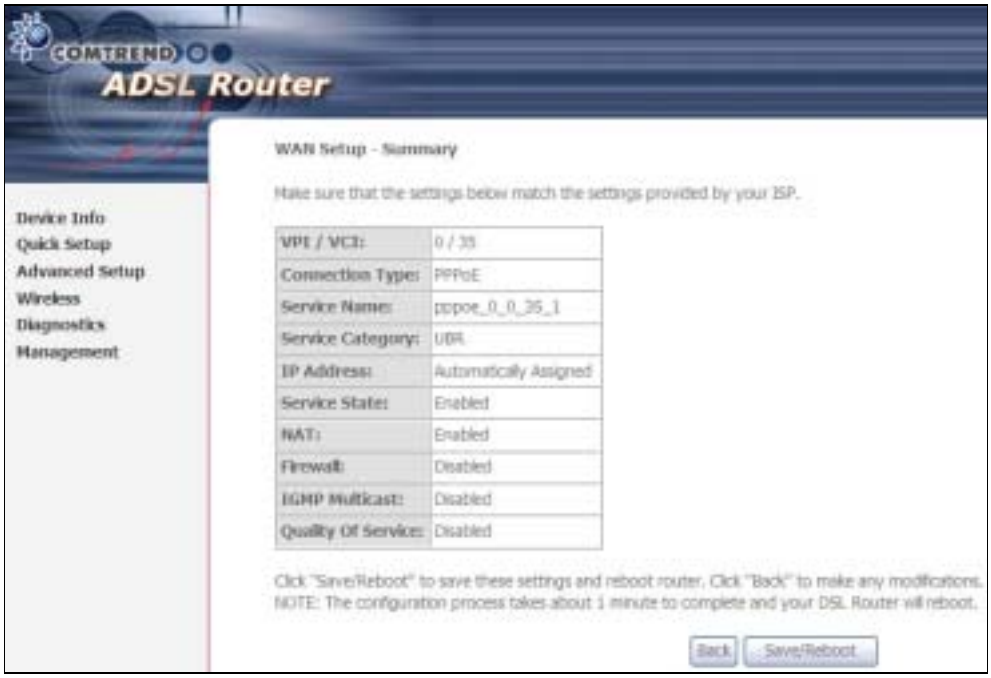
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

4.2.2 MAC Encapsulation Routing (MER)

Step 4: Select the MAC Encapsulation Routing (MER) radio button and click **Next**.

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

NOTE:	DHCP can be enabled for PVC in MER mode 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. Your ISP should provide the values to be entered in these fields.

Step 5: Click **Next** to display the following screen.

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.

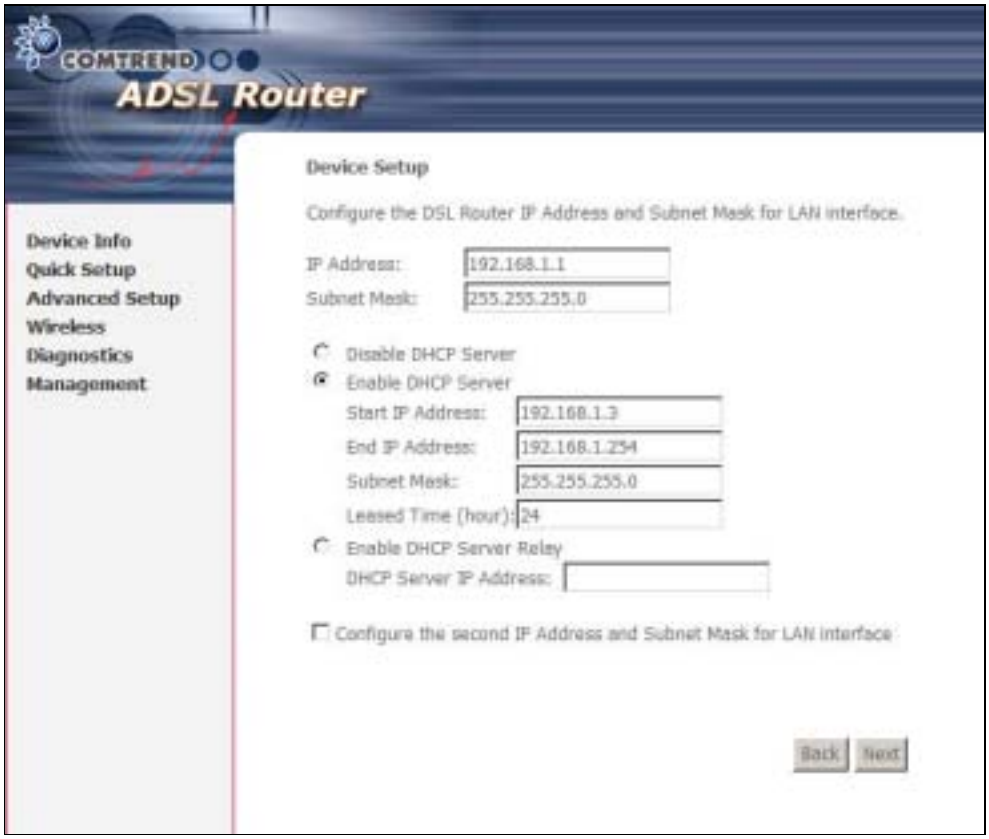
Enable Firewall
If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

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

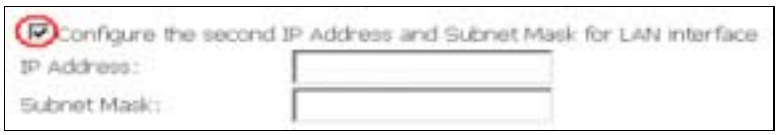


The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

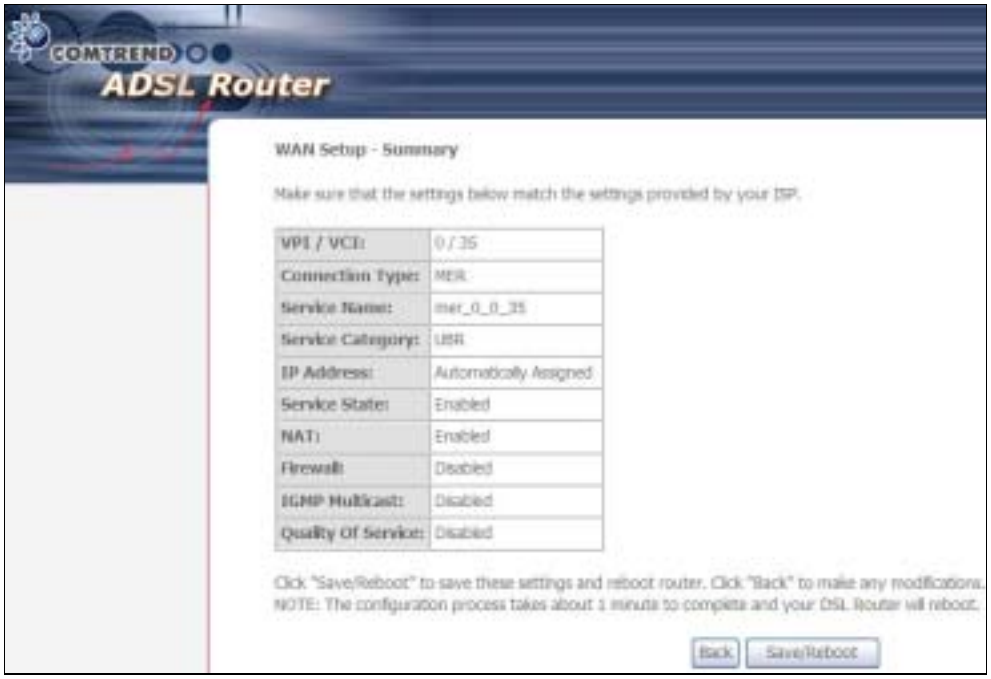
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

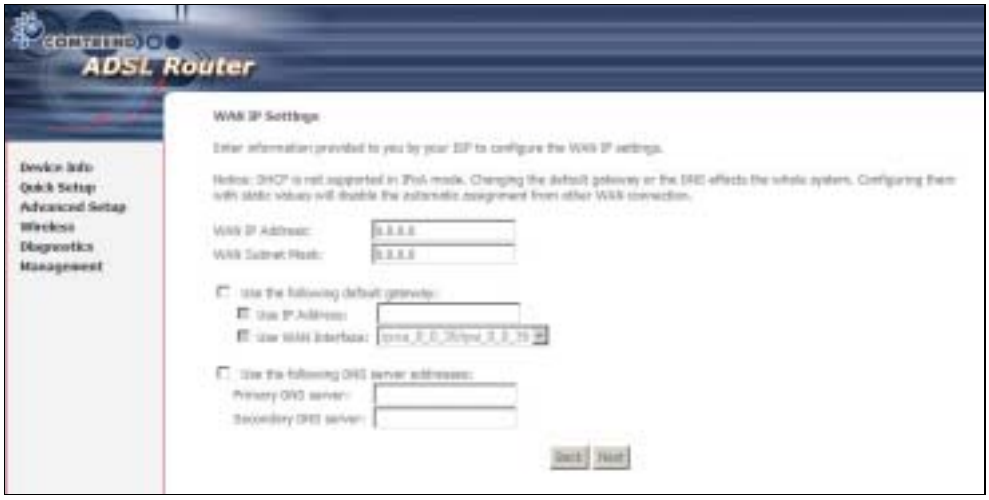
Click **Next** to display the final setup screen.



Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

4.2.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.



NOTE:	DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by their ISP.

Step 5: Click **Next** to display the following screen.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

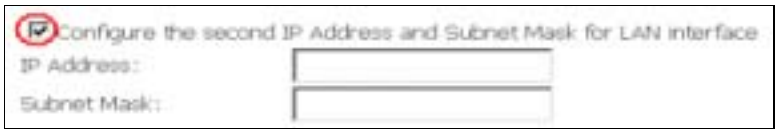
Step 6: Click **Next** to display the following screen.

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 and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.

Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

4.2.4 Bridging

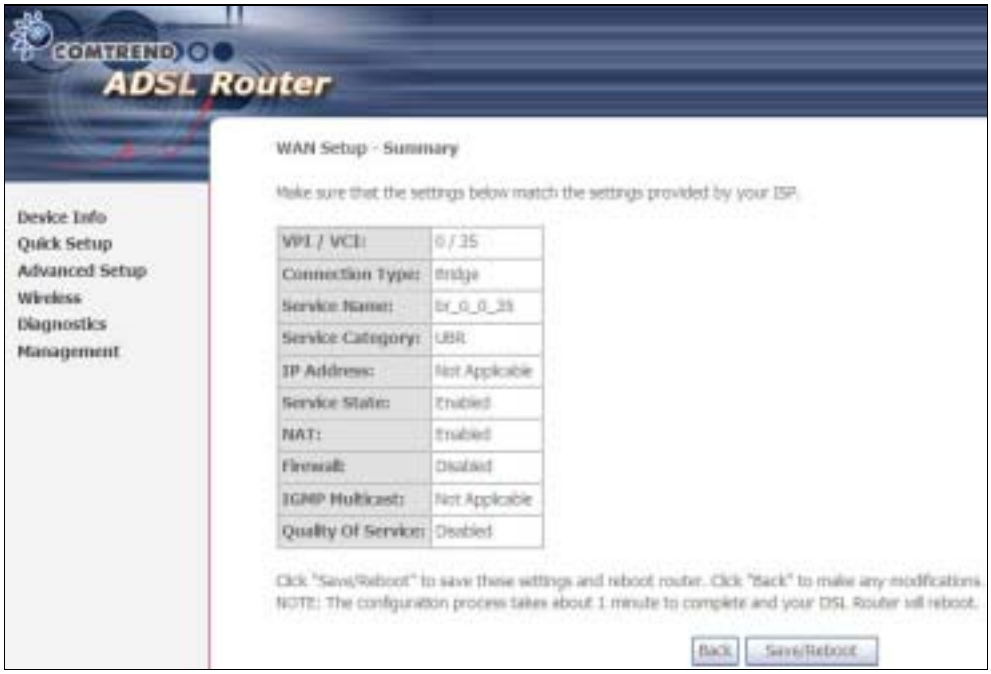
Step 4: Select the ridging radio button and click **Next**. The following screen appears. Select **Enable Bridge Service** and click **Next**.

Step 5: On this screen, you can change the LAN IP address of the router.

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

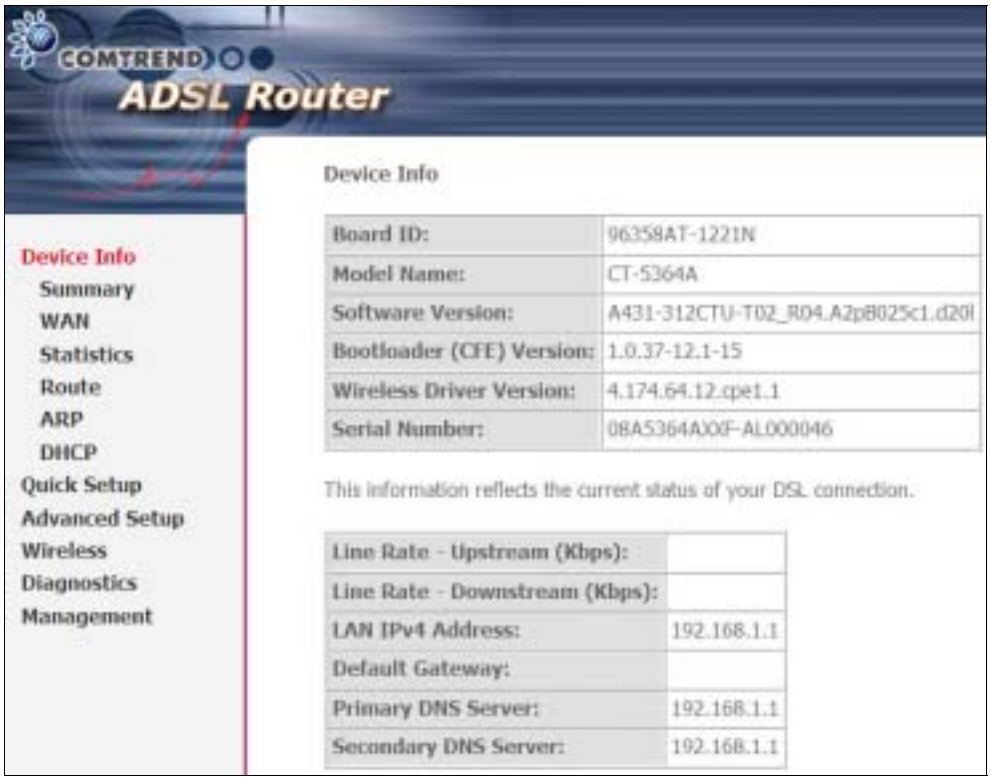
Chapter 5 Device Information

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

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

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

The Device Info Summary screen displays at startup.



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

5.1 WAN

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

Port/VPI/VCI	Shows the values of the ATM VPI/VCI
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	Shows the connection ID
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 status of IGMP
NAT	Shows the status of NAT
Firewall	Shows the status of the Firewall
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address

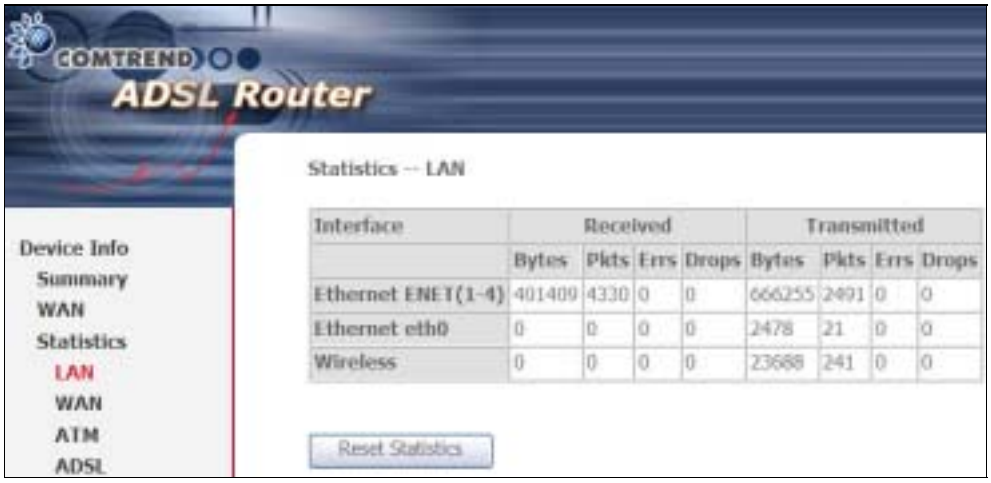
5.2 Statistics

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

NOTE:	These screens are updated every 15 seconds.

5.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



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

5.2.2 WAN Statistics

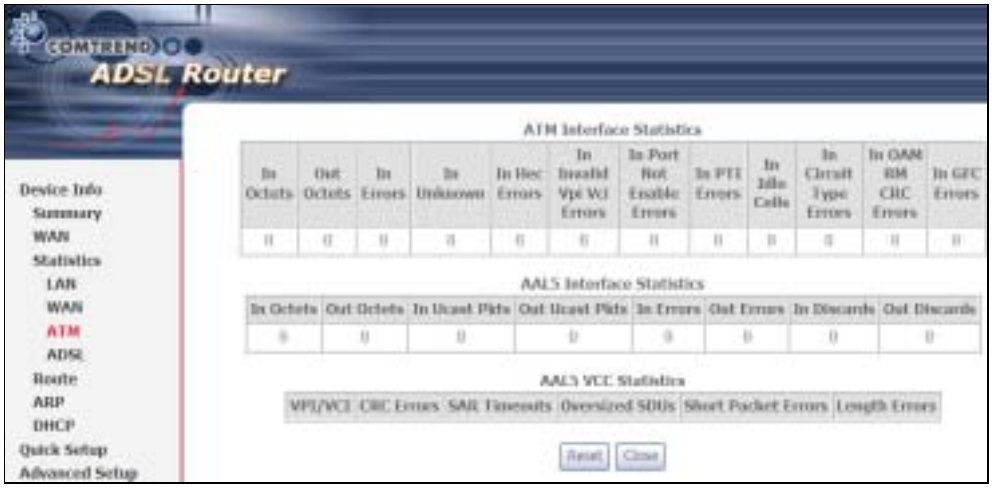
This screen shows data traffic statistics for each WAN interface.

Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted - ytes - 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

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

5.2.3 ATM Statistics

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



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.

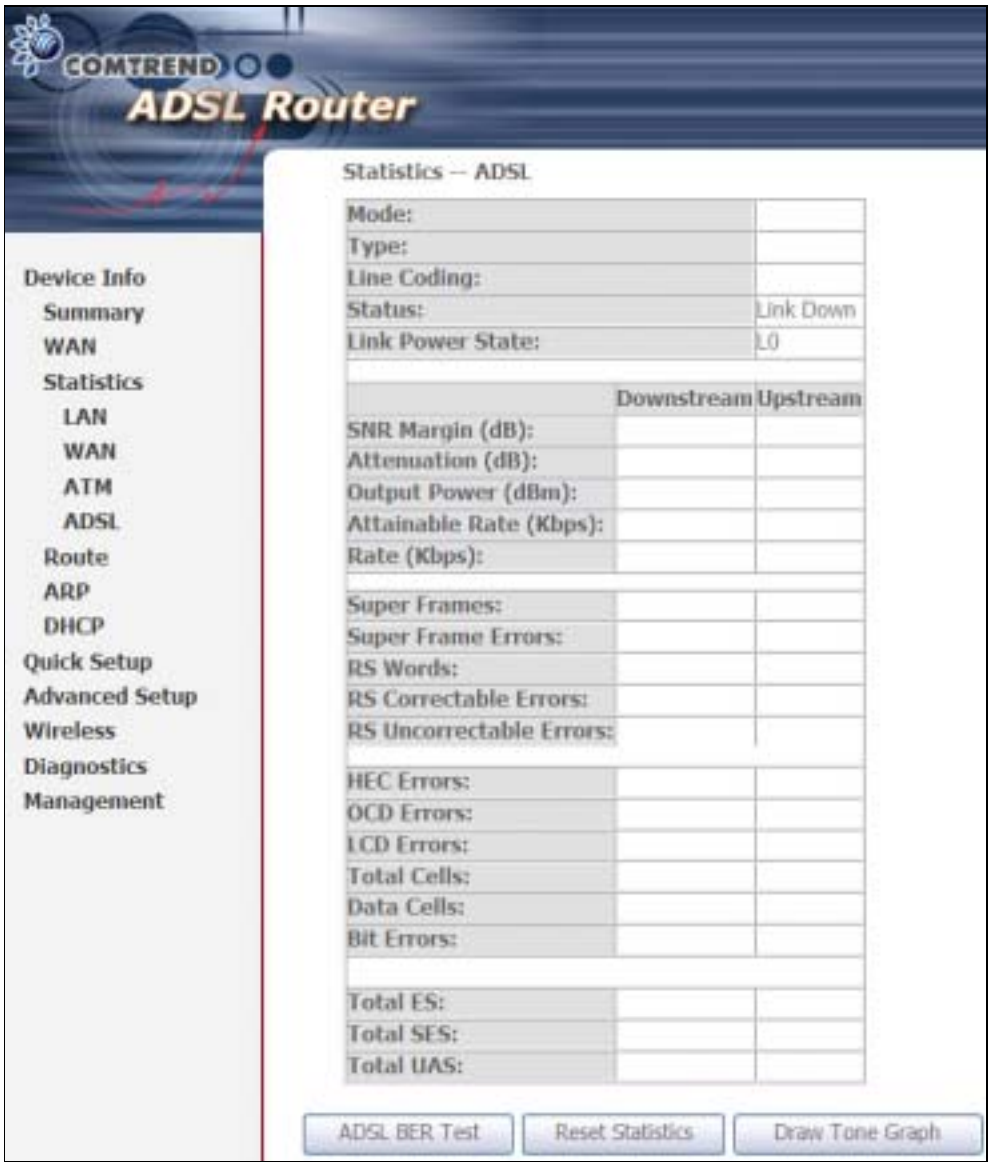
AAL5 Interface Statistics

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

AAL5 VCC Statistics

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.
Oversized 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 xDSL Statistics



Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
PhyR Status:	A new impulse noise protection technology that uses to improve voice, data and video services.
SNR Margin (d)	Signal to Noise Ratio (SNR) margin
Attenuation (d)	Estimate of average loop attenuation in the downstream direction.

Output Power (d m)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
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
it Errors:	Total number of bit errors
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

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.

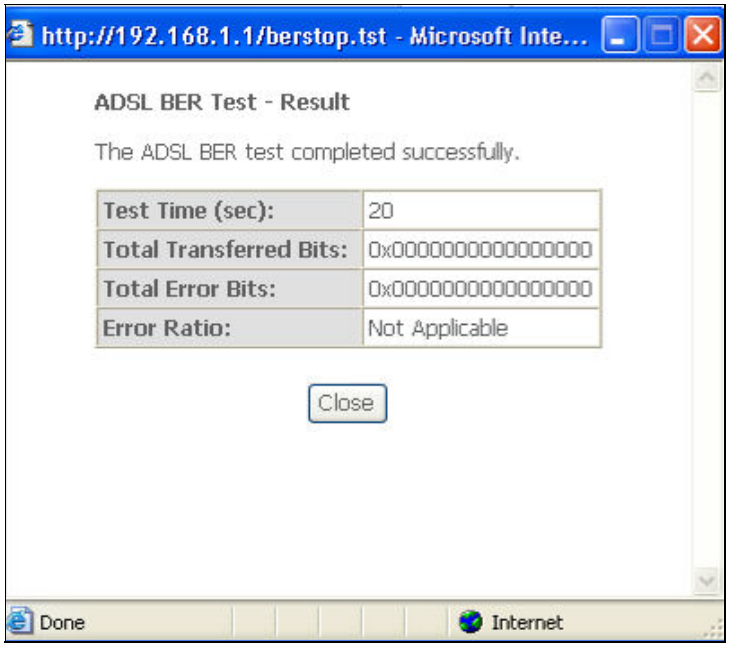
MSGc	Number of bytes in overhead channel message
	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

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

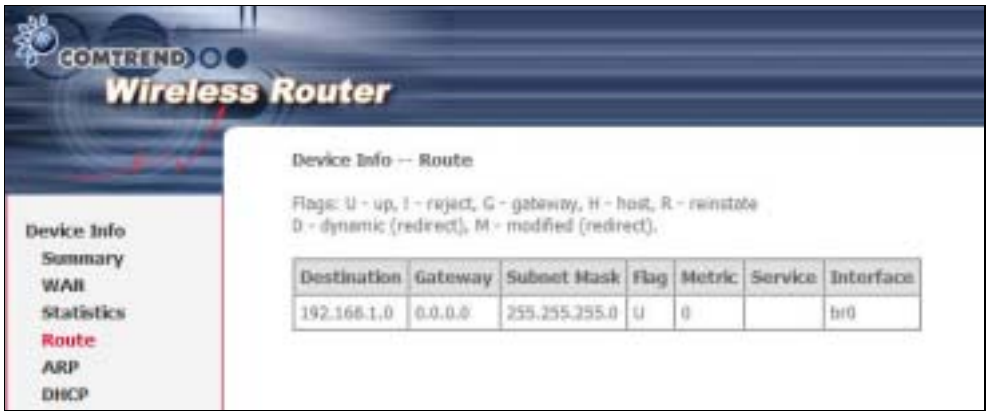
Within the ADSL Statistics window, a it Error Rate (ER) test can be started using the **ADSL BER Test** button. A small window will open when the button is pressed; it will appear as shown below. Click **Start** to start the test or **Close**.

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



5.3 Route

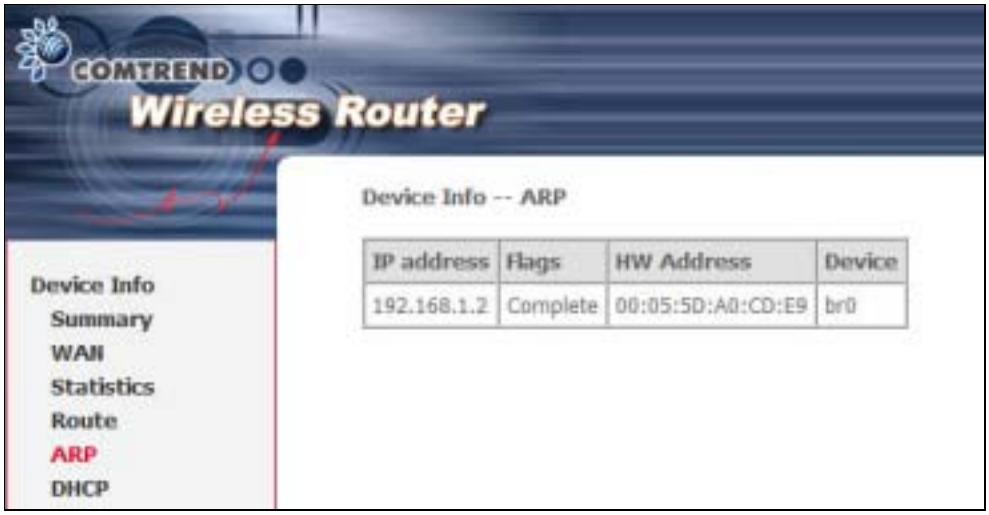
Choose **Route** to display the routes that the CT-5364A has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

5.4 ARP

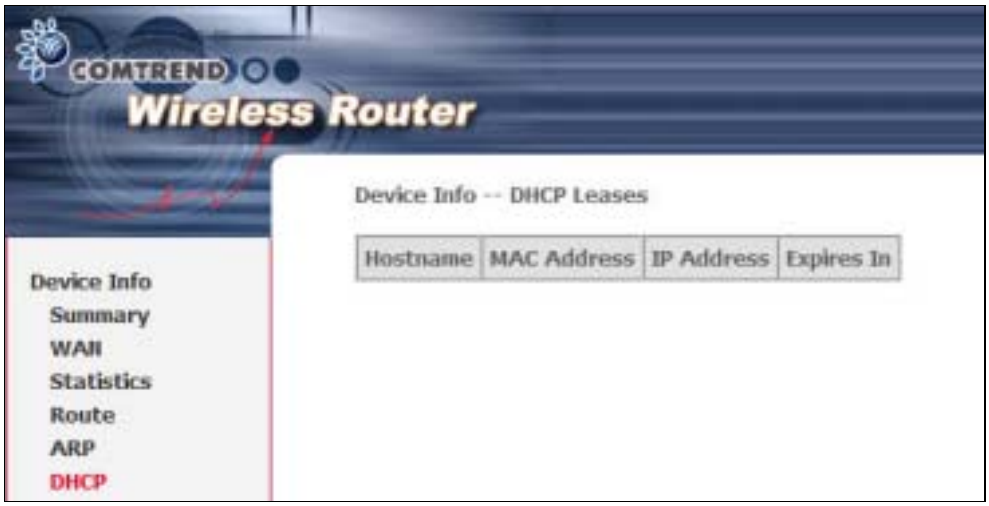
Click **ARP** to display the ARP information.



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

5.5 DHCP

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



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

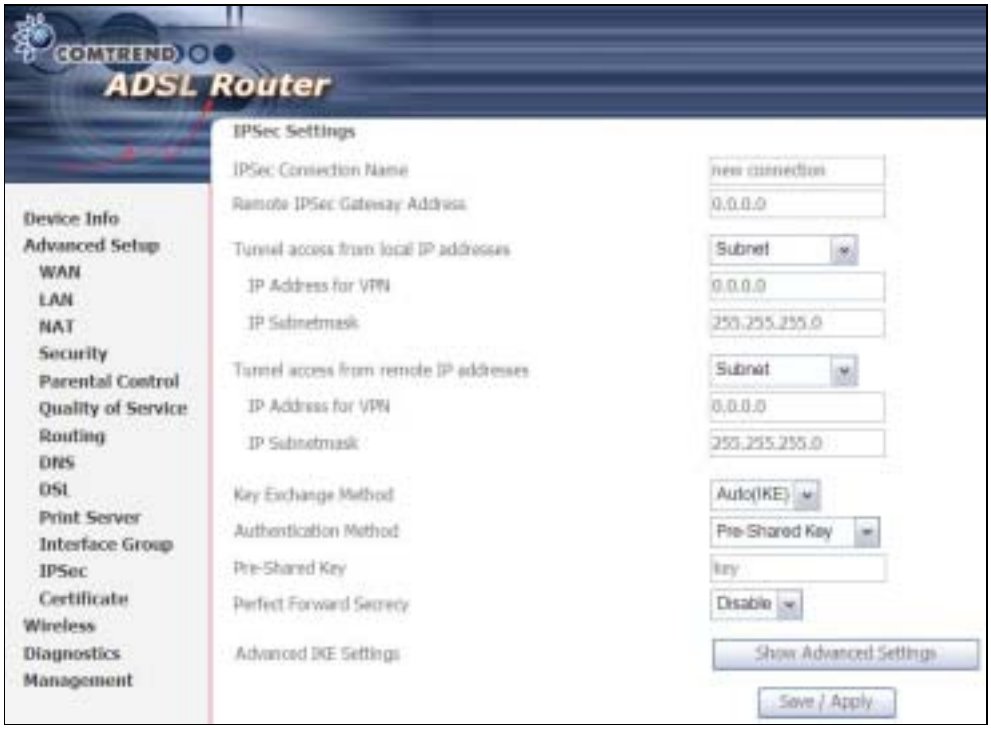
Chapter 6 Advanced Setup

This chapter explains the following screens:

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

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

The following screen will display.



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

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

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

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable

Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.

Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

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

Manual Key Exchange Method	

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

Certificate

6.1 WAN

This screen allows for the advanced configuration of 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 complete the **Add** or **Edit**, on the opening screen, select VLAN Mux (see section 5.1.1) and then proceed to **STEP**

2 in section Manual Quick Setup.

- To remove a connection select its radio button under the **Remove** column in the table and click the **Remove** button under the table.
- **Save / Reboot** activates the new configuration.

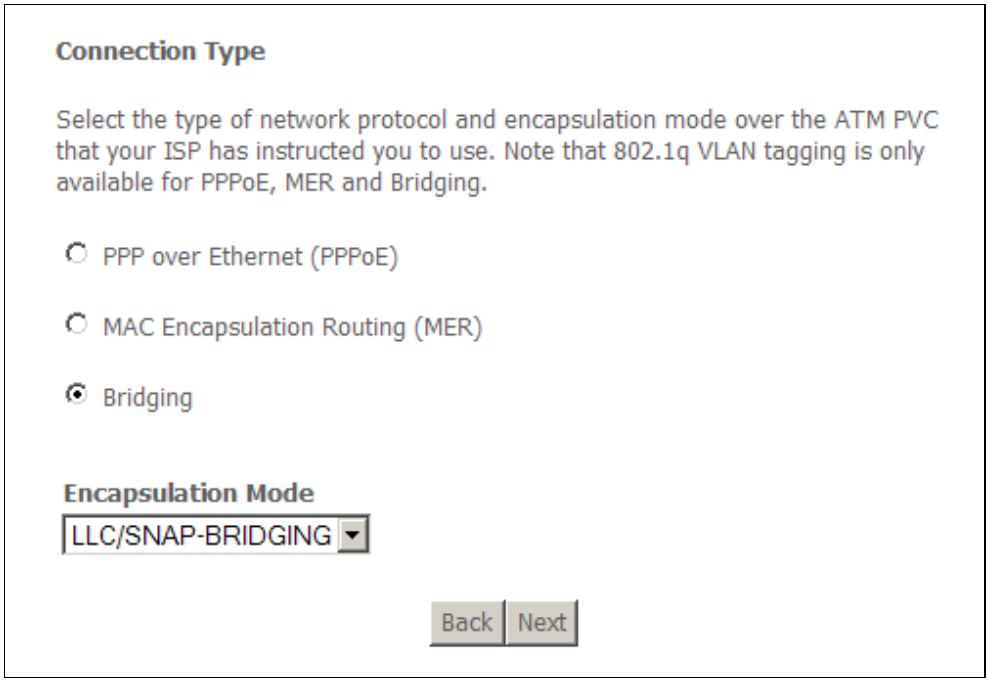
VPI/VCI	VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	ID for WAN connection
Category	ATM service category, e.g. U R, C R...
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
NAT	Shows enable or disable NAT
Firewall	Shows enable or disable Firewall
QoS	Shows enable or disable QoS
State	Shows enable or disable WAN connection
Remove	Select or deselect the connection for removal
Edit	Click **Edit** to change connection settings

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.

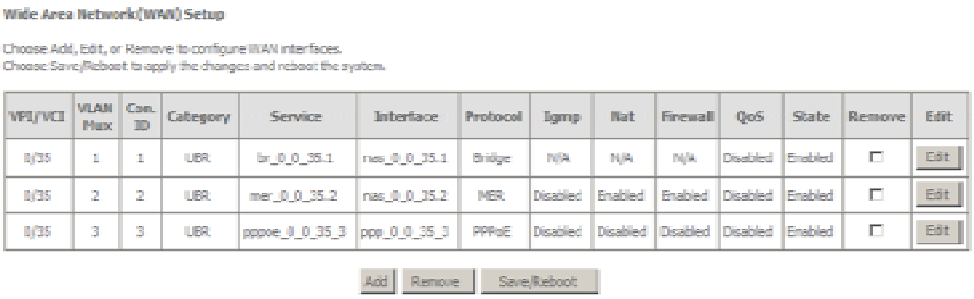
This option is found on the Advanced WAN Setup screen. This is the first screen you will see when adding or editing a connection. VLAN Mux can be enabled by selecting the **VLAN Mux – Enable Multiple Protocols Over a Single PVC** check box, outlined in red below. Enter a value between 0 and 4095 for **802.Q VLAN ID**.

After proceeding to **STEP 3** in section Manual Quick Setup, the screen will appear as follows. Notice that PPPoA and IPoA are not available.



PVCs can be added using the regular procedure, however, now multiple protocols can exist over the same connection, as long as the 802.1Q VLAN IDs differ.

The graphic below shows an example of three protocols over 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	1	1	UBR	br_0_0_35.1	nas_0_0_35.1	Bridge	N/A	N/A	N/A	Disabled	Enabled	☐	Edit
0/35	2	2	UBR	mer_0_0_35.2	nas_0_0_35.2	MER	Disabled	Enabled	Enabled	Disabled	Enabled	☐	Edit
0/35	3	3	UBR	pppoe_0_0_35_3	ppp_0_0_35_3	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	☐	Edit

Add | Remove | Save/Reboot

6.1.2 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the VLAN Mux function, PPPoE, ridge 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 ridge + multiple PPPoE / One MER)

Part 2 - Use Port Mapping to connect LAN / WAN interfaces

The following example shows how to configure a ridge / PPPoE MSP connection. The same process can be used for ridge / MER MSP connections.

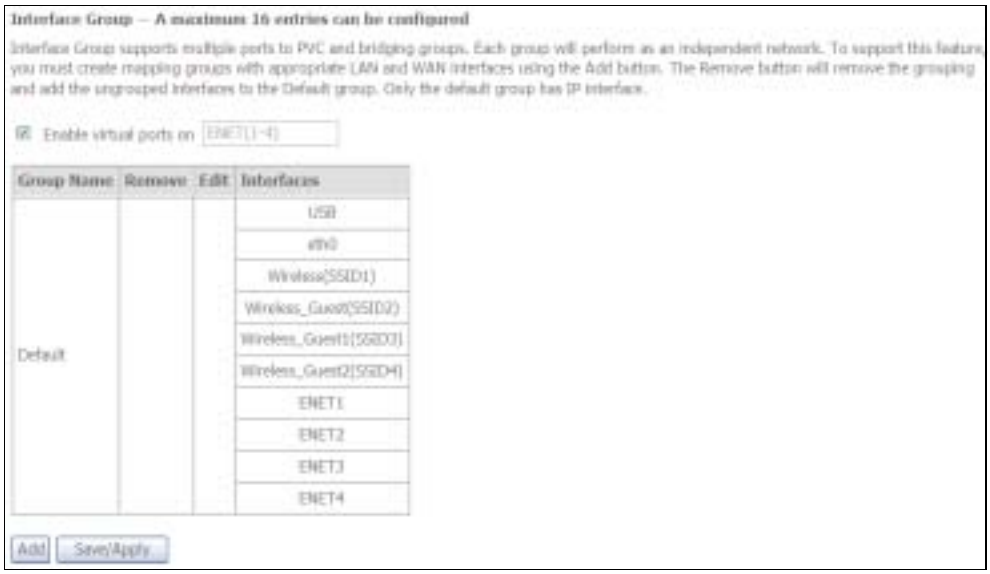
NOTE:	If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections. If a MSP connection is removed every other MSP connection should be removed to avoid port mapping configuration problems.

Part 1 – Create Multiple PVCs

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

Part 2

Go to Advanced Setup – Interface Group screen and select the **Enable Virtual Ports** checkbox. The screen will display as follows.

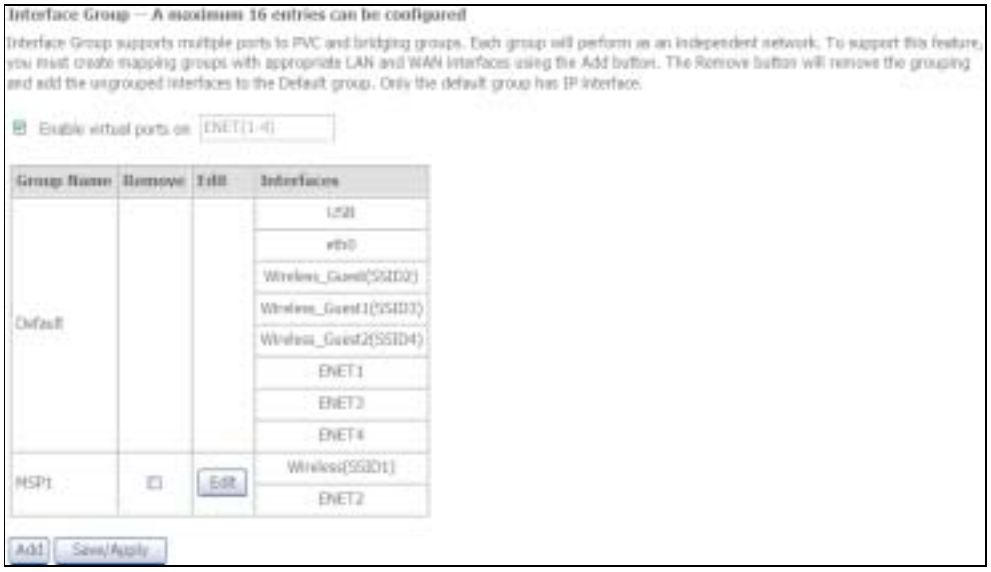


NOTE: Only the ridge PVC is shown on the Port Mapping configuration. It is in

the format of “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 next screen, select the bridge connection and one Ethernet virtual port (ENET 1-4) and enter a **Group Name**, such as “MSP1”, as shown below. Click **Save/Apply**.

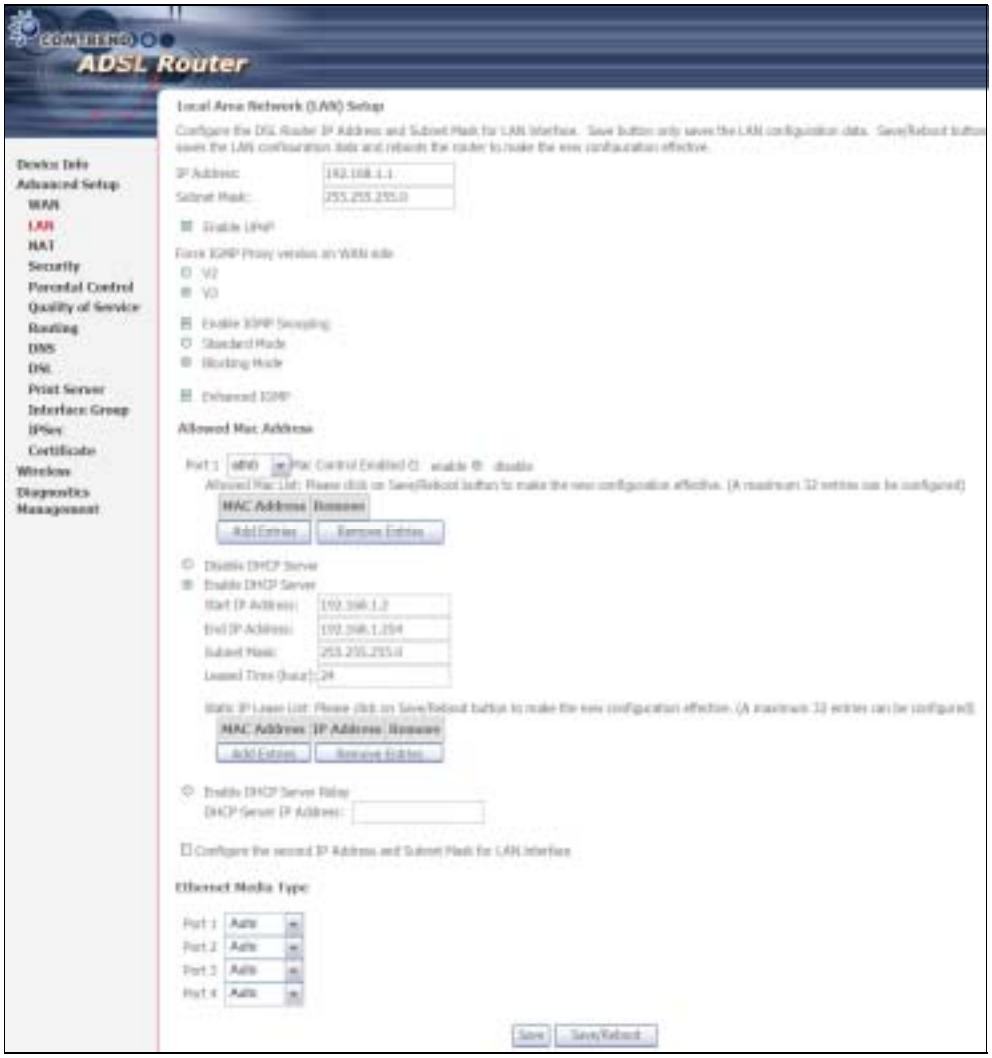
If successfully configured, the Port Mapping screen will display as follows.



NOTE: If you wish to maintain local access to the web user interface, avoid grouping the Ethernet interface that is attached to the host PC.

6.2 LAN

Configure local area network (LAN) settings here.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

<u>1st LAN INTERFACE</u>

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.
<u>This option is hidden when NAT disabled or if no PVC exists</u>

Force IGMP Proxy version on WAN side: V2 is selected by default. Select V3 if required.

Enable IGMP Snooping: Enable by ticking the checkbox ☑.

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

locking 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.

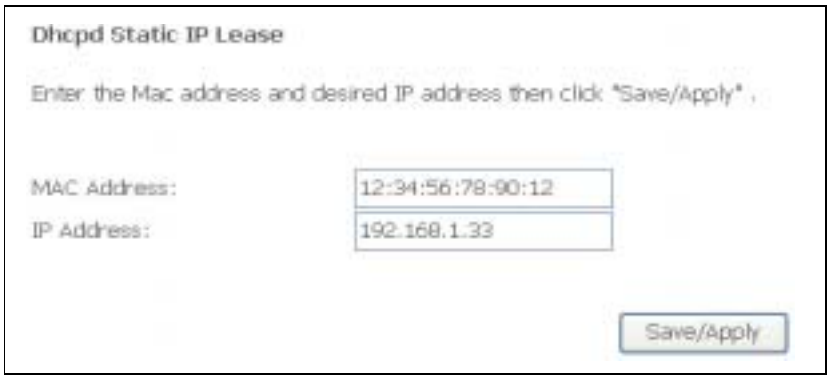
Enhanced IGMP: When enabled, IGMP packets will not flood to all bridge ports.

Allowed Mac Address: Displays the MAC address(es) allowed to pass throughput LAN interface.

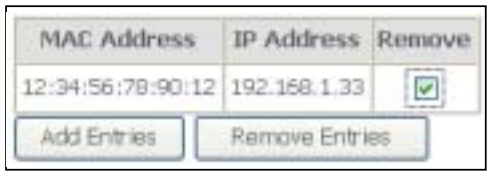
DHCP Server: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. *This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.*

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

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



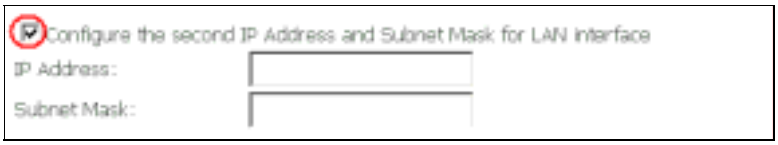
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



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*

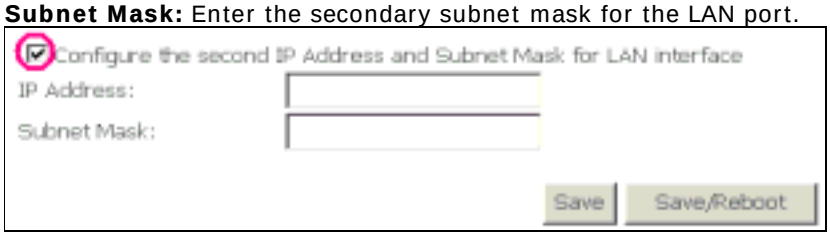
2ND LAN INTERFACE

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



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

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



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).

Ethernet Media Type: Select from Auto, 10_Half, 10_Full, 100_Half or 100_Full for each Ethernet port.

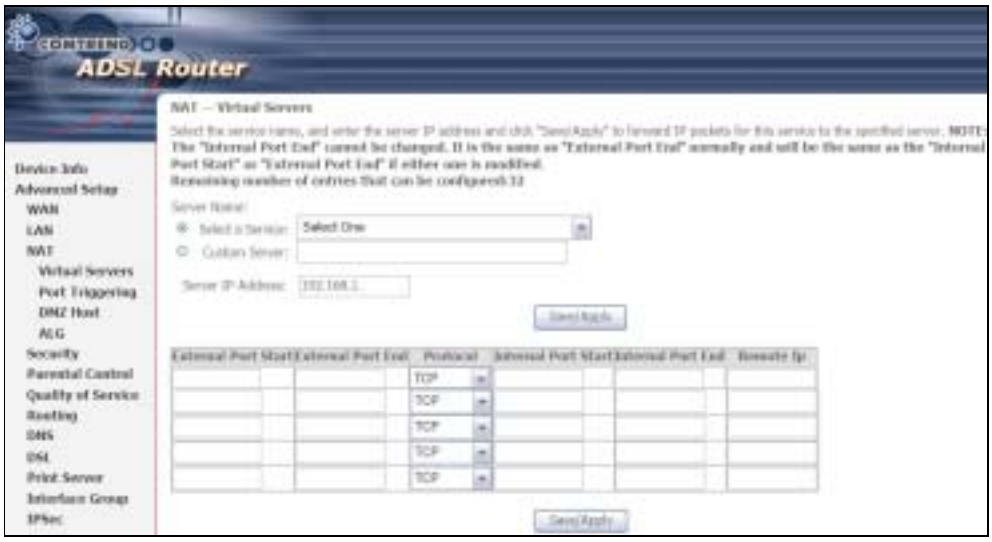
6.3 NAT

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

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 **Add**. The following will be displayed.



Consult the table below for field and header descriptions.

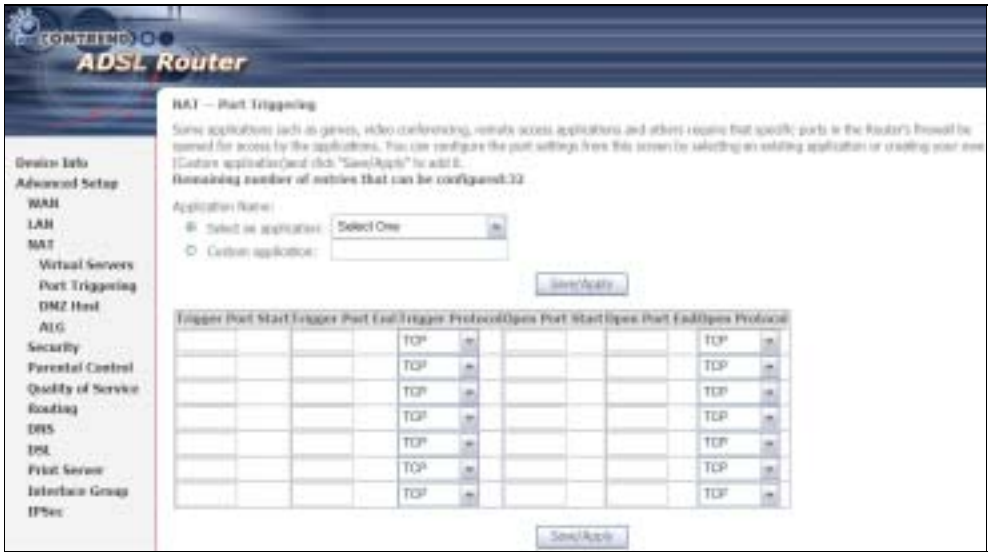
Field / Header	Description
Select a Service **Or** Custom Server	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.

Field / Header	Description
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

6.3.2 Port Triggering

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

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



Consult the table below for field and header descriptions.

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

6.3.3 DMZ Host

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

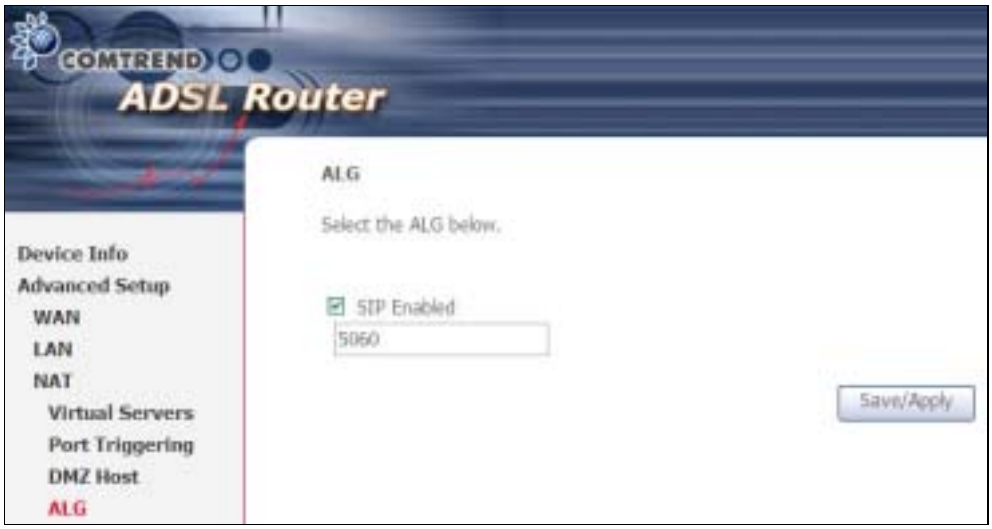
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save / Apply**.

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

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

6.4.1 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering (pg. 61) performs a similar function.

格式化: 醒目提示

OUTGOING IP FILTER

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

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

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
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 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

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

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

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
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 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.

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

6.4.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use IP Filtering (pg. 59) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5364A can be set according to the following procedure.

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

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

Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, Net EUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to selected WAN interfaces in bridge mode. These rules are arranged according to these interfaces, as shown under the **Interface** heading on the previous screen.

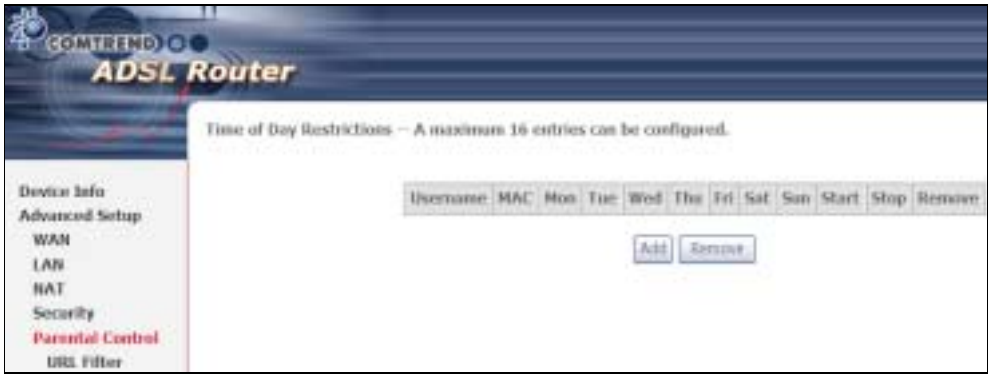
6.5 Parental Control

This selection provides WAN access control functionality.

6.5.1 Time of Day Restrictions

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 9.5, so that the scheduled times match your local time.

格式化: 醒目提示



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

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

User Name: A user-defined label for this restriction.

Browser's MAC Address: MAC address of the PC running the browser.

Other MAC Address: MAC address of another LAN device.

Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

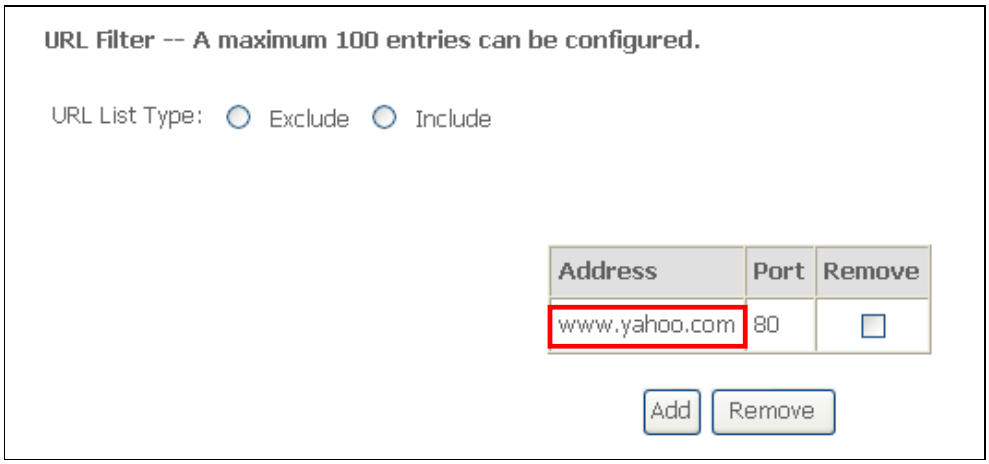
End Blocking Time: The time the restrictions end.

6.5.2 URL Filter

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

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. URL Addresses begin with "www", as shown in this example.



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.

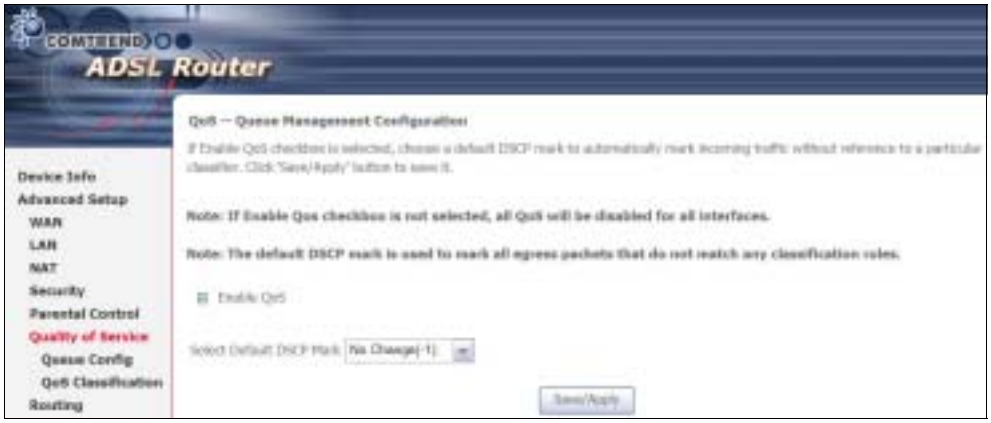
6.6 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.

6.6.1 Queue Management Configuration

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

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



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

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

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

6.6.2 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.

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

Queue Configuration Status: Select Enable or Disable the Queue entry.

Queue: Assign queue to a specific network interface with QoS enabled.

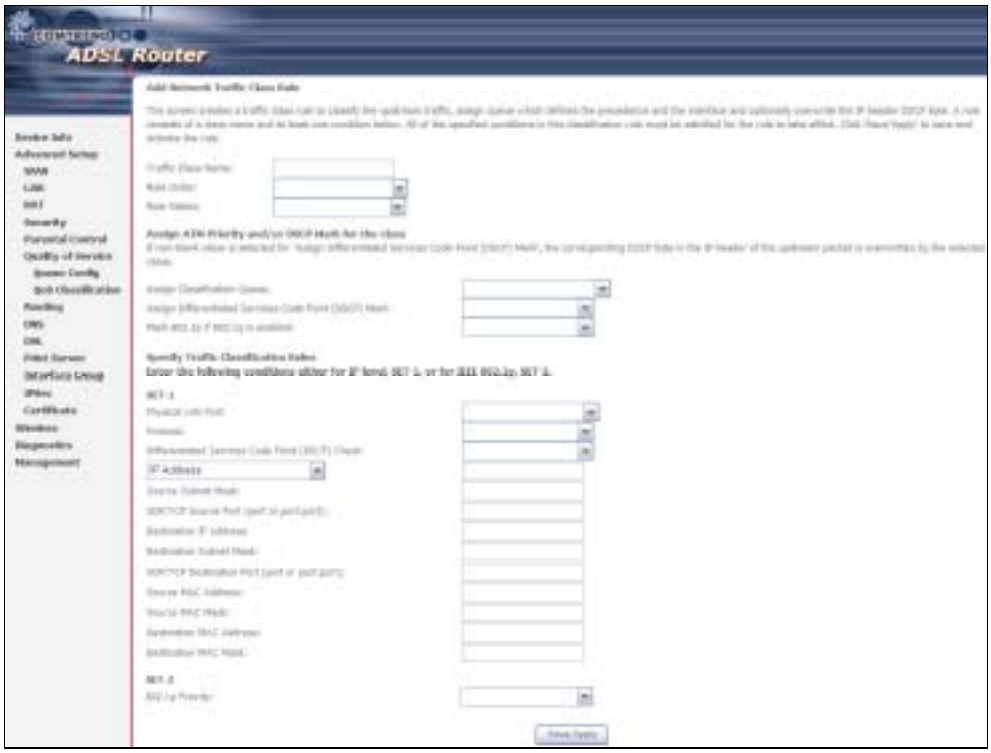
Queue Precedence: Configure precedence for the Queue entry. Lower integer values for precedence imply higher priority for this entry relative to others.

6.6.3 QoS Classification

The network traffic classes are listed in the following table.

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

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



Click **Save / Apply** to save and activate a rule.

Field	Description
Traffic Class Name	Enter a name for the traffic class.

Field	Description
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 eth0-eth4 or Wlan from the dropdown menu.
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.
IP Address	Select IP Address, Vendor Class ID (DHCP Option 60), or User Class ID (DHCP Option 77)
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 controls **Default Gateway, Static Route, Policy Routing** and **RIP**.

NOTE:	In bridge mode, the **RIP** screen is hidden while the other configuration screens are shown but ineffective.

6.7.1 Default Gateway

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.

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

6.7.2 Static Route

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

Click the **Add** button to display 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.

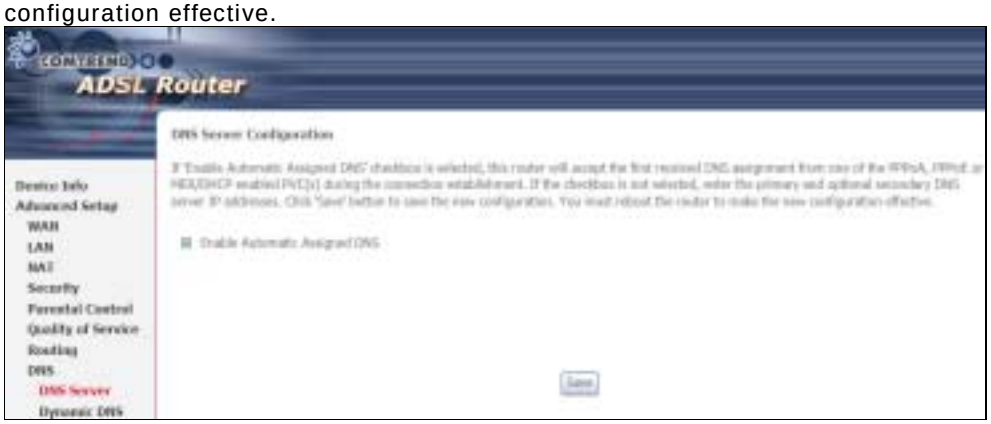
6.7.3 RIP

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

6.8 DNS

6.8.1 DNS Server

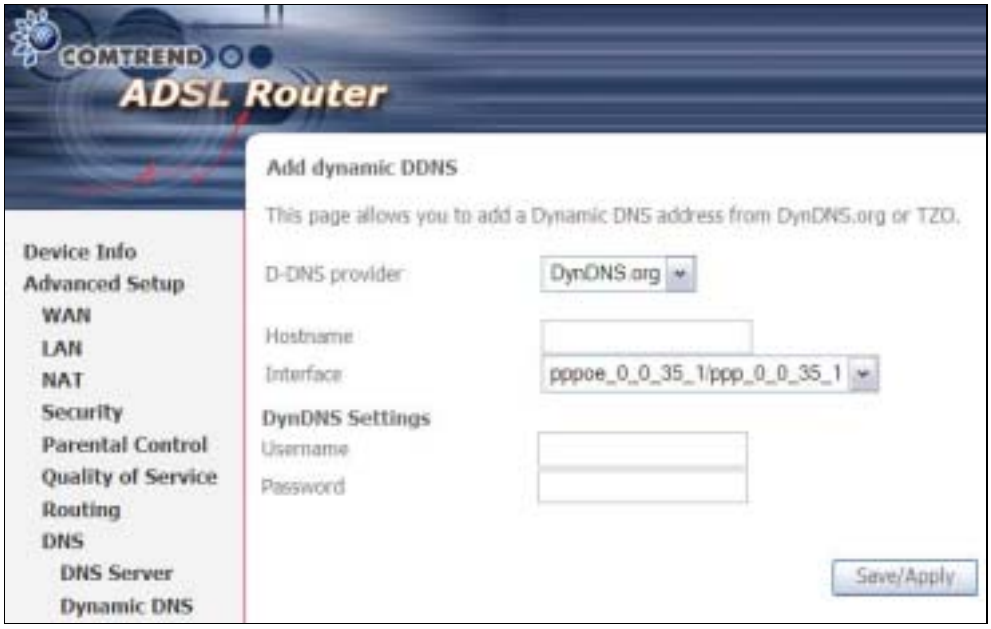
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.



6.8.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the CT-5364A to be more easily accessed from various locations on the Internet.

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

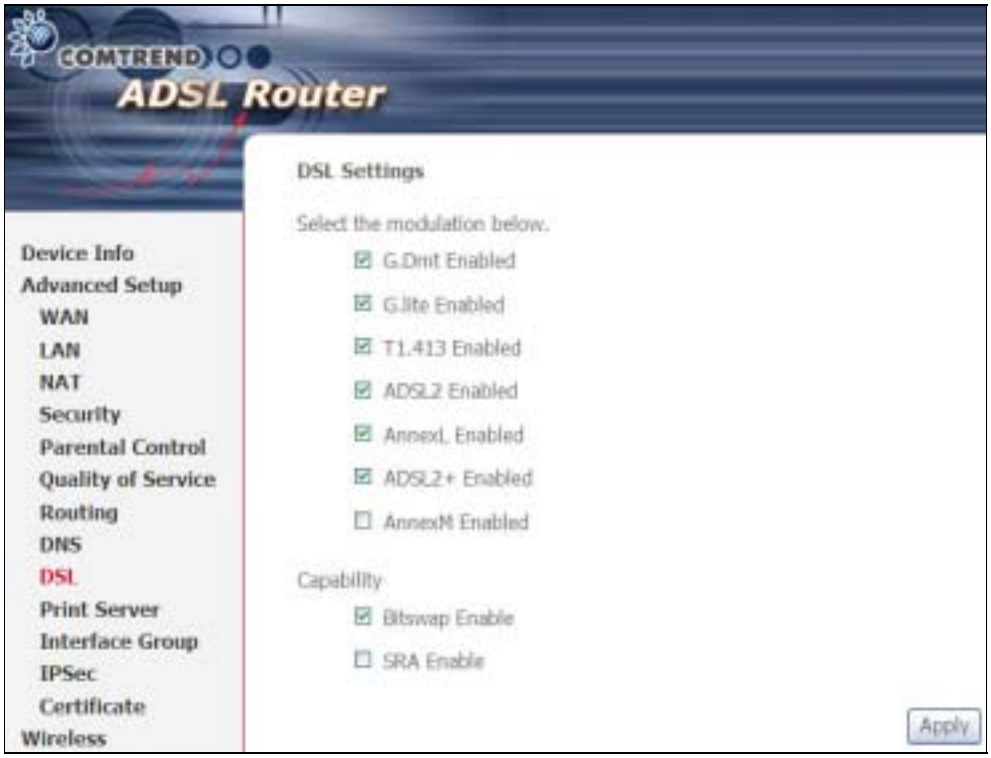


Consult the table below for field descriptions.

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

6.9 DSL

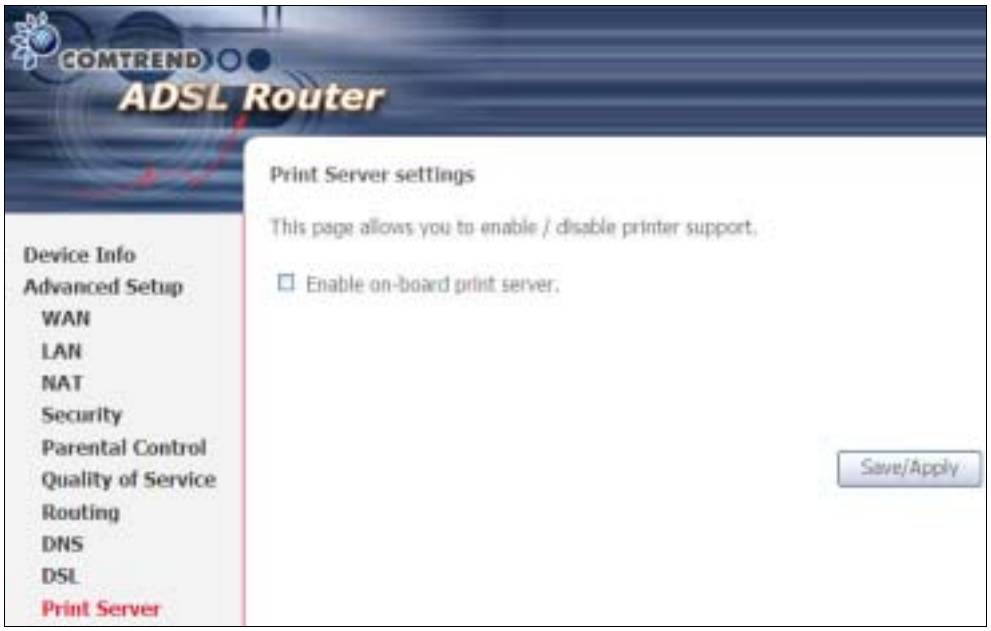
The DSL Settings screen allows for the selection of DSL modulation modes.
For optimum performance, the modes selected should match those of your ISP.



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**
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
itswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)

6.10 Print Server

The CT-5364A provides printer support through a high-speed US 2.0 host port. Please refer to Appendix E for detailed installation instructions.



6.11 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.

The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

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

NOTE:	To assign Ethernet Ports ENET(1-4) to separate Interface Groups, the VLAN Port feature must be activated. See section 錯誤! 找不到參照來源。 for details.

格式化: 醒目提示

DHCP Vendor IDs

Add support to automatically map LAN interfaces using DHCP vendor ID (option 60). The local DHCP server will forward these types of requests to a remote DHCP server.

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

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

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

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

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

6.12 IP Sec

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

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

The following screen will display.

IPSec Connection Name	User-defined label
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.

Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

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

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

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.
Advanced IKE Settings Phase 1 Mode Encryption Algorithm Integrity Algorithm Select Diffie-Hellman Group for Key Exchange Key Life Time Phase 2 Encryption Algorithm Integrity Algorithm Select Diffie-Hellman Group for Key Exchange Key Life Time	Hide Advanced Settings Main 3DES MD5 1024bit 3600 Seconds 3DES MD5 1024bit 3600 Seconds
Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

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

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

6.13 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.

6.13.1 Local

CREATE CERTIFICATE REQUEST

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

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

The following table is provided for your reference.

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

IMPORT CERTIFICATE

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

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

6.13.2 Trusted CA

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

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

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

Chapter 7 Wireless

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

7.1 Basic

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

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

Consult the table below for descriptions of all these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.

Option	Description
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Not supported.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
SSID	The SSID is a 48-bit identity used to identify a particular SS (asic Service Set) within an area. In Infrastructure SS networks, the SSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent SS or ad hoc networks, the SSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

7.2 Security

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

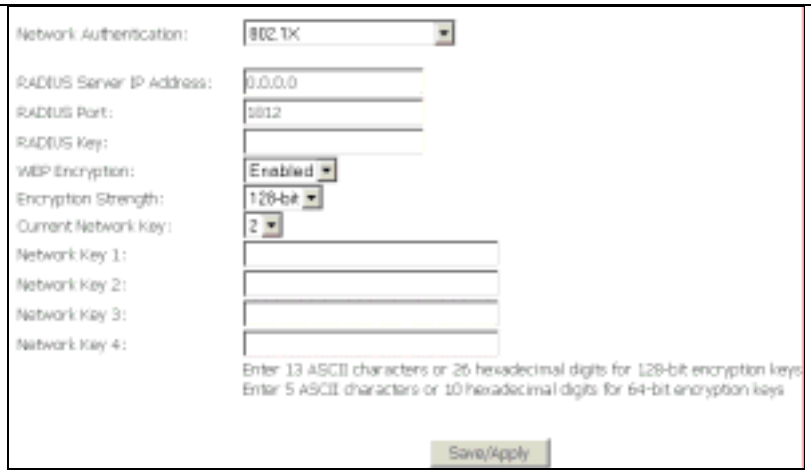
Click **Save / Apply** to implement new configuration settings.

WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see section 7.2.1) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

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

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



The settings for WPA authentication are shown below.

The settings for WPA-PSK authentication are shown next.

WEP Encryption

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

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.
Encryption Strength
This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

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-5364A has both a WPS button on the side panel and a virtual button accessed from the web user interface (WUI).

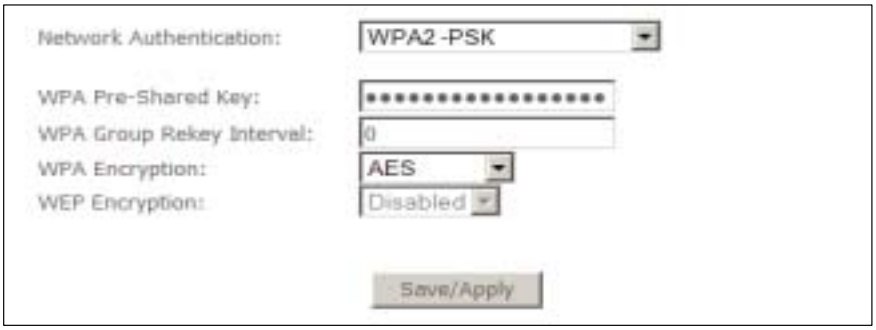
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".

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

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

I. Setup

Step 1: Select WPA-PSK, WPA2-PSK or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The figure here shows WPA2-PSK.



Note: The WSC AP mode is Configured by default.

Step 2: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key (The WPA Pre-Shared Key is set by default).

Step 3: Click the **Save / Apply** button at the bottom of the screen.

IIIa. PUSH-BUTTON CONFIGURATION

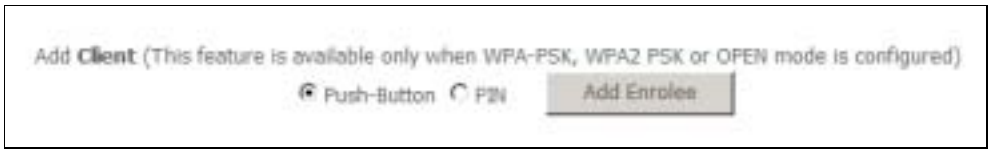
The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

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 5, return to Step 4.

Step 4: **First method: WPS button**
Press the WPS button on the rear panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Second method: WUI virtual button
From the WUI, select the Push- utton radio button in the WSC Add Client section of the Wireless Security screen. Then click the Add button.



Step 5: 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.

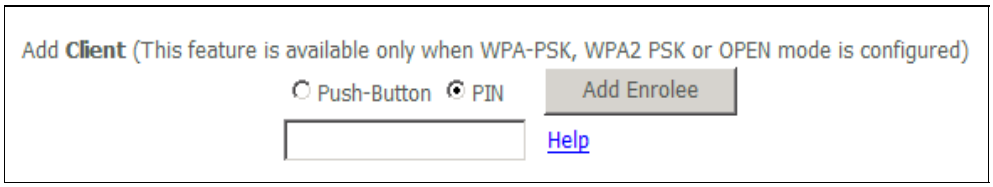
IIIb. WPS – PIN CONFIGURATION

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.

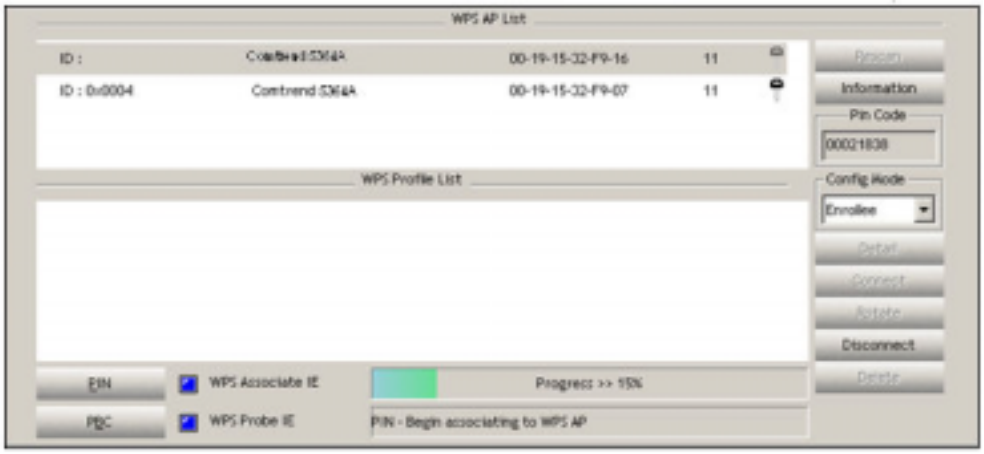
The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function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

NOTE:	The wireless AP on the router will search for WPS clients for 2 minutes. If the router stops searching before you complete Step 5, then return to Step 4 and try again.

Step 6: Select the PIN radio button in the WSC Add Client section of the Wireless Security the client PIN in the box provided and click Add.



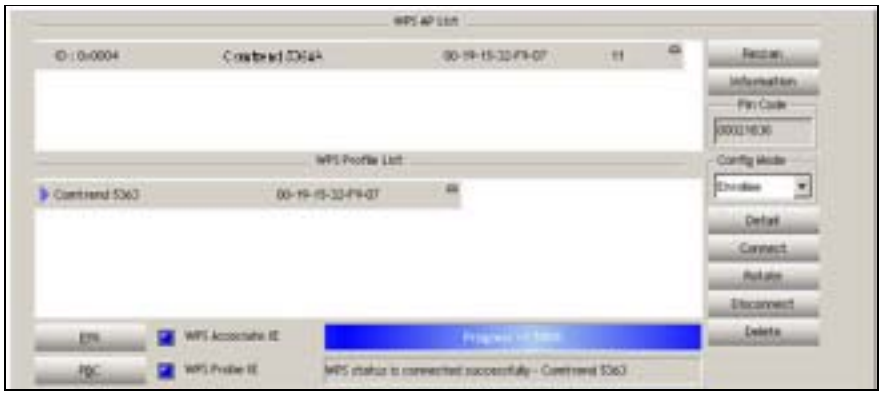
Step 7: Go to your WPS certified client device and activate the PIN function. A screenshot of typical WPS client software is given below as an example.



Proceed to **Step 8** to check the connection.

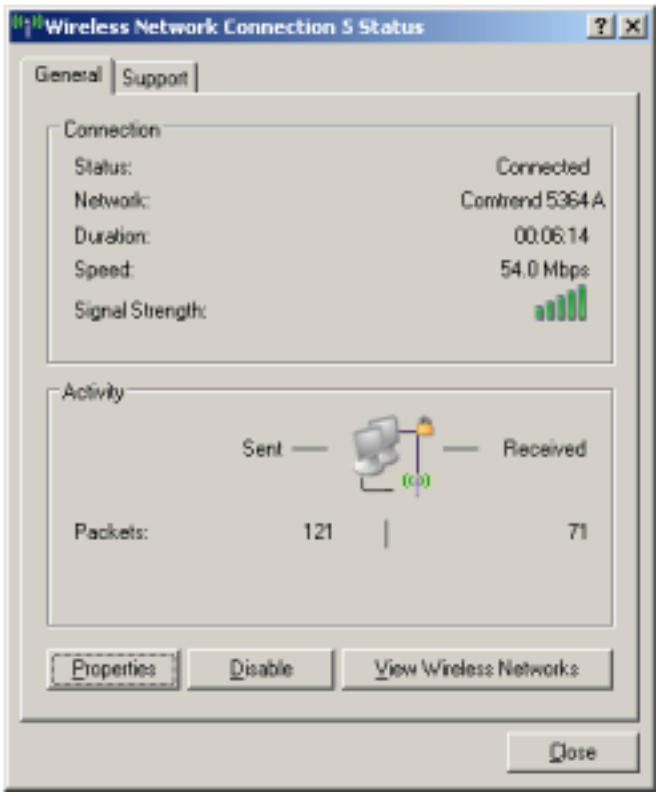
III. CHECK CONNECTION

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 figure below shows an example of a successful connection.



Double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the new connection.

It should appear as shown in the dialog-box below.


Wireless Network Connection 5 Status
General
Support
Connection
Status:
Connected
Network:
Comtrend 5364 A
Duration:
00:06:14
Speed:
54.0 Mbps
Signal Strength:
Activity
Sent
Received
Packets:
121
71
Properties
Disable
View Wireless Networks
Close

7.3 MAC Filter

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

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

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

7.4 Wireless Bridge

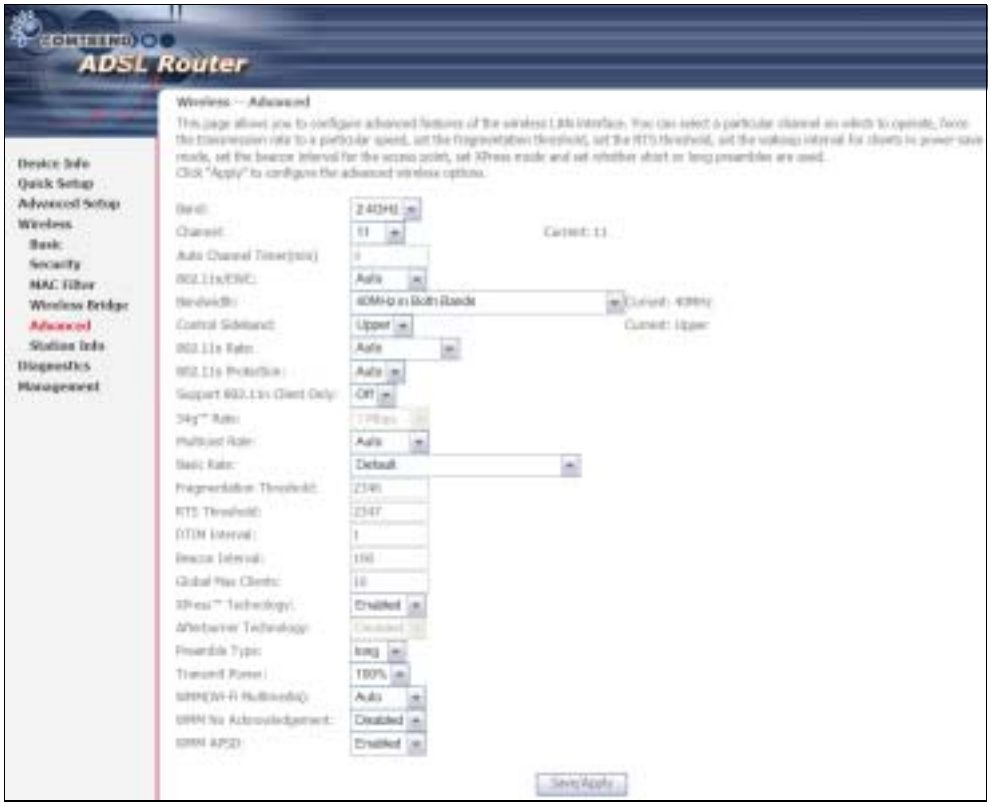
This screen allows for the configuration of wireless bridge features of the WLAN interface. See the table beneath for detailed explanations of the various options.

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

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

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 (**In the U.S only channel 11 can be selected**), force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save / Apply** to set new advanced wireless options.



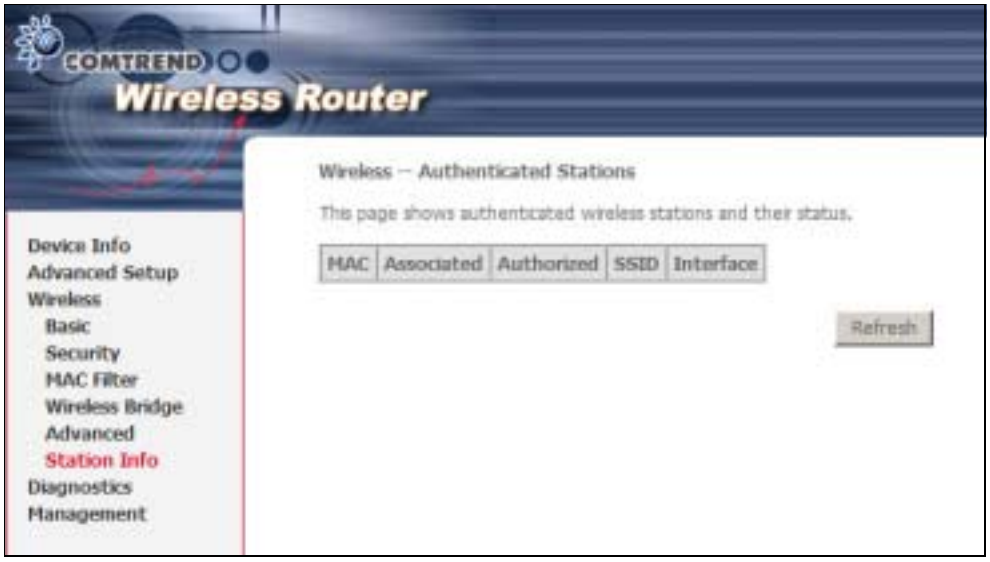
Field	Description
and	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel. **Note:** In the U.S only channel 11 can be selected.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)

Field	Description
andwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.
802.11n Rate	Set the physical transmission rate (PHY) from 6.5 to 130 Mbps.
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
asic Rate	Setting for basic transmission rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as eacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
eacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. y default, network devices passively scan all RF channels listening for beacons coming from access points. efore 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).

Field	Description
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Afterburner Technology	Afterburner technology is an enhancement for the 54g™ platform and can achieve optimal speeds when all network devices include the new technology.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

7.6 Station Info

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



Consult the table below for descriptions of each column heading.

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

Heading	Description
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

8.1 Diagnostics

Diagnostics screens for ATM ridge and PPPoE connection types are shown below.

Bridge Connection

PPPoE Connection

The Diagnostics menu provides feedback on the connection status of the CT-5364A. If a test displays a fail status, click the **Test** button to retest and confirm the error. If the test continues to fail, click Help and follow the troubleshooting procedures provided.

Chapter 9 Management

The Management menu has the following maintenance functions and processes:

99.1 Settings 9.5 Internet Time
9.2 System Log 9.66 Access Control
0 SNMP Agent 9.7 Update Software
9.4

9.3 SNMP Agent
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select desired values and click **Save / Apply** to configure SNMP options.

TR-069 Client 9.88 Reboot

9.1 Settings

This includes ackup Settings, Update Settings, and Restore Default screens.

9.1.1 Backup Settings

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

9.1.2 Update Settings

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

9.1.3 Restore Default

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

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

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

NOTE:	This entry has the same effect as the **Reset** button. The CT-5364A board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

9.2 System Log

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

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

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

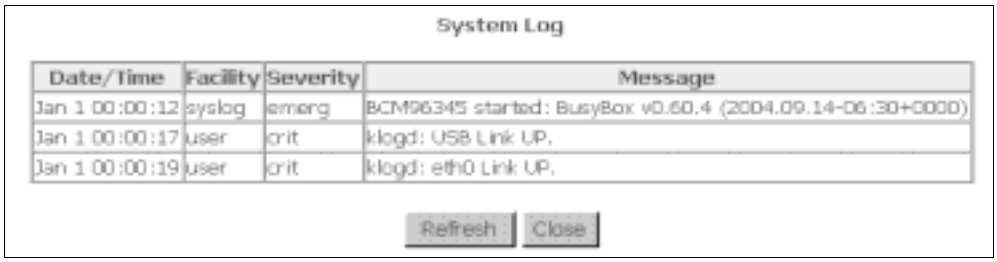
STEP 2: Select desired options and click **Apply / Save**.

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

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

Option	Description
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5364A SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. y default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or oth mode is configured, the WE UI will prompt the user to enter the Server IP address and Server UDP port.

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



9.3 SNMP Agent

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

9.4 TR-069 Client

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

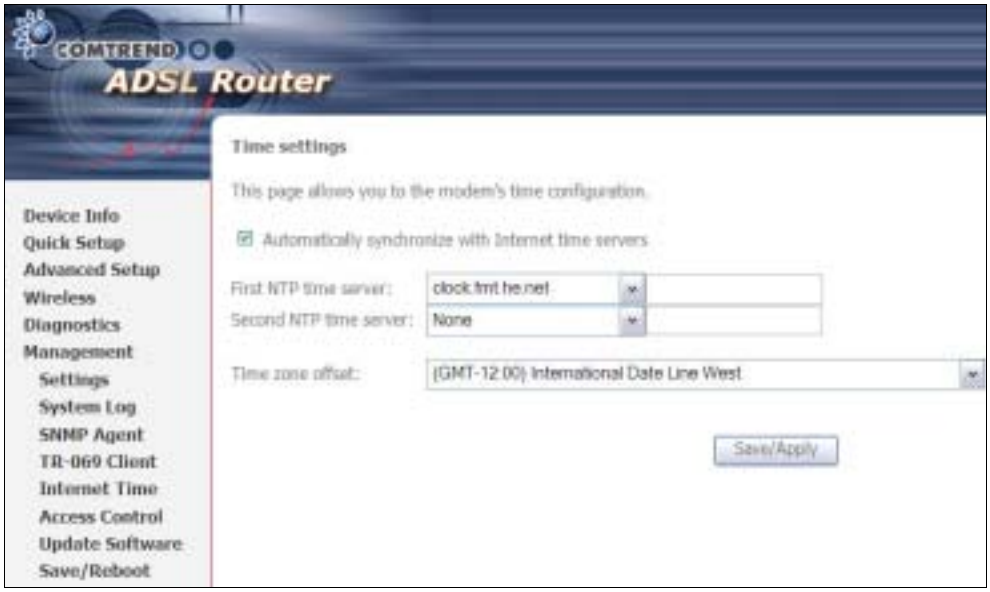
The table below is provided for ease of reference.

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

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

9.5 Internet Time

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



NOTE: Internet Time must be activated to use Parental Control (page 62). In addition, this menu item is not displayed when in ridge mode since the router would not be able to connect to the NTP timeserver.

格式化: 醒目提示

9.6 Access Control

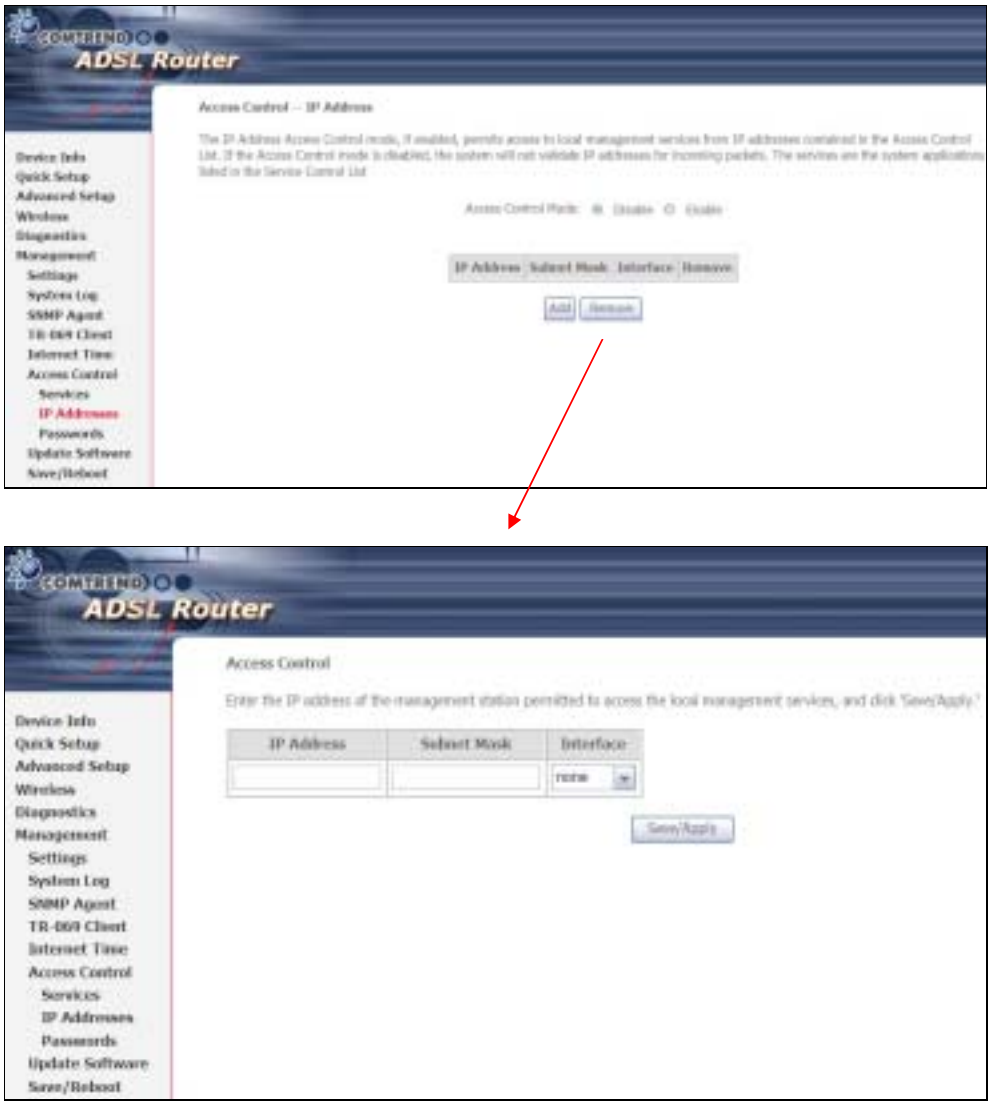
The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.

9.6.1 Services

The Services option limits or opens the access services over the LAN or WAN. These services are provided FTP, HTTP, ICMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click Save/Apply.

9.6.2 IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. efore you enable it, configure the IP addresses by clicking the `Add` button. Enter the IP address and click `Apply` to allow the PC with this IP address managing the DSL Router.



9.6.3 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5364A is controlled through the following three user accounts:

- **root** - has unrestricted access to change and view the configuration.
- **support** - is used for remote maintenance and diagnostics of the router
- **user** - has limited access. This account can view configuration settings and statistics, as well as, update the router firmware.

Use the fields below to change password settings. Click **Save / Apply** to continue.

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

9.7 Update Software

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

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

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

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

NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Quick Setup

After login, the **Quick Setup** screen will appear as shown.

NOTE:	The selections available on the main menu are based upon the configured connection type and user account privileges.

The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.

NOTE:	Up to sixteen PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

9.8 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

STEP 1: Select **Quick Setup** to display this screen.

STEP 2: Click **Next** to start the setup process. Follow the online instructions to complete the settings. This procedure will skip some processes such as the PVC index and encapsulation mode selection.

STEP 3: After the settings are complete, you can use the ADSL service.

9.9 Manual Quick Setup

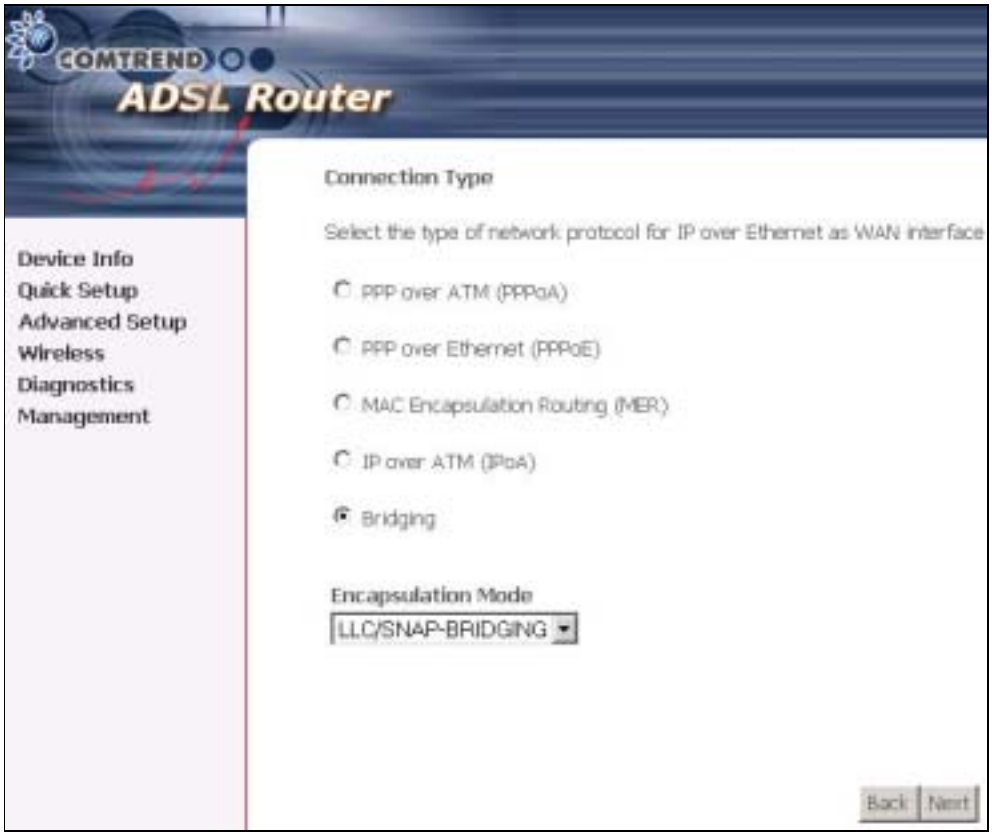
STEP 1: Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.

STEP 2: Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) values. Select Enable Quality Of Service if required and click **Next**.

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

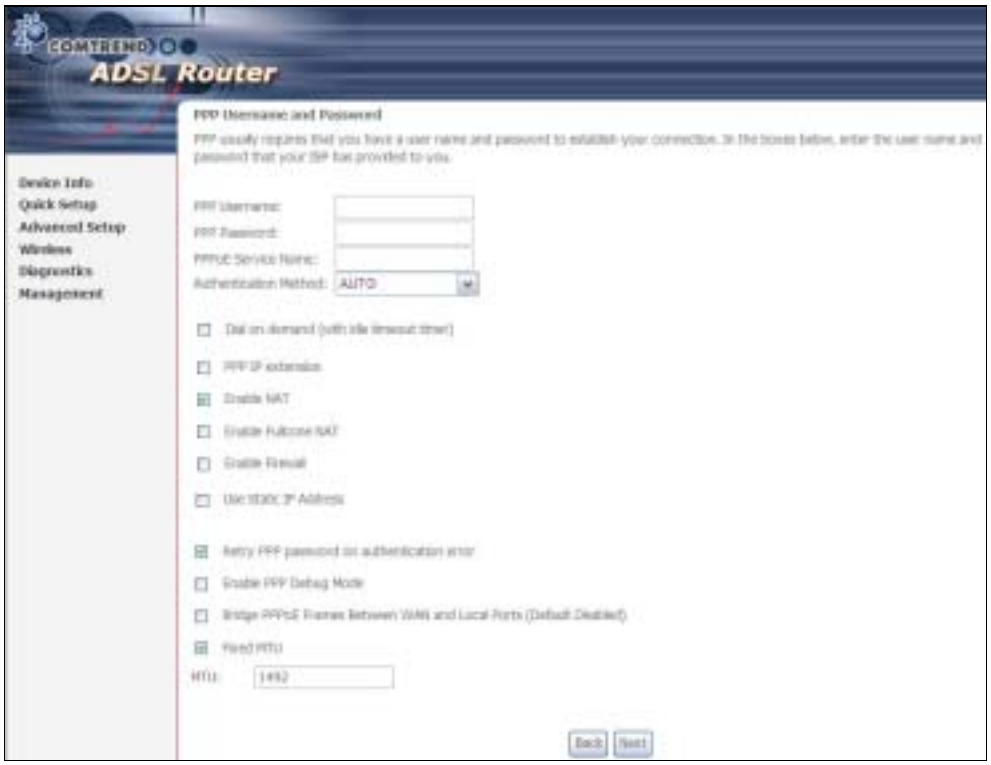
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP RIDGING, VC/MUX
- MER- LLC/SNAP- RIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX



NOTE:	Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

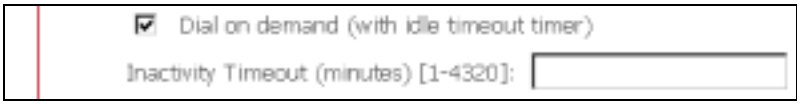


PPP Username/PPP Password: The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.



PPP IP Extension
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, 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.
- 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 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: 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.

Use Static IP Address
Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address.

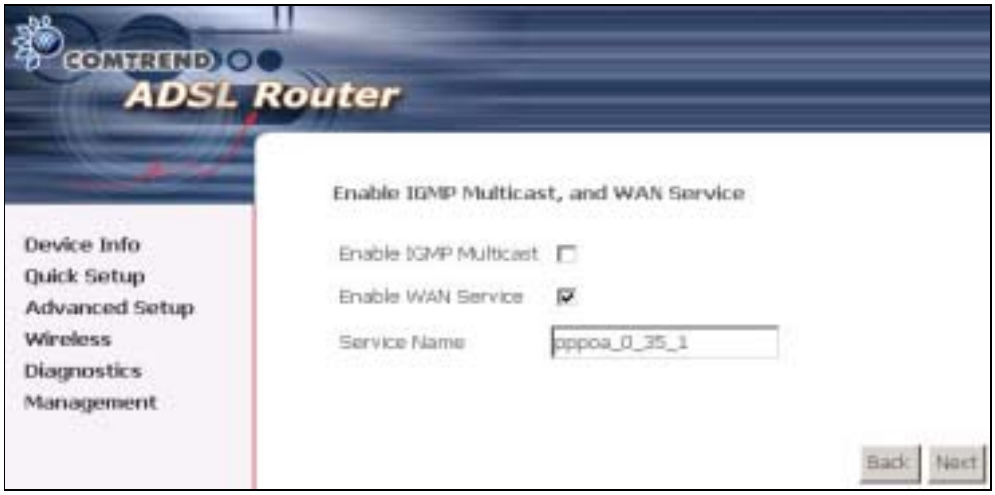
Retry PPP password on authentication error
Tick the box to select.

Enable PPP Debug Mode
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports
If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU
Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click **Next** to display the following screen.



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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

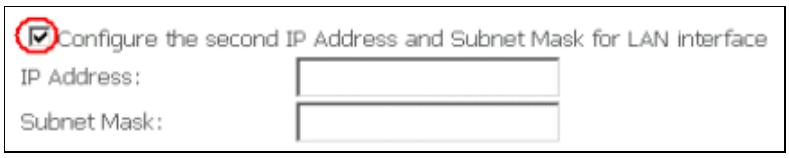
STEP 6: After entering your settings, select **Next**. The following screen appears.

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 and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

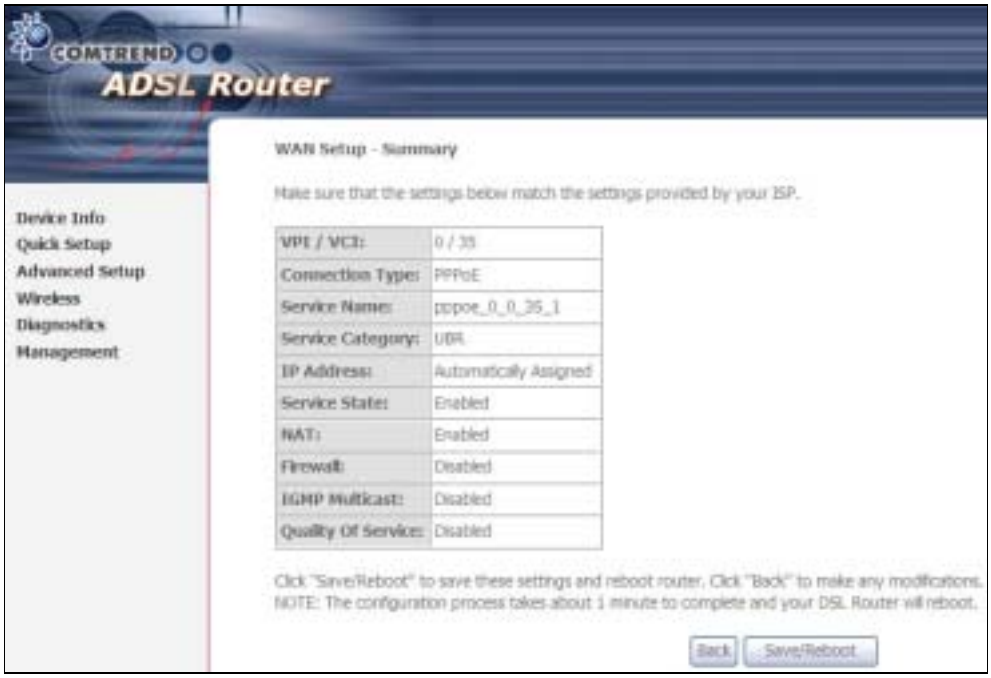
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

9.9.2 MAC Encapsulation Routing (MER)

Step 4: Select the MAC Encapsulation Routing (MER) radio button and click **Next**.

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

NOTE:	DHCP can be enabled for PVC in MER mode 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. Your ISP should provide the values to be entered in these fields.

Step 5: Click **Next** to display the following screen.

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.

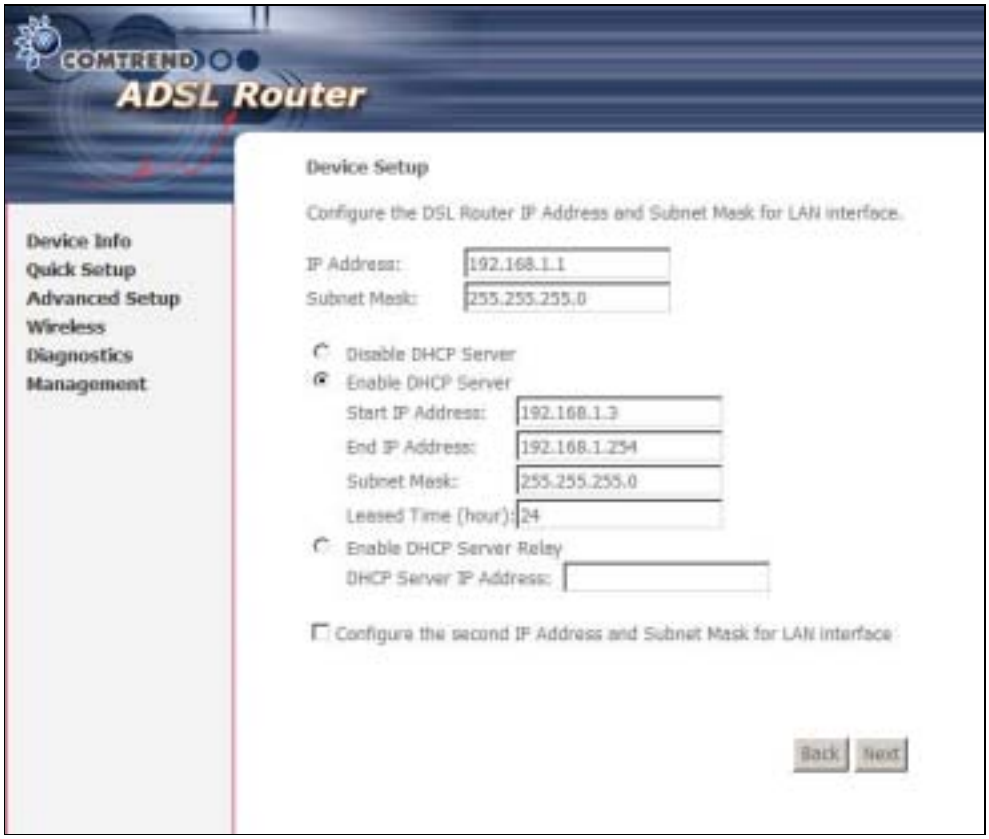
Enable Firewall
If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

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

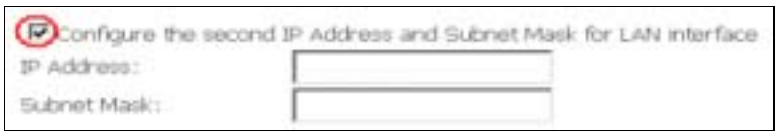


The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

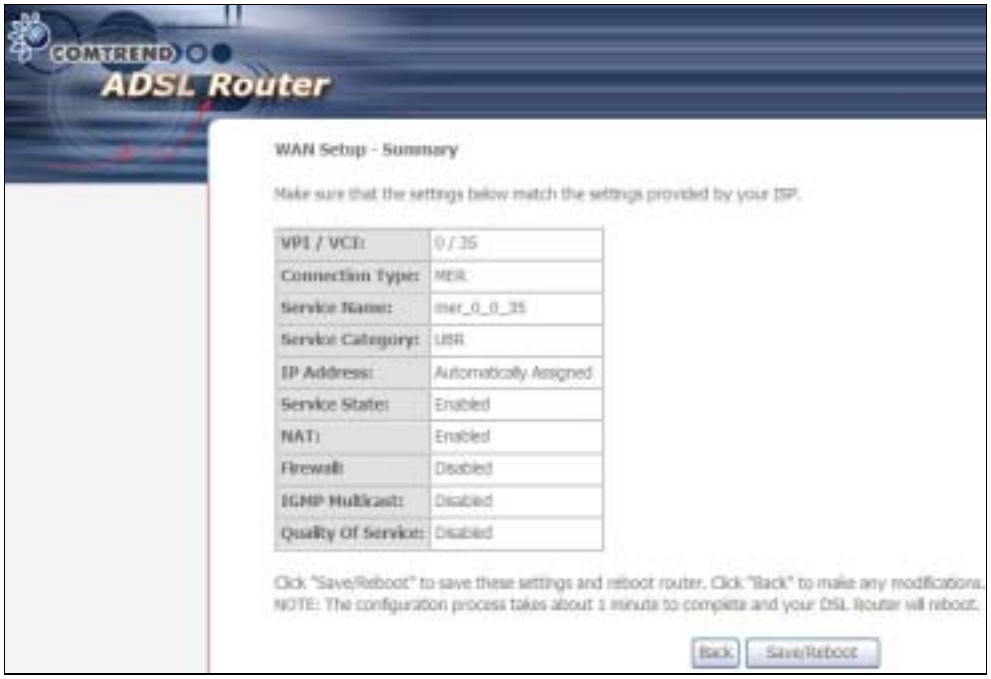
If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

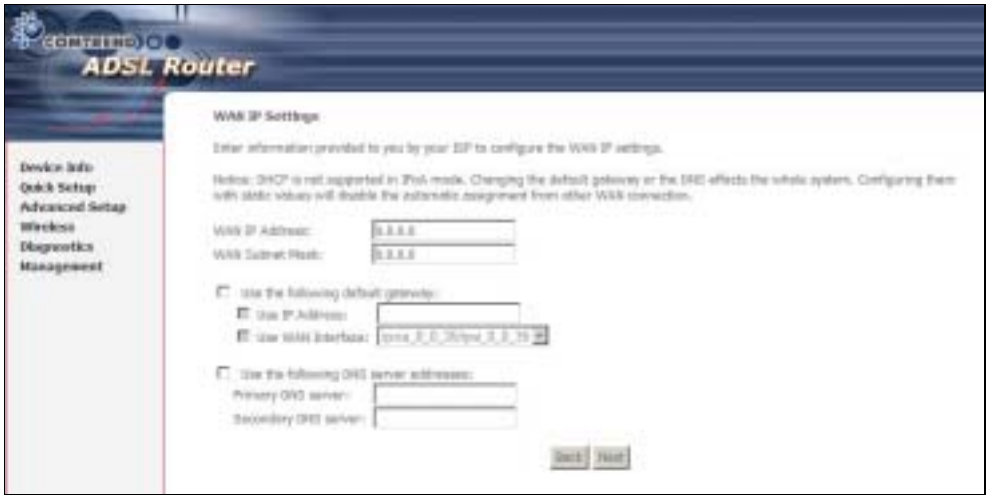
Click **Next** to display the final setup screen.



Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

9.9.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.



NOTE:	DHCP is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup and the DNS server addresses provided by their ISP.

Step 5: Click **Next** to display the following screen.

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

Enable WAN Service:
Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

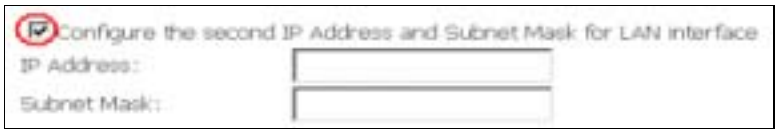
Step 6: Click **Next** to display the following screen.

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 and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from the remote DHCP server. The remote DHCP server will provide the IP address.

To configure a secondary IP address for the LAN port, click the checkbox shown.



STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.

Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

9.9.4 Bridging

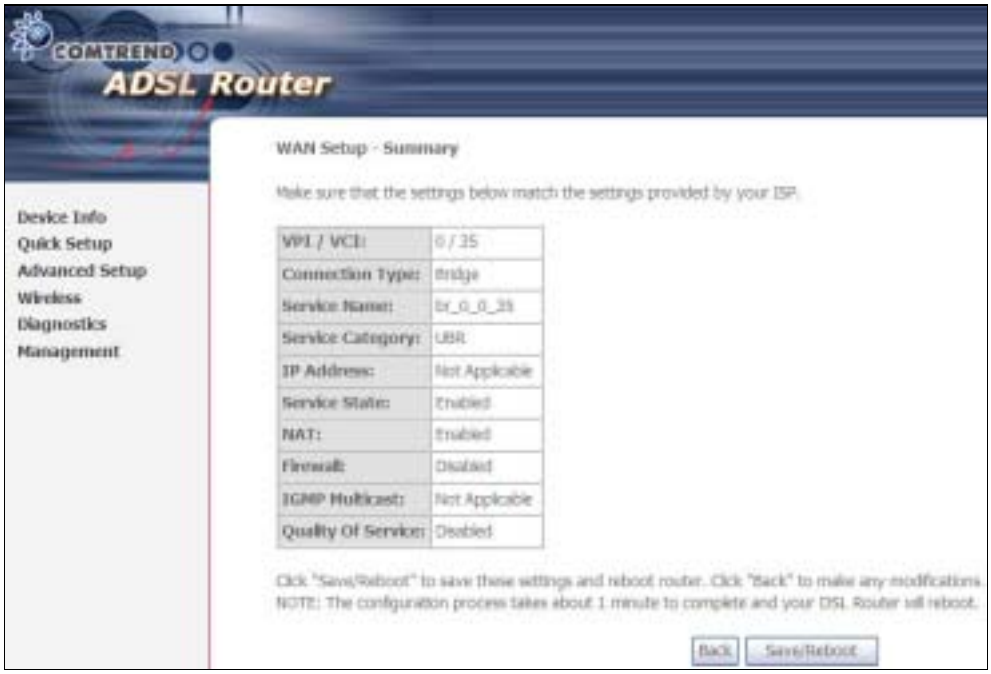
Step 4: Select the ridging radio button and click **Next**. The following screen appears. Select **Enable Bridge Service** and click **Next**.

Step 5: On this screen, you can change the LAN IP address of the router.

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

Click **Next** to display the final setup screen.



Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click **Back** to modify these settings. To apply these settings, click **Save/Reboot**. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the **Device Info** screen.

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

9.10 Reboot

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

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

Appendix A - Firewall

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

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

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

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

Example 1:	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source IP address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA

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

Example 2:	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source IP Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. IP Address	: 172.16.13.4
	Dest. Subnet Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

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

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

Example 1:

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

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

Example 2:

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

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

MAC LAYER FILTER

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

Example 1:

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

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

Example 2:

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

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

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the CT-5364A, as per chosen days of the week and the chosen times.

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

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

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

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

Appendix C - Specifications

Hardware Interface

RJ-11 X 1 for ADSL, RJ-45 X 1 for ETH WAN, RJ-45 X 4 for LAN, US Host, Power Switch X 1, Reset utton X 1, WPS X 1, Wi-Fi Antenna X 2

WAN Interface

ADSL 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

LAN Interface

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

WLAN Interface

Standard ..... IEEE 802.11n (IEEE 802.11b/g compatible)
Encryption ..... 64/128-bit Wired Equivalent Privacy (WEP)
Channels ..... 11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate ..... Up to 270Mbps
WPA/WPA2 ..... Yes
IEEE 802.1x..... Yes
WDS ..... Yes
WMM ..... Yes
WPS ..... Yes
MAC Filtering ..... Yes
Optional ..... Afterburner mode (Turbo mode)***

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) bridge/route; RFC 2516 (PPPoE); RFC 1577 (IPoA)
Support PVCs..... 16
AAL type AAL5
ATM service class ..... U R/C R/V R
ATM UNI support UNI3.1/4.0
OAM F4/F5 ..... Yes

Management

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

Networking Protocols

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

Security Functions

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

Application Passthrough

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

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

Power Supply ..... Input: 220 - 230 Vac
Output: 15 Vdc / 0.8 A

Environment Condition

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

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

Kit Weight

(1*CT-5364A, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 0.9 kg

Certifications..... CE, FCC

NOTE: Specifications are subject to change without notice

Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

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

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

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

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

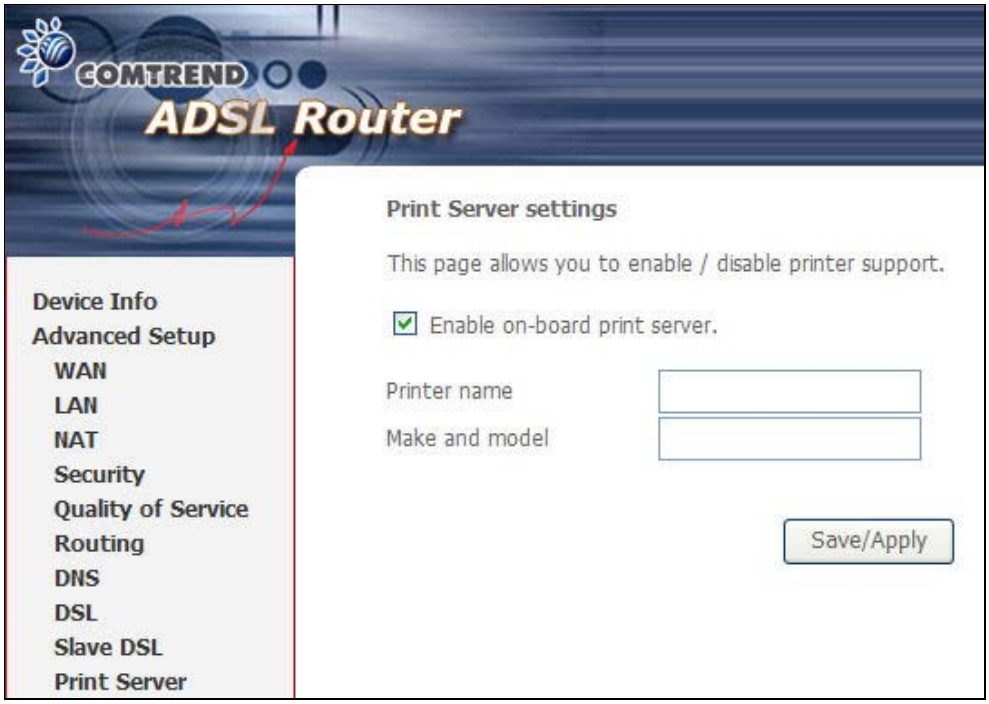
NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix E - Printer Server

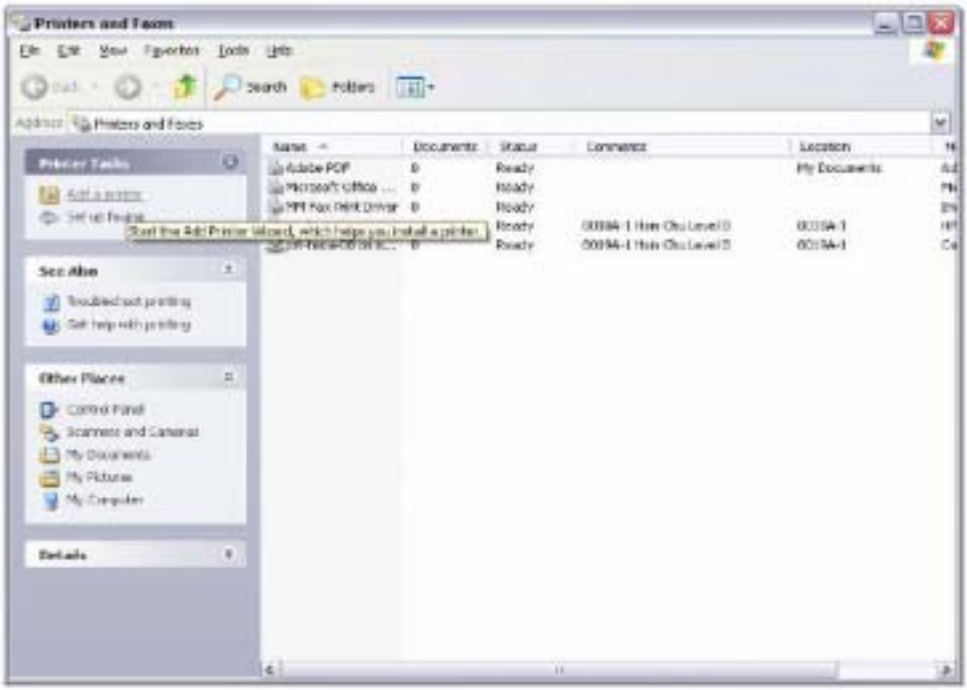
These steps explain the procedure for enabling the Printer Server.

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

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



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



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

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

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

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

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

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

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

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

STEP 10: Click Finish.

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