COMTREND CORPORATION

CT-5372
Multi-DSL Router
User's Manual

Version A1.0, August 15, 2006

261074-001

⚠ Warning

- Before servicing or disassembling this equipment, always disconnect all power and telephone lines from the device.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix D - Specifications.

Preface

This manual provides information to network administrators. It covers the installation, operation and applications of the wireless ADSL2+ router.

The reader reading this manual is presumed to have a basic understanding of telecommunications. For product update, new product release, manual revision, software upgrade, technical support, etc., visit Comtrend Corporation at http://www.comtrend.com

This document is subject to change without notice.

Copyright

Technical support

When you find the product out of service, or that it doesn't work properly, please contact technical support engineer for immediate servicing or email to INT-support@comtrend.com

Table of Contents

Chapter 1 Introduction

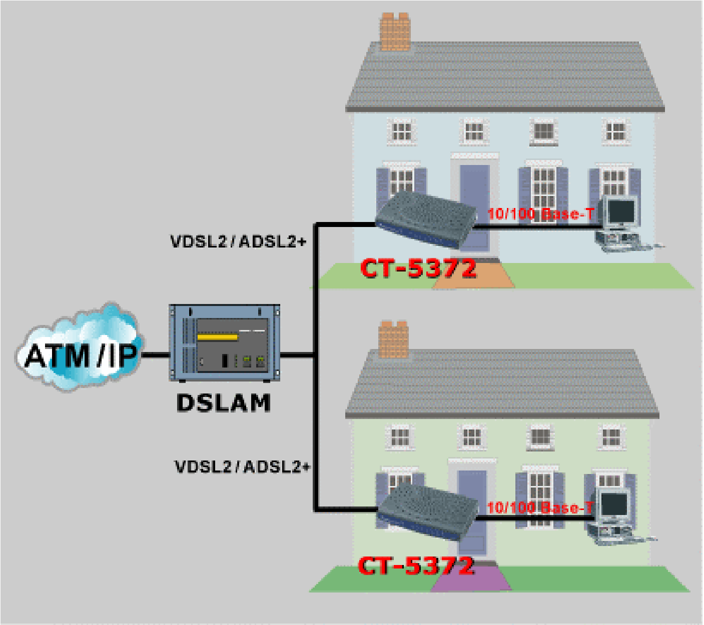
The CT-5372 is a leading Multi-DSL wireless router that can support both ADSL2+ and VDSL2. VDSL2 is a brand new standard and technology that is perfectly suitable for triple play (video, voice and data) applications.

1.1 Features

- Supports both ADSL2+ and VDSL2
- Automatically switches to ADSL2+ or VDSL2 according to the port setting of DSLAM
- Wi-Fi Certified (optional)
- UPnP
- Integrated 802.11g AP (optional)
- WPA and 802.1x
- RADIUS client
- IP /MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- IP QoS
- NAT/PAT
- IGMP Proxy and fast leave
- DHCP Server/Relay/Client
- DNS Proxy
- Auto PVC configuration
- Per-VC packet level QoS
- Up to 8 VCs
- Embedded SNMP agent
- Web-based management
- Remote configuration and upgrade
- Supports TR-069
- Configuration backup and restoration
- FTP server
- TFTP server

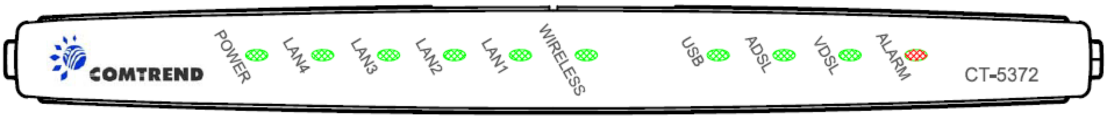
1.2 Application

The following diagram depicts the application of the CT-5372.



1.3 Front Panel LED Indicators

The front panel LEDs are shown in the picture below, followed by an explanation in the table below.

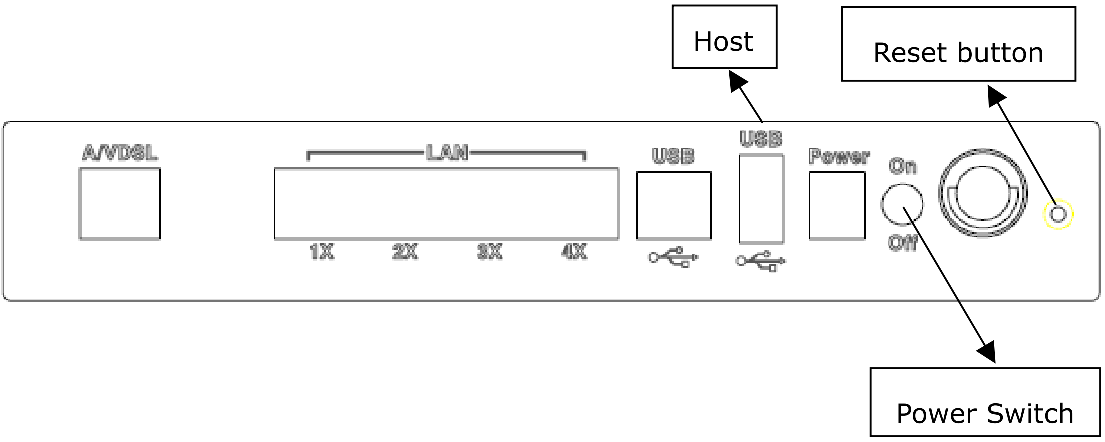


LED	Color	Mode	Function
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
LAN 4X~1X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.
WIRELESS	Green	On	The Wireless is ready and idle.
		Off	The Wireless is not installed.
	Green	Blink	Data transmitting or receiving over Wireless.
USB	Green	On	A USB link is established.
		Off	A USB link is established.
	Green	Blink	Data transmitting or receiving over USB.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
	Green	Blink	The ADSL link is training or some traffic is passing through ADSL.
VDSL	Green	On	The VDSL link is established.
		Off	The VDSL link is not established.
	Green	Blink	The VDSL link is training or some traffic is passing through VDSL.
ALARM	Red	On	The A/VDSL link is terminated.
		Off	Normal operating status.

Chapter 2 Installation

2.1 Hardware Installation

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for at least 5 seconds.



Follow the instructions below to complete the hardware connections.

Connection to LINE port

If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ11 connection cable.

Connection to LAN port

To connect to a hub or PC, use a RJ45 cable. You can connect the router to up to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to USB port

Connect the USB port to a PC with a standard USB cable.

Connection to USB host port

The CT-5372 is equipped with one high-speed USB2.0 host connection.

With software support, users can connect USB devices such as printers and a hard disc to the CT-5372. For this software release, printer server is supported.

Connection to Power

Connect the **Power** jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source.

After all connections have been made, press the power-switch in to turn the device on. After power on, the router performs a self-test. Wait for a few seconds until the test is finished, then the router will be ready to operate.

Caution 1: If the router fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

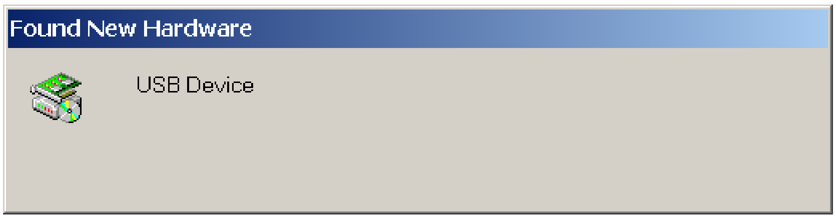
Caution 2: Before servicing or disassembling this equipment, always disconnect all power cords and telephone lines from the wall outlet.

2.2 Installing the USB Device Driver

Before you connect your router's USB cable to your PC, you must load the ADSL USB drivers. The USB driver supports Windows 98, ME, 2000, and XP.

To connect the router to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below:

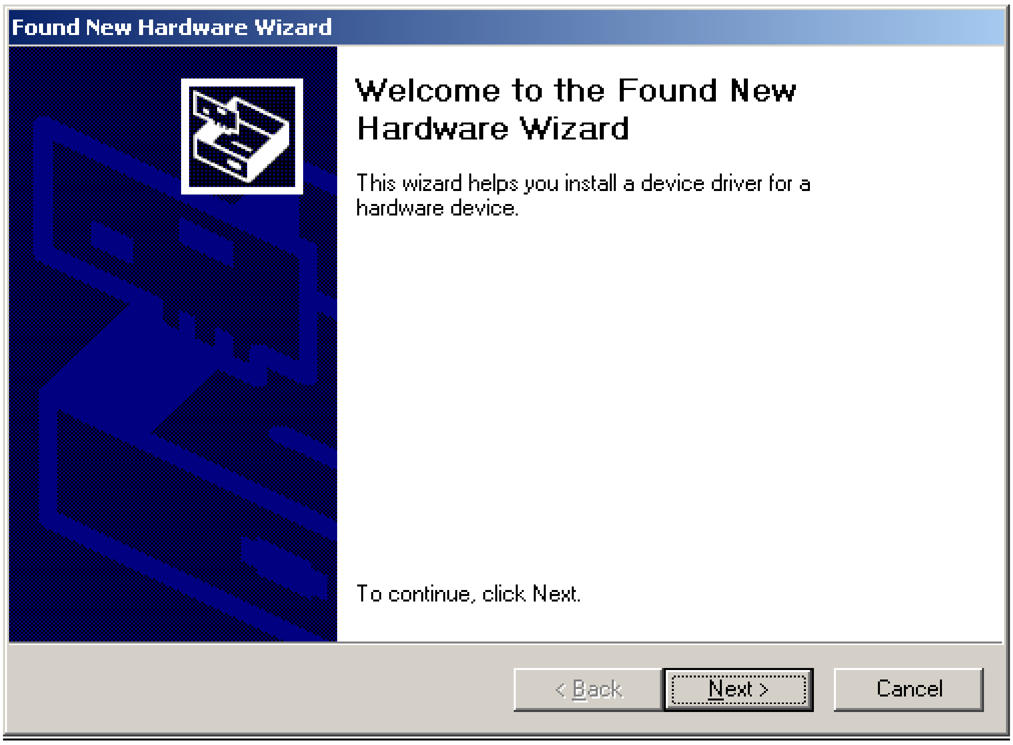
STEP 1: Connect the USB router to the PC by plugging the flat connector of a standard USB cable into your PC, and plugging the square connector into the router. The screen will display as below:



Found New Hardware

USB Device

STEP 2: When the screen displays as below, click the **Next** button.



Found New Hardware Wizard

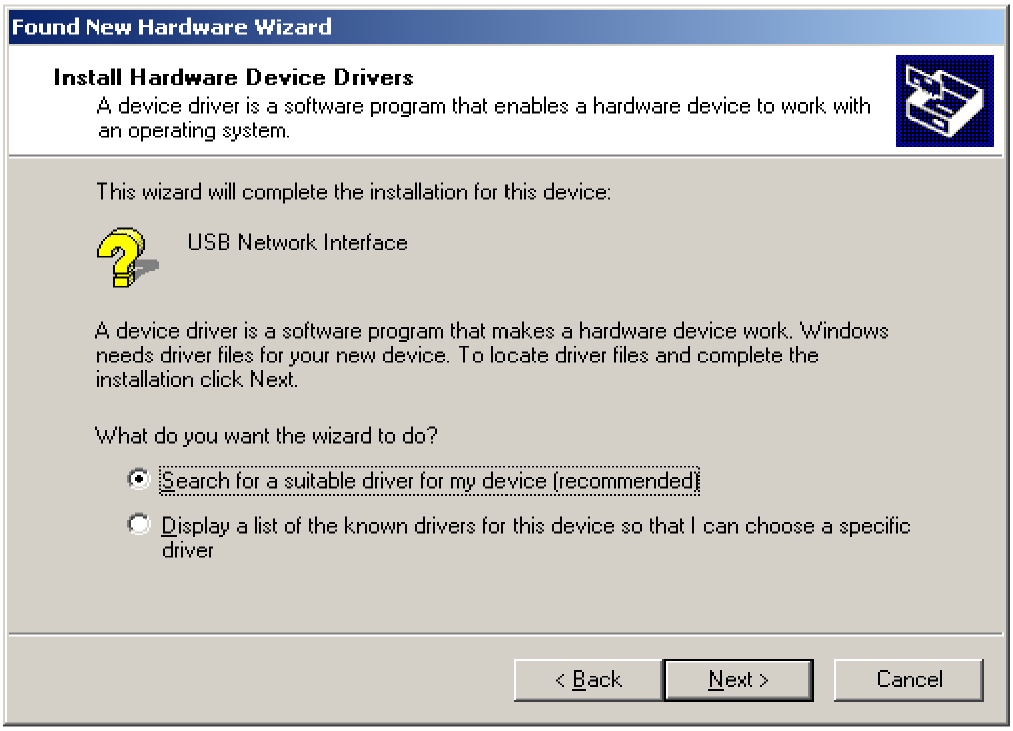
Welcome to the Found New Hardware Wizard

This wizard helps you install a device driver for a hardware device.

To continue, click Next.

Note: This screen won't be displayed if the USB Driver has been previously un/installed.

STEP 3: When the screen displays as below, select **Search for a suitable driver** and click the **Next** button.



Found New Hardware Wizard

Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard will complete the installation for this device:

USB Network Interface

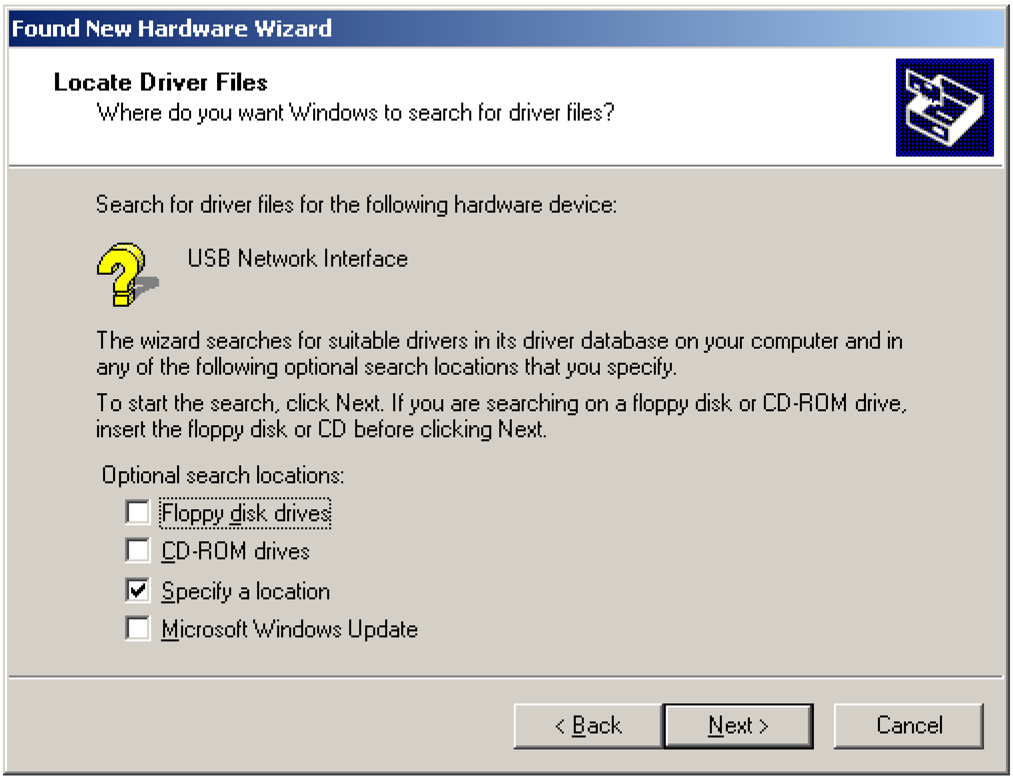
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

STEP 4: Select Specify a location and click the Next button. If you are installing the software from a disk, insert the disk.



Found New Hardware Wizard

Locate Driver Files

Where do you want Windows to search for driver files?

Search for driver files for the following hardware device:

USB Network Interface

The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.

To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.

Optional search locations:

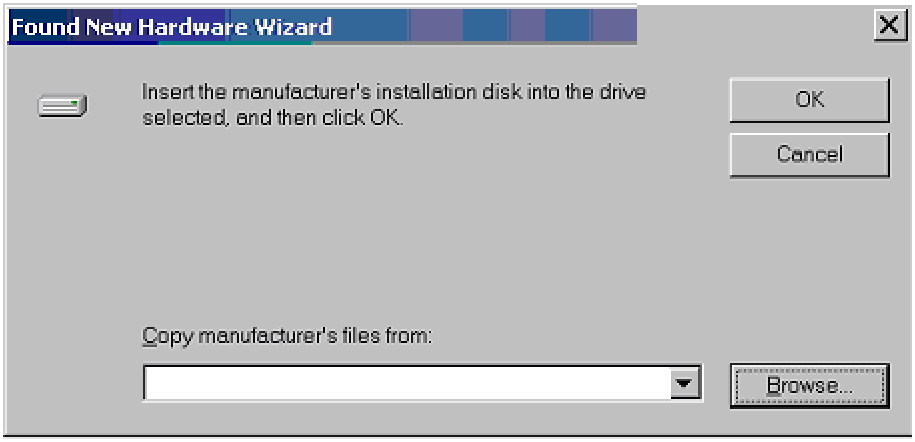
□ Floppy disk drives

□ CD-ROM drives

☑ Specify a location

□ Microsoft Windows Update

STEP 5: Select the location of the file using the **Browse** button. Normally, the file is on the CD-ROM shipped with the device.

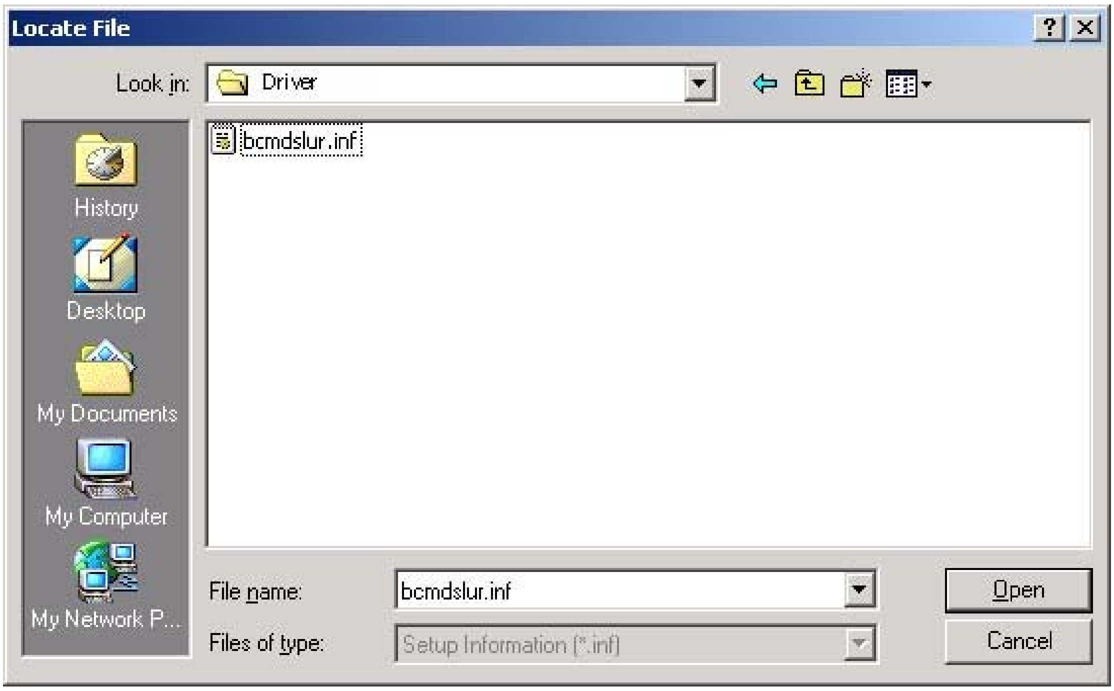


Found New Hardware Wizard

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from:

STEP 6: Locate the file, and click the **Open** button.



Locate File

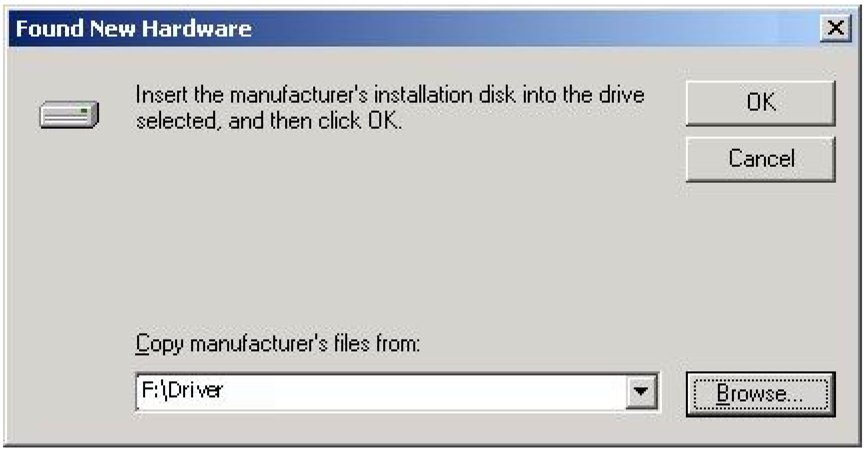
Look in: Driver

bcmdslur.inf

File name: bcmdslur.inf

Files of type: Setup Information (*.inf)

STEP 7: When the screen displays as below, click the **OK** button.



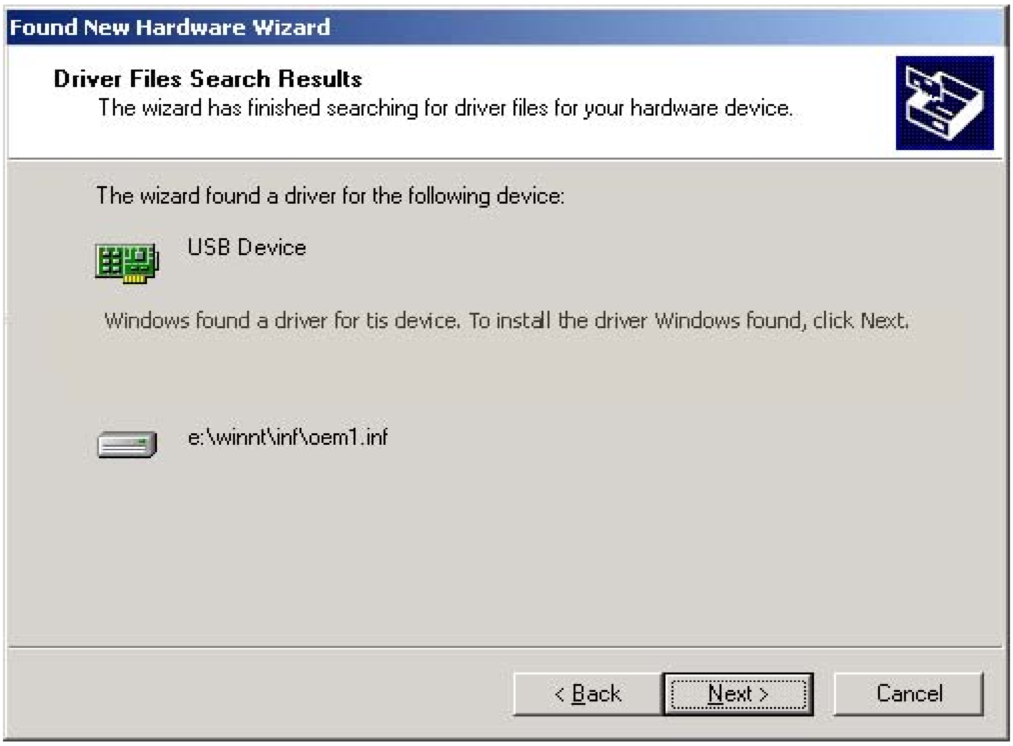
Found New Hardware

Insert the manufacturer's installation disk into the drive selected, and then click OK.

Copy manufacturer's files from:

F:\Driver

STEP 8: When the screen below displays, click the **NEXT** button.



Found New Hardware Wizard

Driver Files Search Results

The wizard has finished searching for driver files for your hardware device.

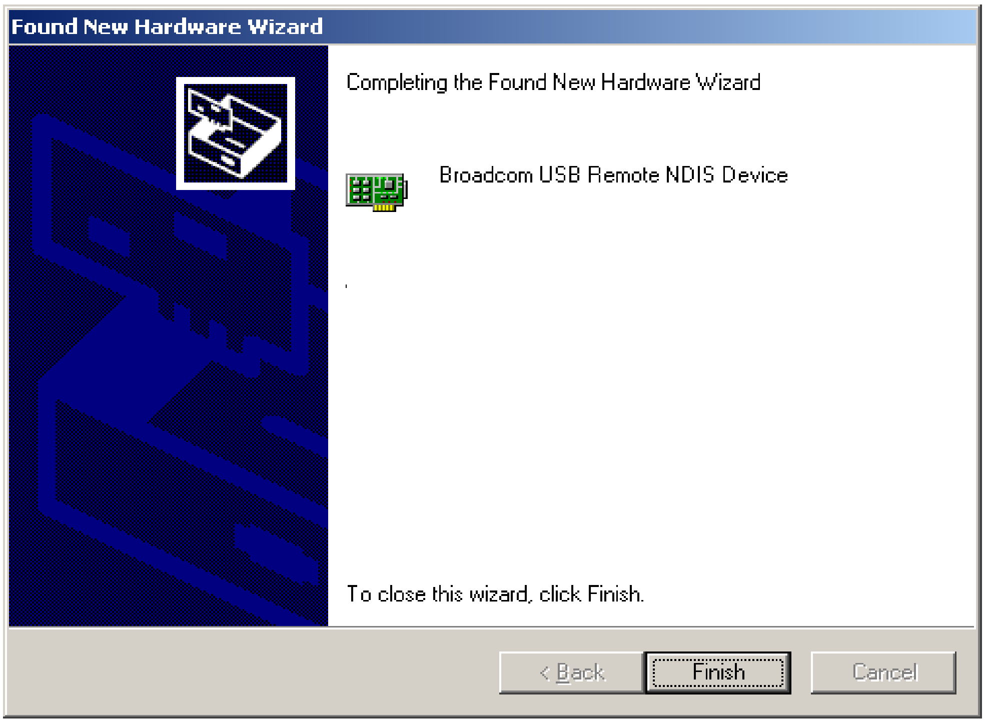
The wizard found a driver for the following device:

USB Device

Windows found a driver for tis device. To install the driver Windows found, click Next.

e:\winnt\inf\oem1.inf

STEP 9: Click the **Finish** button, when the screen displays as below.



Found New Hardware Wizard

Completing the Found New Hardware Wizard

Broadcom USB Remote NDIS Device

To close this wizard, click Finish.

STEP 10: Installation is complete.

Chapter 3 Login via the Web Browser

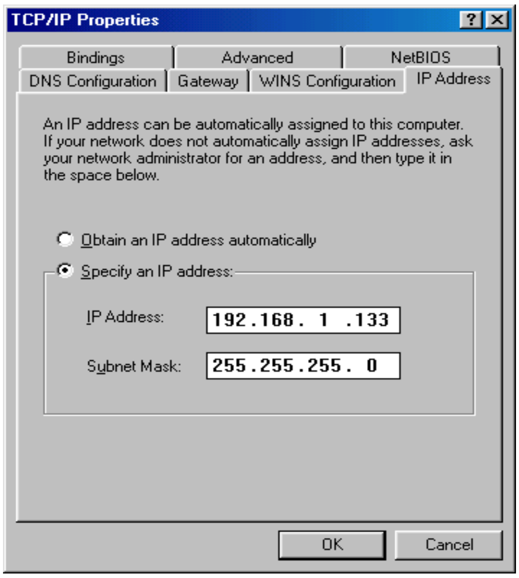
This section describes how to manage the router via a Web browser via the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. (The Web page is best viewed with Microsoft Internet Explorer 5.5 and later): A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

3.1 IP Address

The default IP address of the CT-5372 (LAN port) is 192.168.1.1. To configure the CT-5372 for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

STEP 1: Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

STEP 2: Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168. 1 .133

Subnet Mask: 255.255.255. 0

STEP 3: Click **OK** to submit the settings.

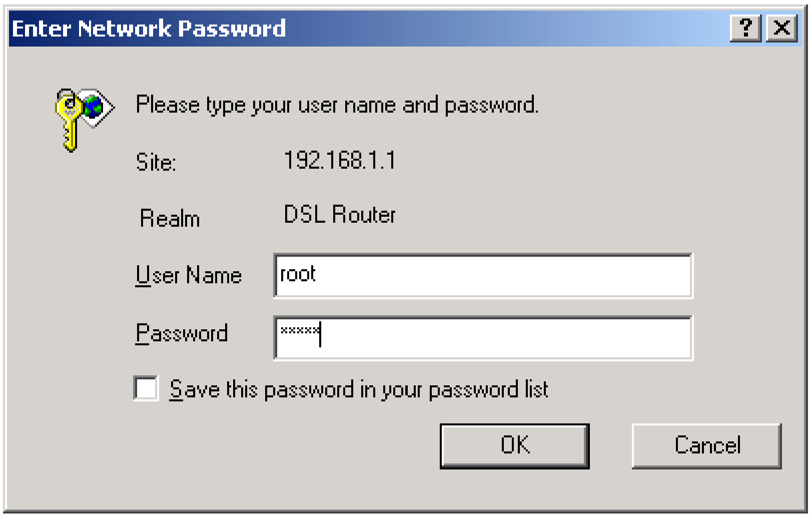
STEP 4: Start your Internet browser and type the IP address for the router (192.168.1.1) in the Web address bar.

3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-5372. To log on to the system from the Web browser, follow the steps below:

STEP 1: Start your Internet browser. Type the IP address for the router in the Web address field. For example, if the IP address is 192.168.1.1, type **http://192.168.1.1**

STEP 2: You will be prompted to enter your user name and password. Type **root** in the user name and **12345** in the password field, and click **OK**. These values can be changed later in the Web User Interface by selecting the **Management** link.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

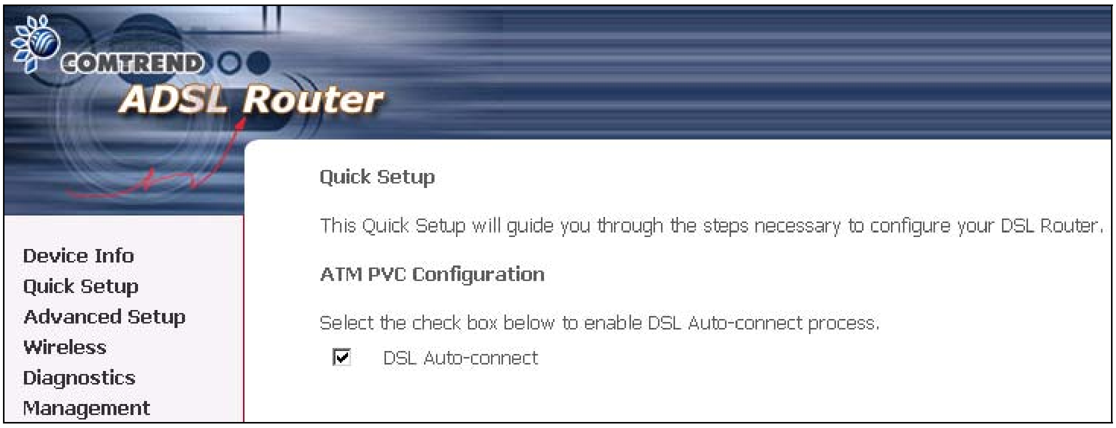
Realm DSL Router

User Name: root

Password: *****

□ Save this password in your password list

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



Quick Setup

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

ATM PVC Configuration

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

☑ DSL Auto-connect

3.3 Default Settings

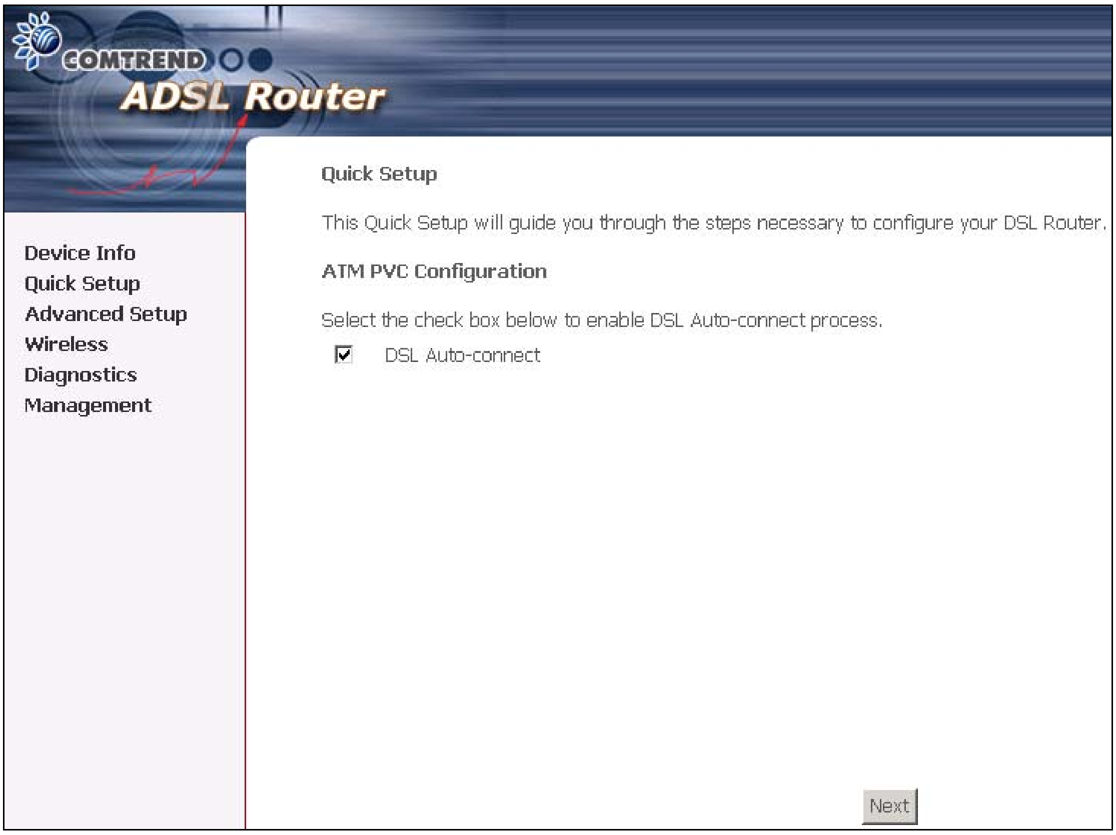
During power on initialization, the CT-5372 initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section on the flash memory. The default attributes are overridden when identical attributes with different values are configured. 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, or by clicking the Restore Default Configuration option in the Restore Settings screen.

The following default settings are present when setting up the router for the first time.

- LAN port IP address: 192.168.1.1
- Local administrator account name: root
- Local administrator account password: 12345
- Local non- administrator account name: user
- Local non- administrator account password: user
- Remote WAN access account name: support
- Remote WAN access account password: support
- DHCP server on LAN interface: enabled
- WAN IP address: none

Chapter 4 Quick Setup

After login, the **Quick Setup** screen appears as shown.



Quick Setup

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

ATM PVC Configuration

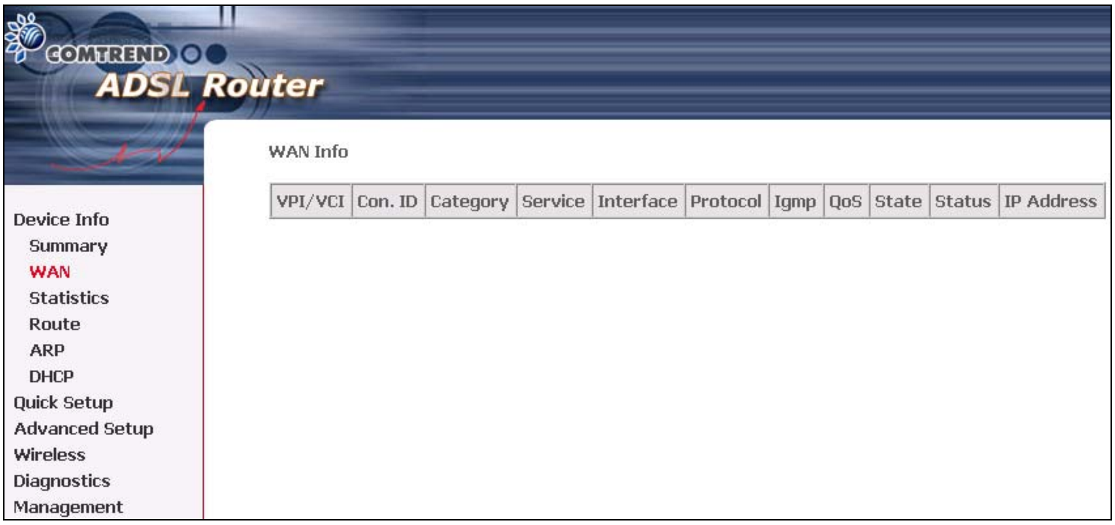
Select the check box below to enable DSL Auto-connect process.

☑ DSL Auto-connect

Note: The selections available on the left side of menu are based upon the configured connection.

4.1 WAN

Click **Device Info** on the menu bar to display the WAN option. Then, click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



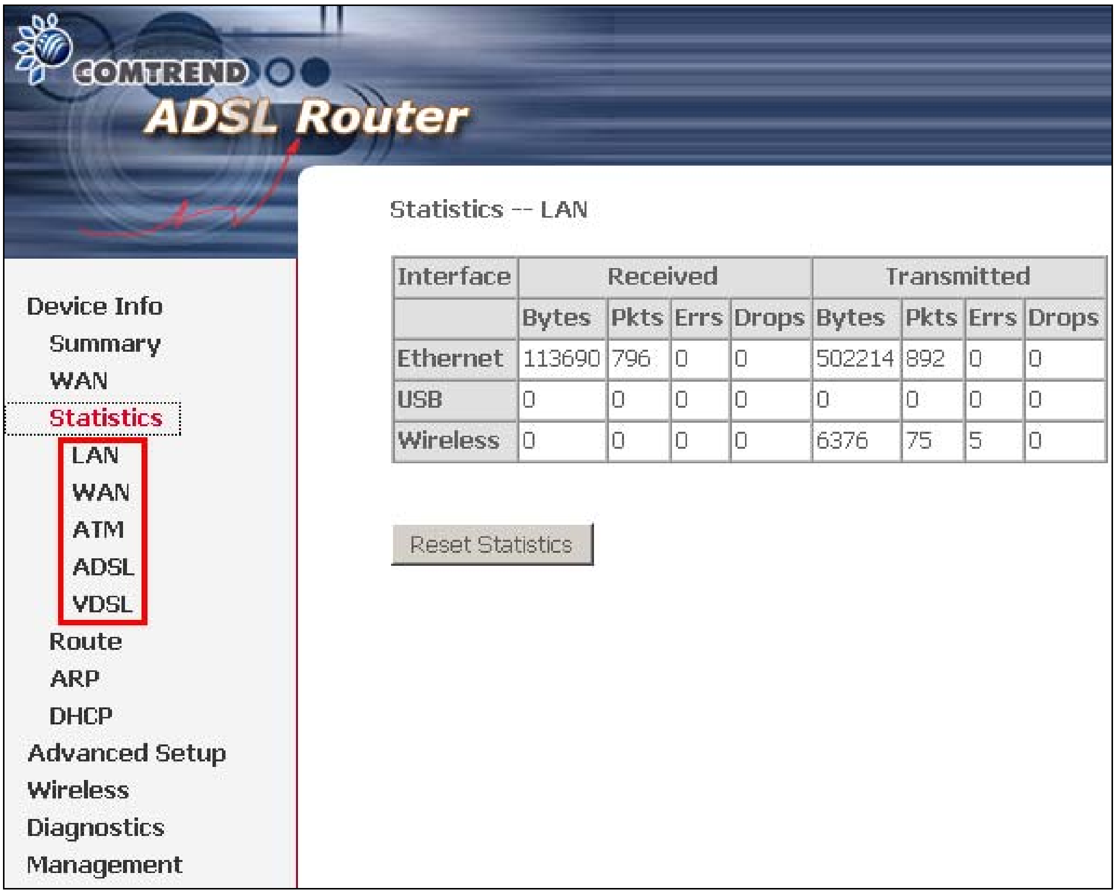
WAN Info

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address

VPI/VCI	Shows the values of the ATM VPI/VCI
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 state of the IGMP function
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

4.2 Statistics

Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM, ADSL and VDSL. All statistics screens are updated every 15 seconds.

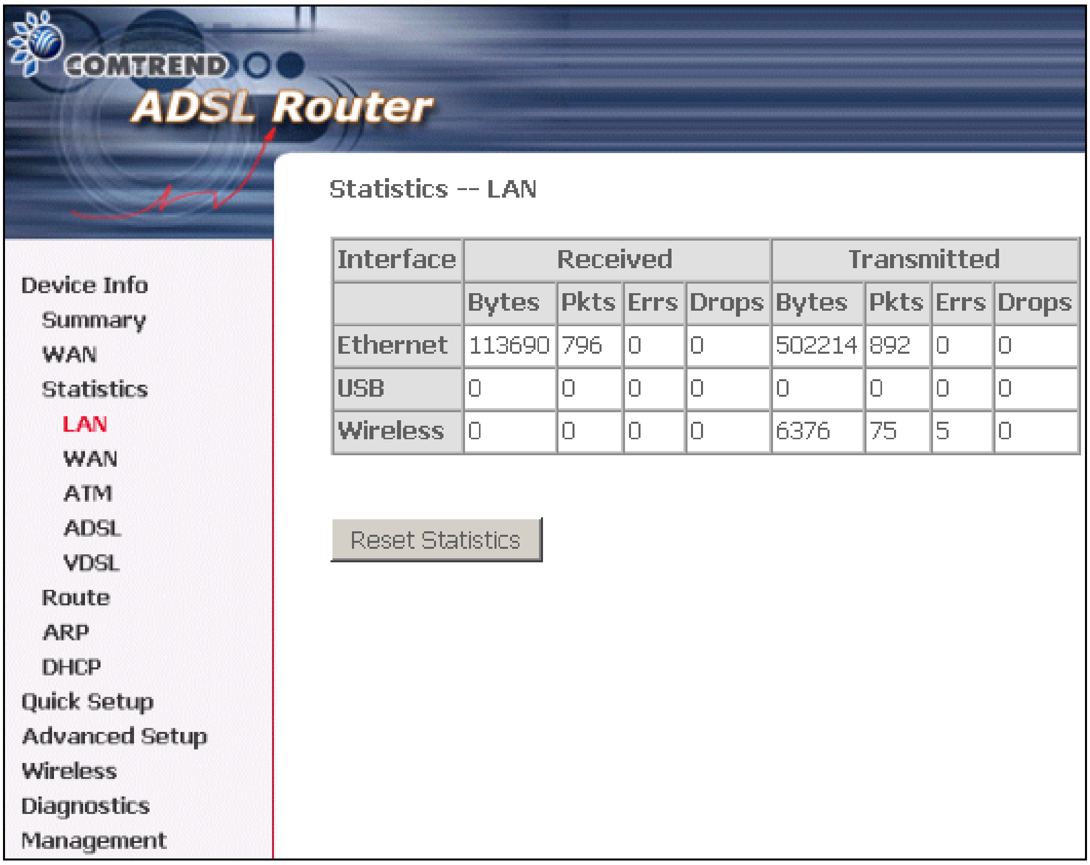


Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	113690	796	0	0	502214	892	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	6376	75	5	0

4.2.1 LAN Statistics

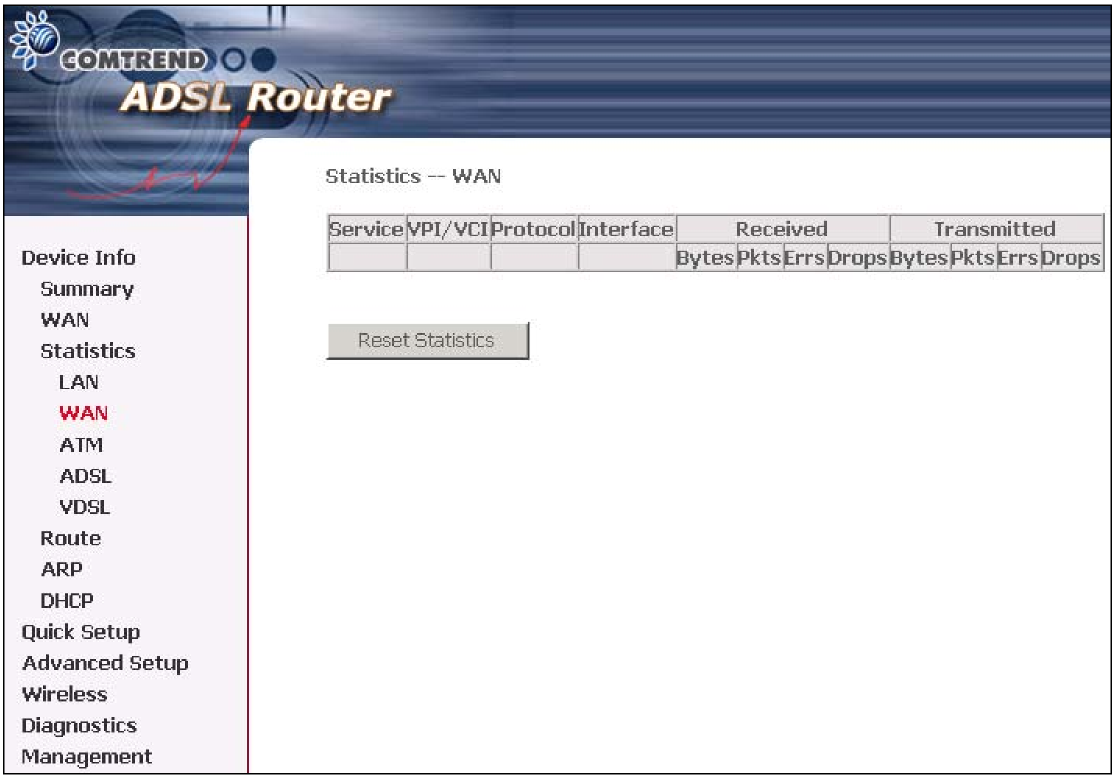
The Network Statistics screen shows the interface statistics for the ATM AAL5 interface, and Ethernet interfaces. (The Network Statistics screen shows the interface statistics for the LAN interface. This provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	113690	796	0	0	502214	892	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	6376	75	5	0

4.2.2 WAN Statistics



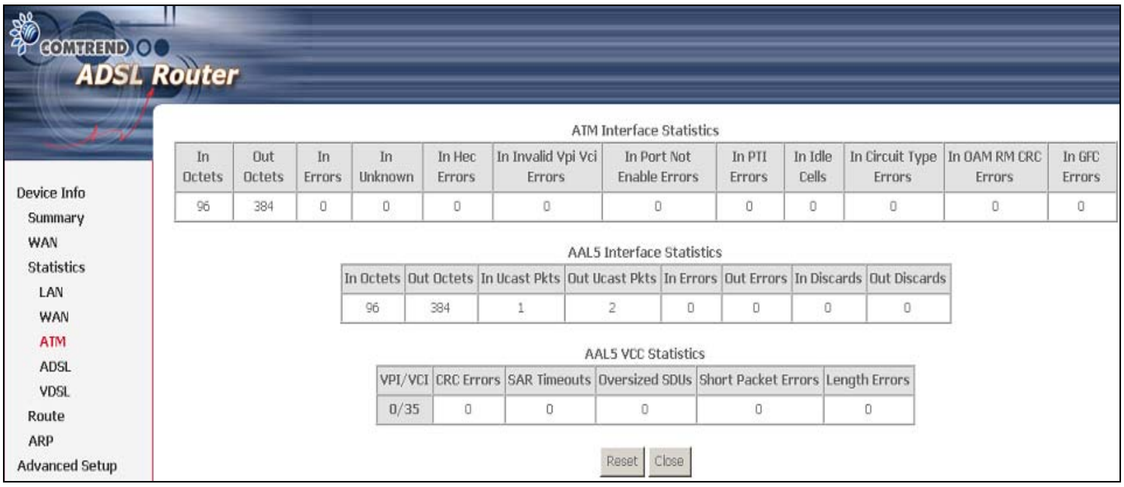
Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

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 - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in Bytes Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) the errored packets Rx/TX (receive/transmit) dropped packets

4.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
96	384	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
96	384	1	2	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0

ATM Interface Statistics

Field	**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 Enabled Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In Oam RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ATM AAL5 Layer Statistics over ADSL interface

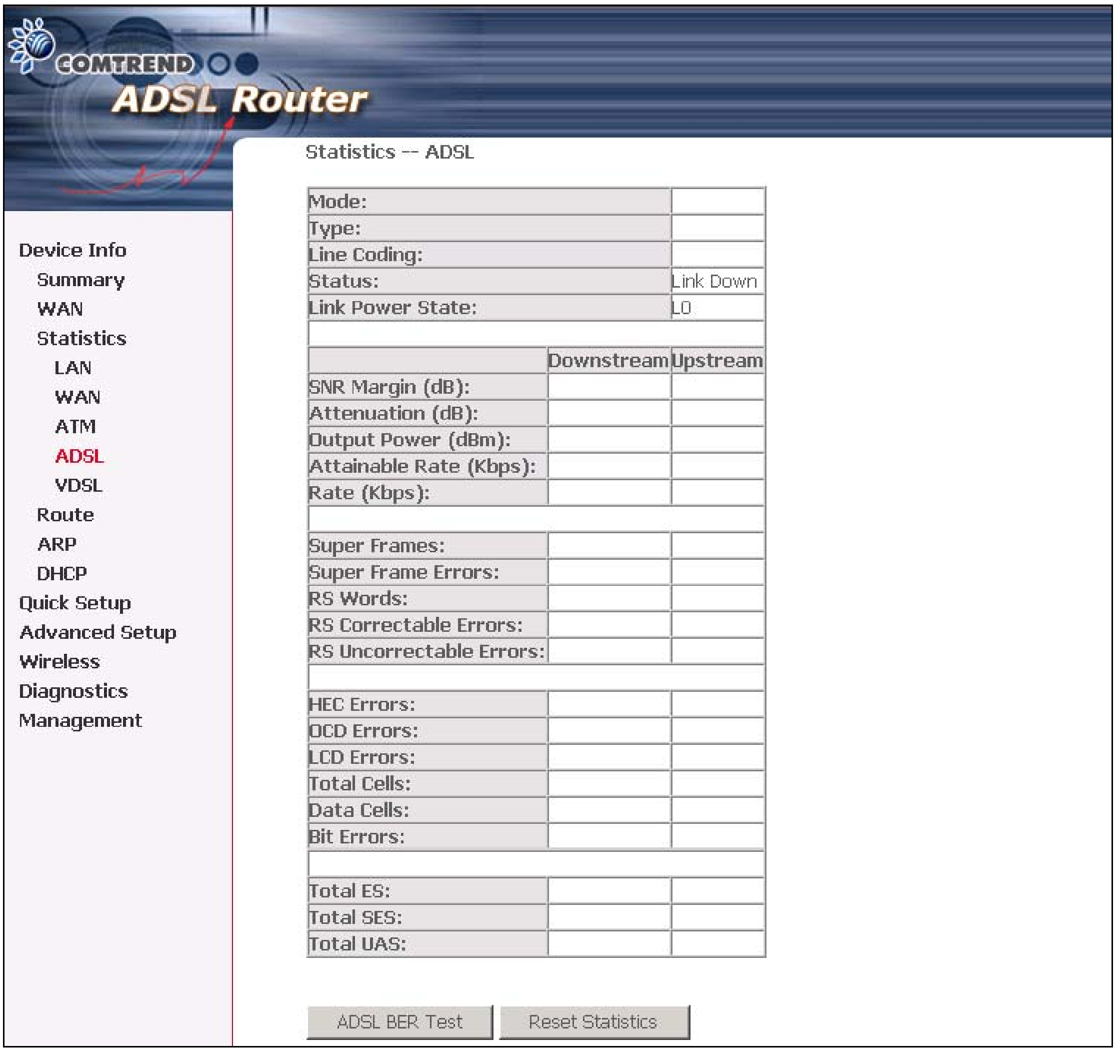
Field	**Description**
In Octets	Number of received AAL5/AAL0 CPCS PDU octets
Out Octets	Number of received AAL5/AAL0 CPCS PDUs octets transmitted
In Ucst Pkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer
Out Ucast Pkts	Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmission
In Errors	Number of received AAL5/AAL0 CPCS PDUs received in error. The types of errors counted include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could be not 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

ATM AAL5 Layer Statistics for each VCC over ADSL interface

Field	**Descriptions**
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets 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

4.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.



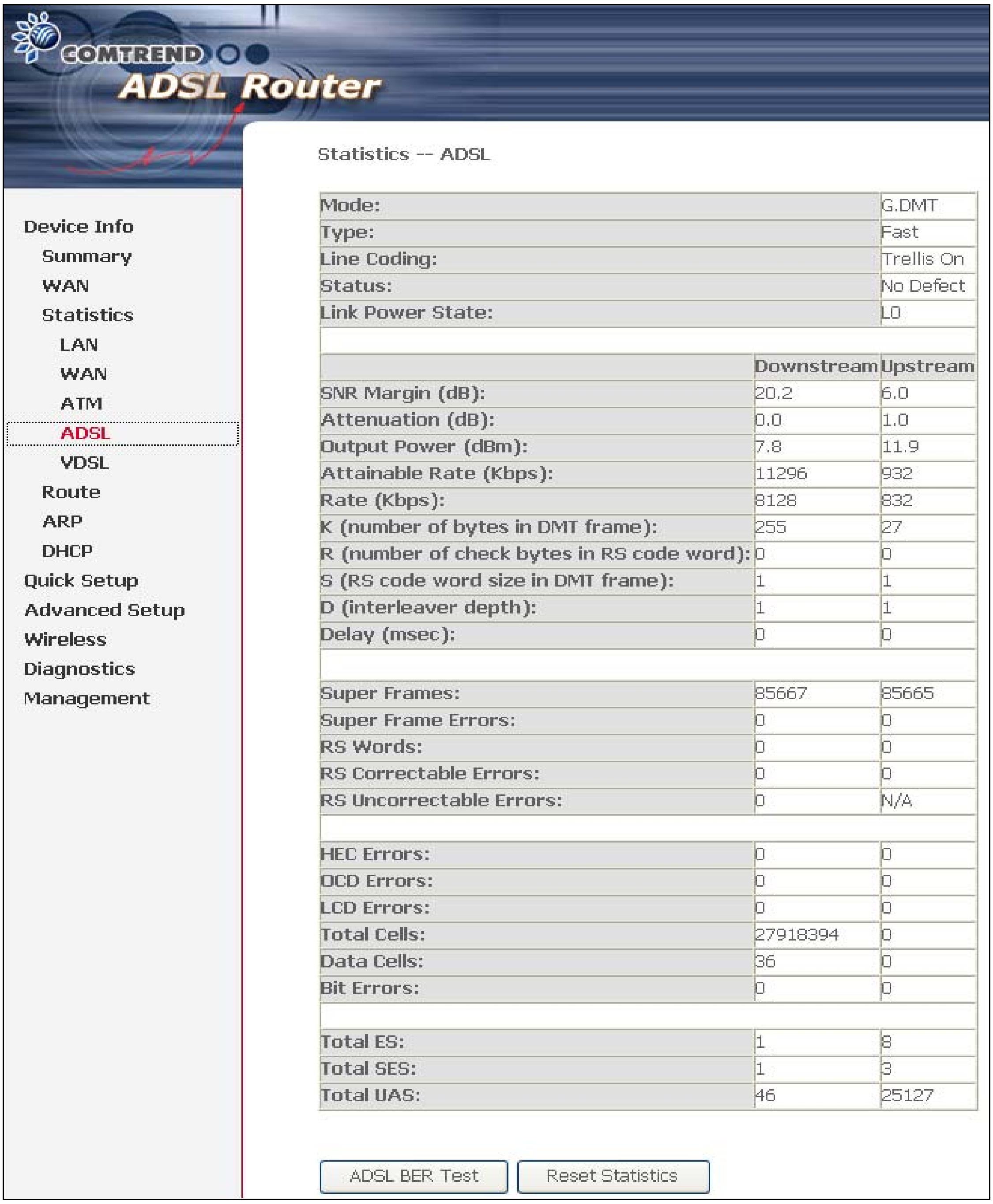
Statistics -- ADSL

Mode:	
Type:	
Line Coding:	
Status:	Link Down
Link Power State:	L0

	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

Field	**Description**
Mode	Modulation protocol ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2
Type	Channel type Interleave or Fast
Line Coding	DMT Trellis on
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
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 ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

If you are connected to an ADSL link the following page will be displayed.



Statistics -- ADSL

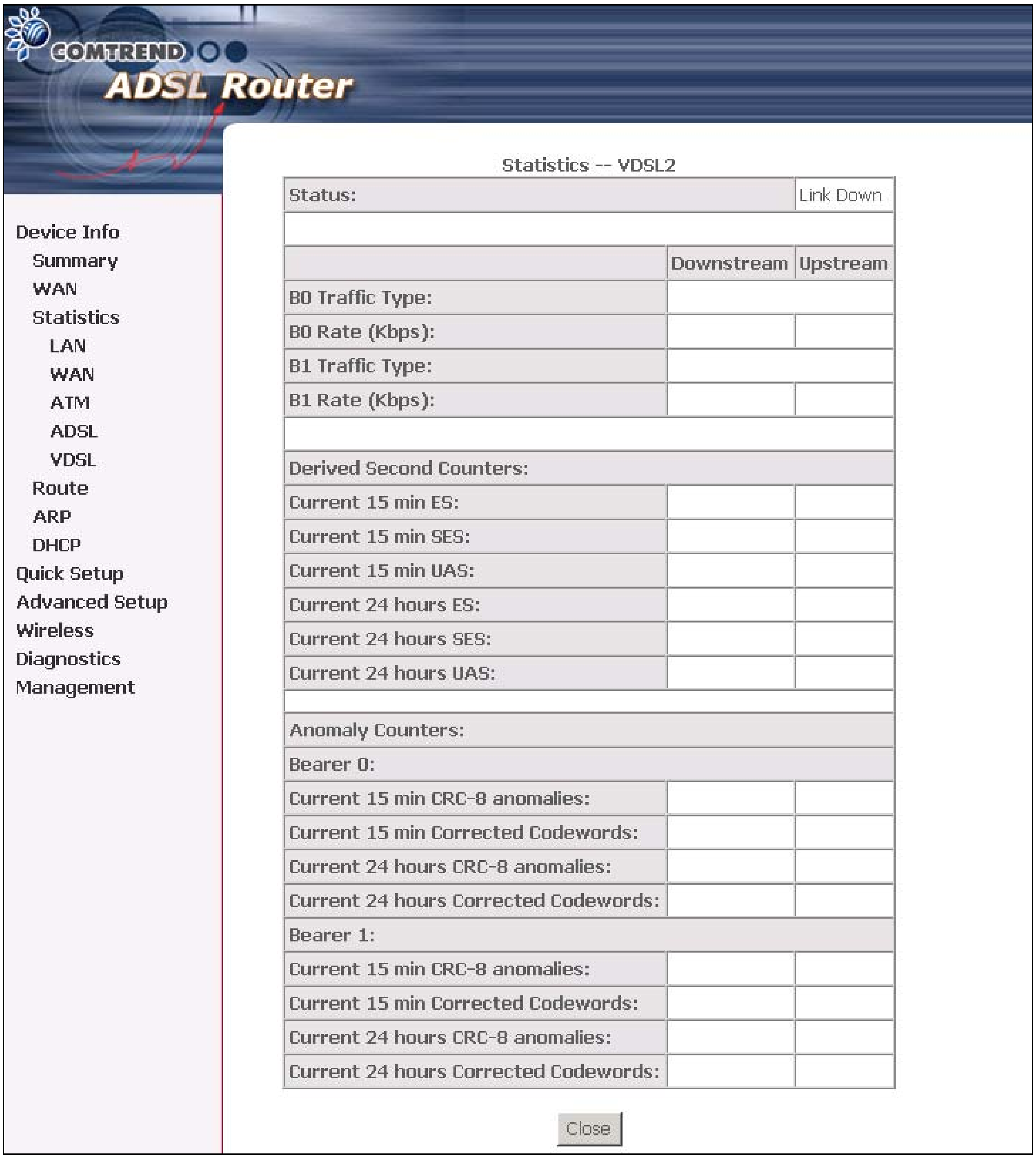
Mode:	G.DMT
Type:	Fast
Line Coding:	Trellis On
Status:	No Defect
Link Power State:	L0

	Downstream	Upstream
SNR Margin (dB):	20.2	6.0
Attenuation (dB):	0.0	1.0
Output Power (dBm):	7.8	11.9
Attainable Rate (Kbps):	11296	932
Rate (Kbps):	8128	832
K (number of bytes in DMT frame):	255	27
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	85667	85665
Super Frame Errors:	0	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	27918394	0
Data Cells:	36	0
Bit Errors:	0	0
Total ES:	1	8
Total SES:	1	3
Total UAS:	46	25127

The extra items are explained here.

K (number of bytes in DMT frame):	255	27
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0

4.2.5 VDSL Statistics



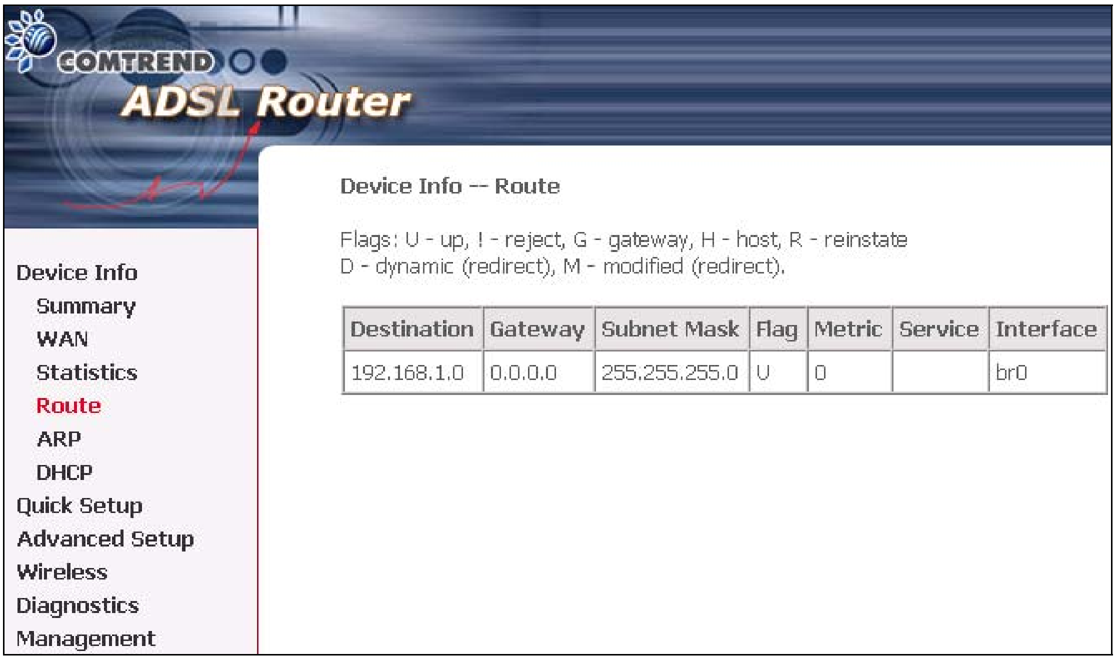
Statistics -- VDSL2

Status:		Link Down
	Downstream	Upstream
B0 Traffic Type:		
B0 Rate (Kbps):		
B1 Traffic Type:		
B1 Rate (Kbps):		
Derived Second Counters:		
Current 15 min ES:		
Current 15 min SES:		
Current 15 min UAS:		
Current 24 hours ES:		
Current 24 hours SES:		
Current 24 hours UAS:		
Anomaly Counters:		
Bearer 0:		
Current 15 min CRC-8 anomalies:		
Current 15 min Corrected Codewords:		
Current 24 hours CRC-8 anomalies:		
Current 24 hours Corrected Codewords:		
Bearer 1:		
Current 15 min CRC-8 anomalies:		
Current 15 min Corrected Codewords:		
Current 24 hours CRC-8 anomalies:		
Current 24 hours Corrected Codewords:		

Field	**Description**
Status:	VDSL link status.
B0 Traffic Type:	ATM or PTM
B0 Rate (Kbps):	Bearer 0 current sync rate.
B1 Traffic Type:	ATM or PTM
B1 Rate (Kbps):	Bearer 1 current sync rate.
Derived Second Counters:	
Current 15 min ES:	An accumulative total for current 15 minute ES.
Current 15 min SES:	An accumulative total for current 15 minute SES.
Current 15 min UAS:	An accumulative total for current 15 minutes UAS.
Current 24 hours ES:	An accumulative total for current 24 hours ES.
Current 24 hours SES:	An accumulative total for current 24 hours SES.
Current 24 hours UAS:	An accumulative total for current 24 hours UAS.
Anomaly Counters:	
Bearer 0:	
Current 15 min CRC-8 anomalies:	An accumulative total for current 15 minute CRC-8 anomalies
Current 15 min Corrected Codewords:	An accumulative total for current 15 minute Corrected Codewords
Current 24 hours CRC-8 anomalies:	An accumulative total for current 24 hours CRC-8 anomalies
Current 24 hours Corrected Codewords:	An accumulative total for current hours CRC-8 corrected codewords
Bearer 1:	
Current 15 min CRC-8 anomalies:	An accumulative total for current 15 minute CRC-8 anomalies
Current 15 min Corrected Codewords:	An accumulative total for current 15 minute Corrected Codewords
Current 24 hours CRC-8 anomalies:	An accumulative total for current 24 hours CRC-8 anomalies
Current 24 hours Corrected Codewords:	An accumulative total for current 24 hours CRC-8 corrected codewords

4.2.6 Route

Choose **Route** to display the routes that the route information has learned.



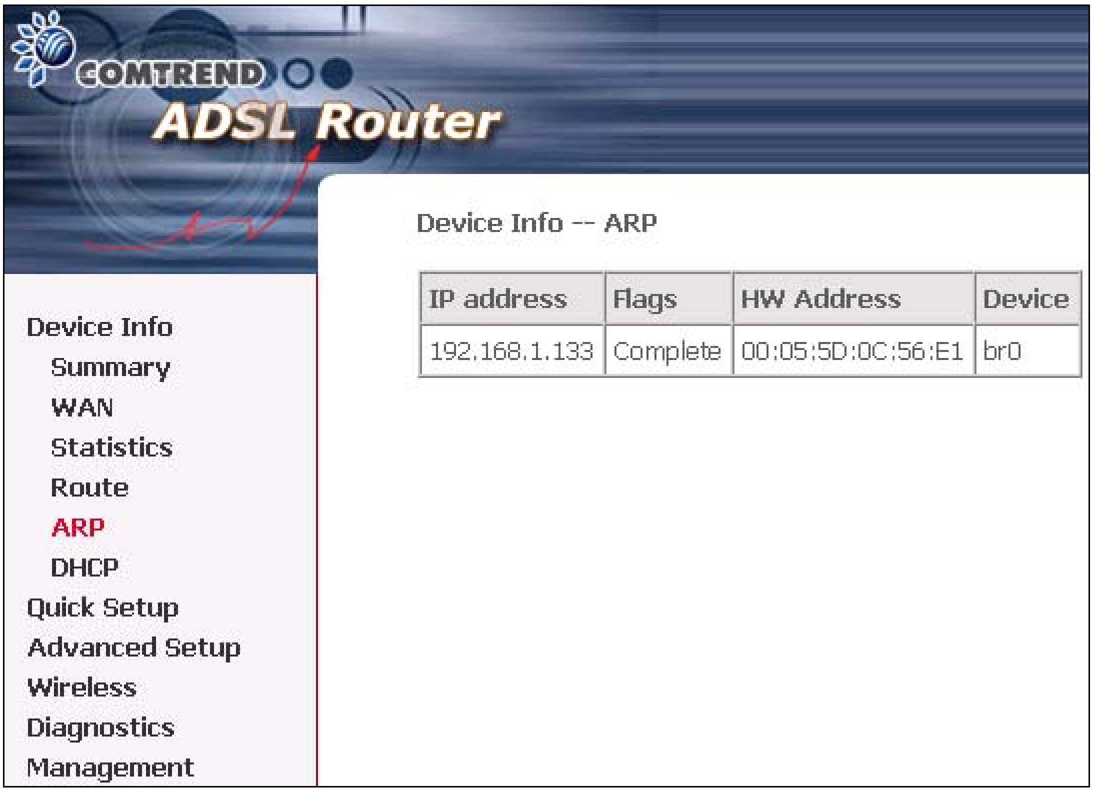
Device Info -- Route

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

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

4.2.7 ARP

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

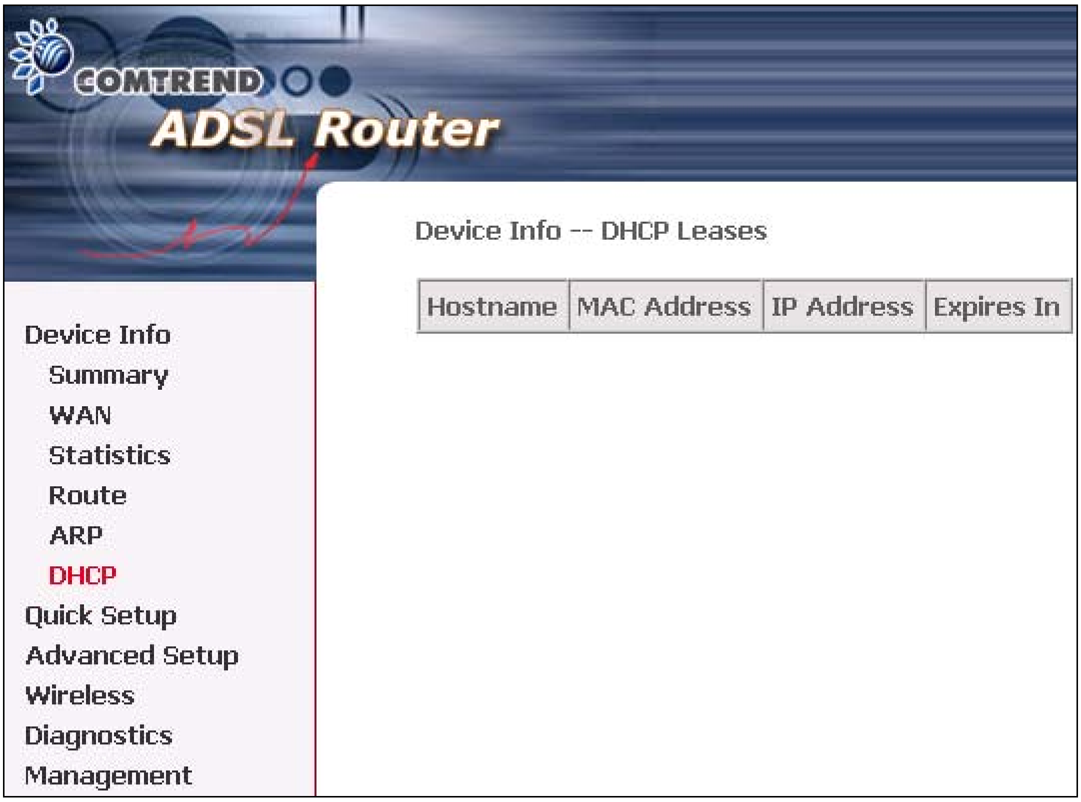


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.133	Complete	00:05:5D:0C:56:E1	br0

4.2.8 DHCP

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



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

Chapter 5 Quick Setup

The Quick Setup allows the user to configure the A/VDSL router for DSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either manually customize the router or follow the online instruction to set up the router.

The CT-5372 A/VDSL router supports the following five network operating modes over an ATM PVC WAN interface.

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

The following configuration considerations apply:

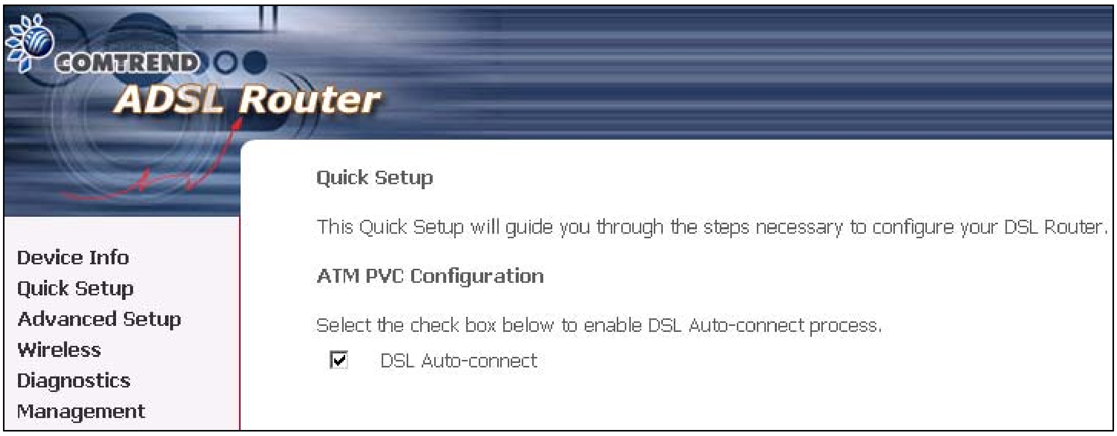
- The WAN network operating mode operation depends on the service provider’s configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-5372 is to run the PPPoE client. The CT-5372 can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge in PPPoE mode. CT-5372 also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client for non-PPPoE LAN devices.
- NAPT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAPT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

Note: Up to eight 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.

5.1 Auto Quick Setup

The auto quick setup requires the A/VDSL link to be up. The A/VDSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted with.

1. Select **Quick Setup** to display the DSL Quick Setup screen.



Quick Setup

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

ATM PVC Configuration

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

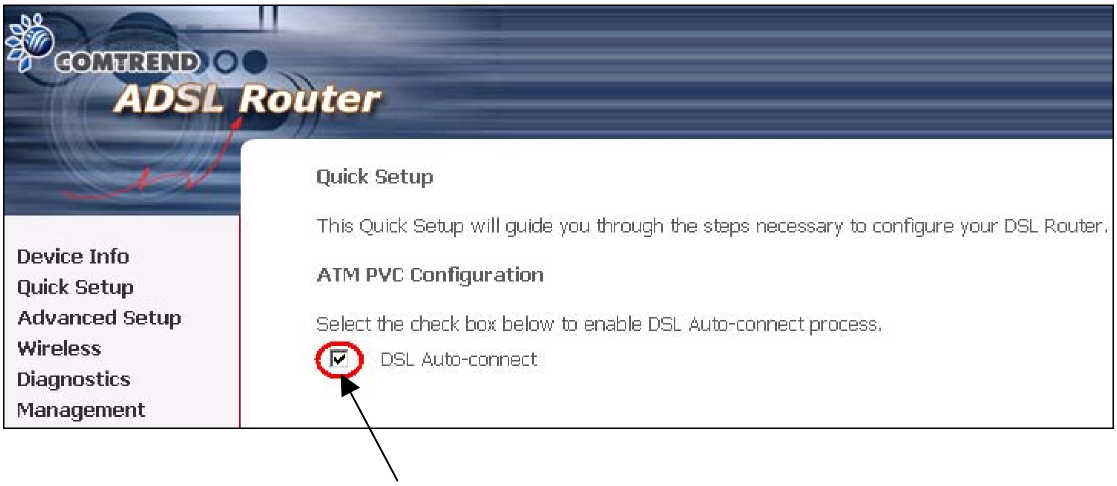
☑ DSL Auto-connect

2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.

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

5.2 Manual Quick Setup

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



Quick Setup

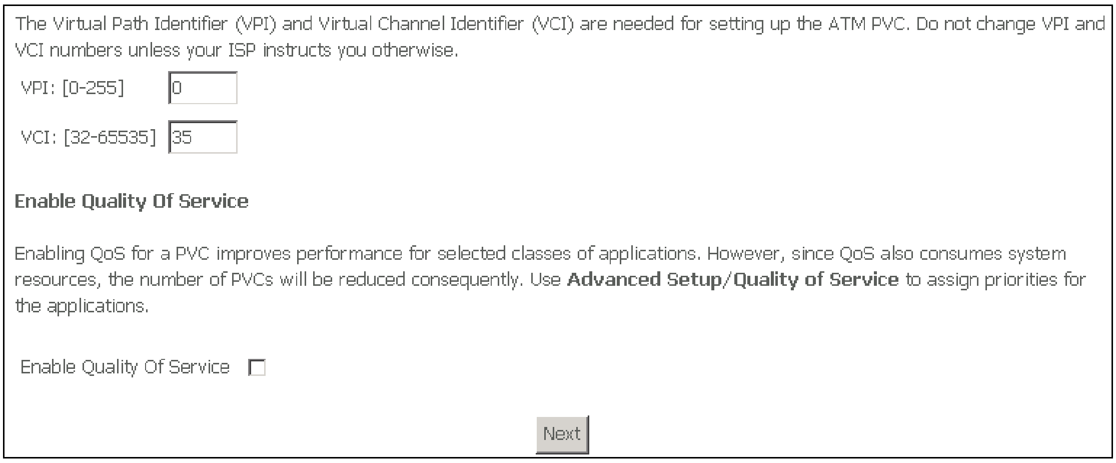
This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

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

☑ DSL Auto-connect

Un-tick this checkbox to enable manual setup and display the following screen.



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

VPI: [0-255] 0

VCI: [32-65535] 35

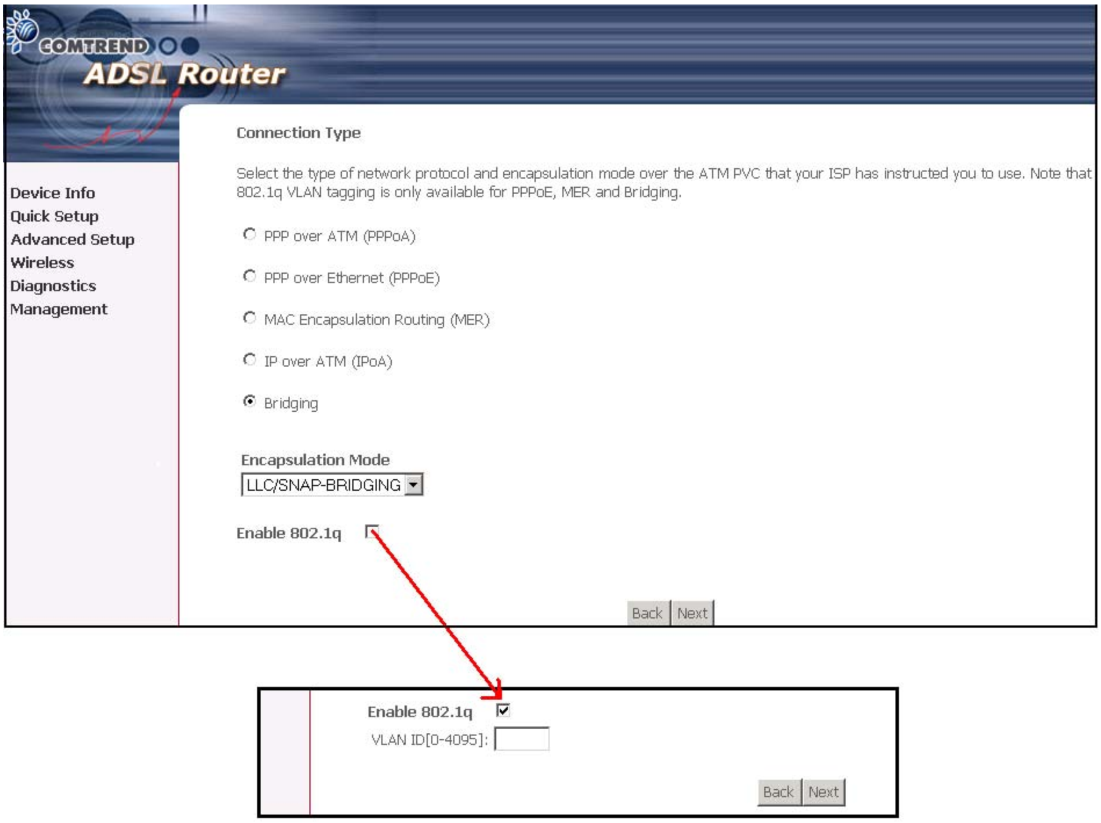
Enable Quality Of Service

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

Enable Quality Of Service □

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

STEP 3: Then, choose the Encapsulation mode. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click Next.



Connection Type

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

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

● Bridging

Encapsulation Mode: LLC/SNAP-BRIDGING

Enable 802.1q □

Back Next

Enable 802.1q ☑

VLAN ID[0-4095]:

Back Next

Encapsulation Mode

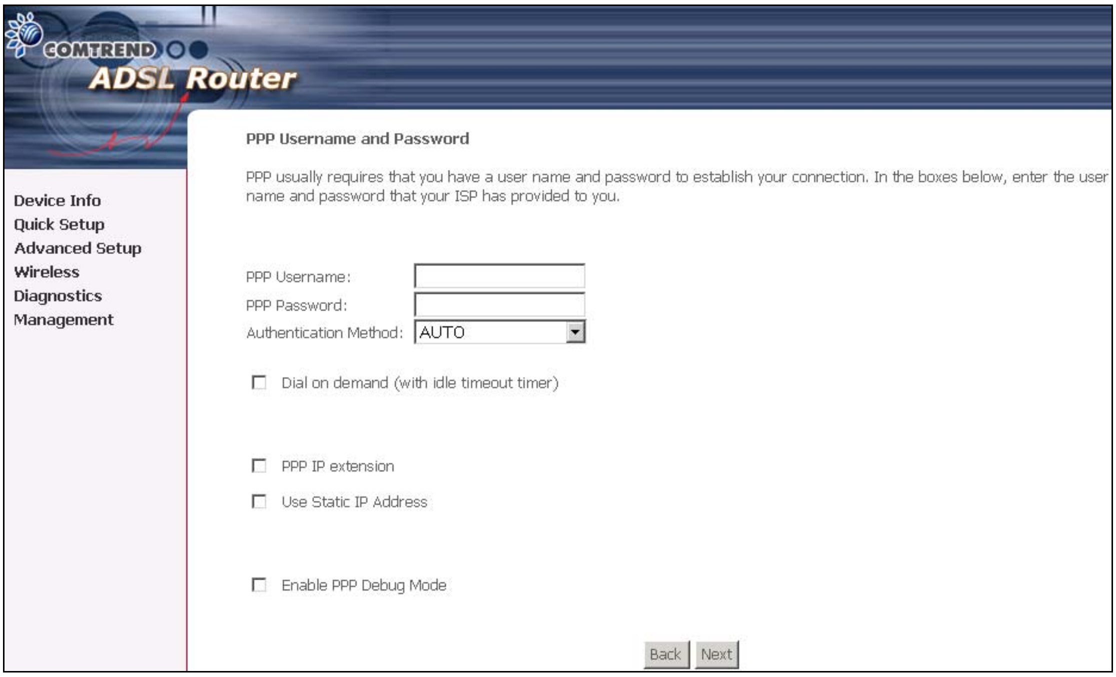
Choosing different connection types provides different encapsulation modes.

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

STEP 4: Click **Next** to display the following screen. Choosing different connection types pops up different settings requests. Enter appropriate settings that are requested by your service provider. The following descriptions state each connection type setup separately.

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

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



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method: AUTO

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

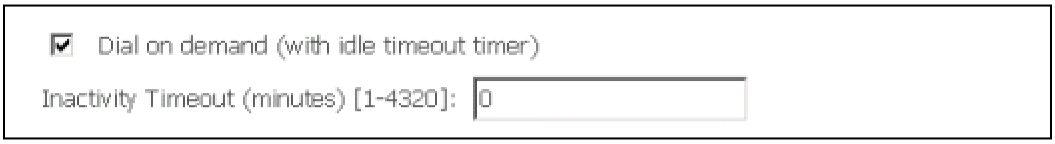
□ Enable PPP Debug Mode

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 WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

Disconnect if no activity

The CT-5372 can be configured to disconnect if there is no activity for a period of time by selecting the **Disconnect if no activity** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes. The default is 0 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]: 0

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.
The PPP IP Extension supports the following conditions:

- 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's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL router has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

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

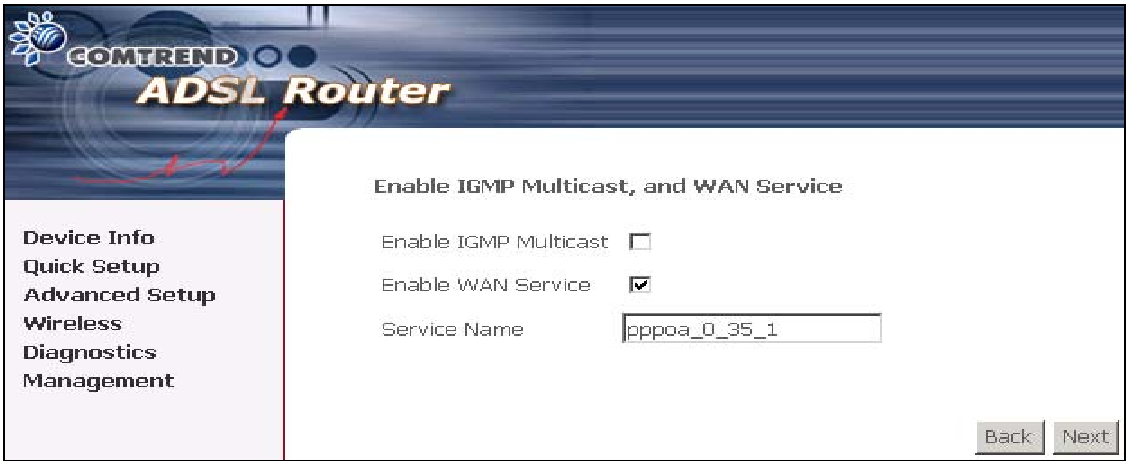
Enable PPP Debug Mode
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

2. Click **Next** to display the following screen.

Enable IGMP Multicast checkbox: 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 checkbox: Tick this item to enable the ADSL service. Untick it to stop the ADSL service.

Service Name: This is user-defined.



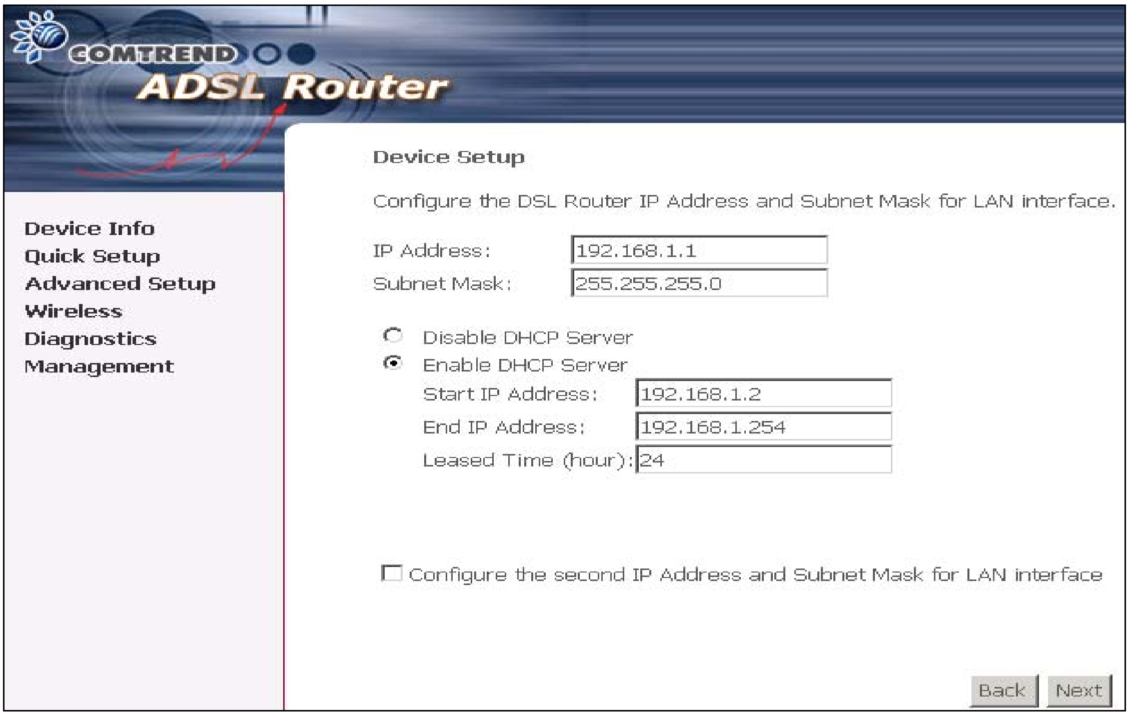
Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name pppoa_0_35_1

3. After entering your settings, select **Next**. The following screen appears. This page allows the user to configure the LAN interface IP address, subnet mask and DHCP server. If the user would like this ADSL router to assign dynamic IP address, DNS server and default gateways to other LAN devices, select the button **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP leased time.



Device Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

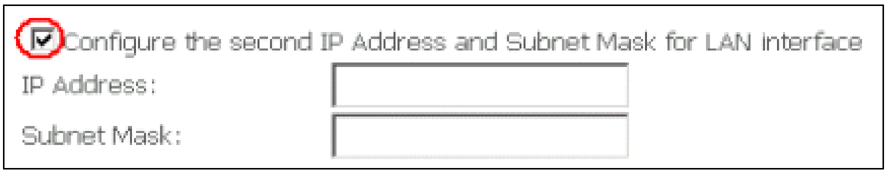
Leased Time (hour): 24

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

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the router's default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

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

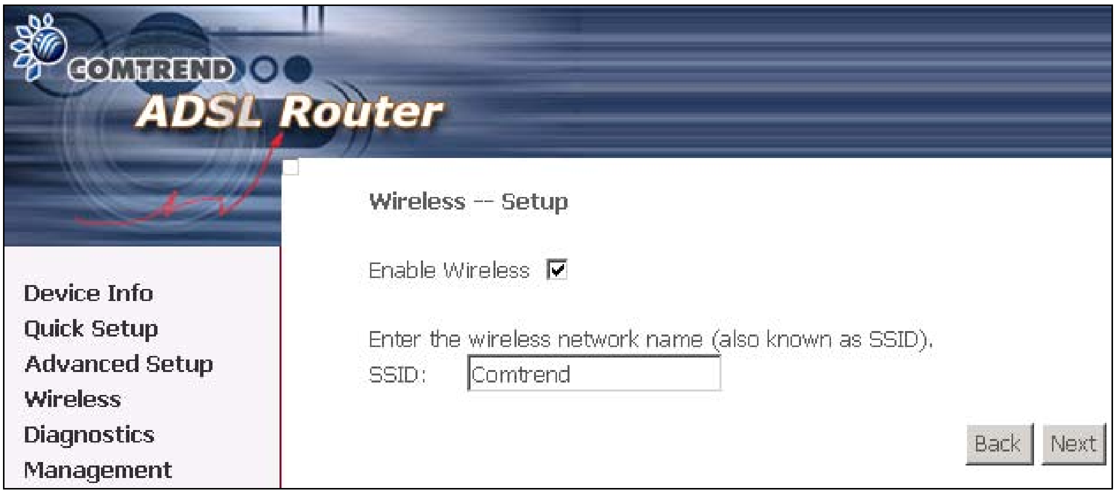


☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

4. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



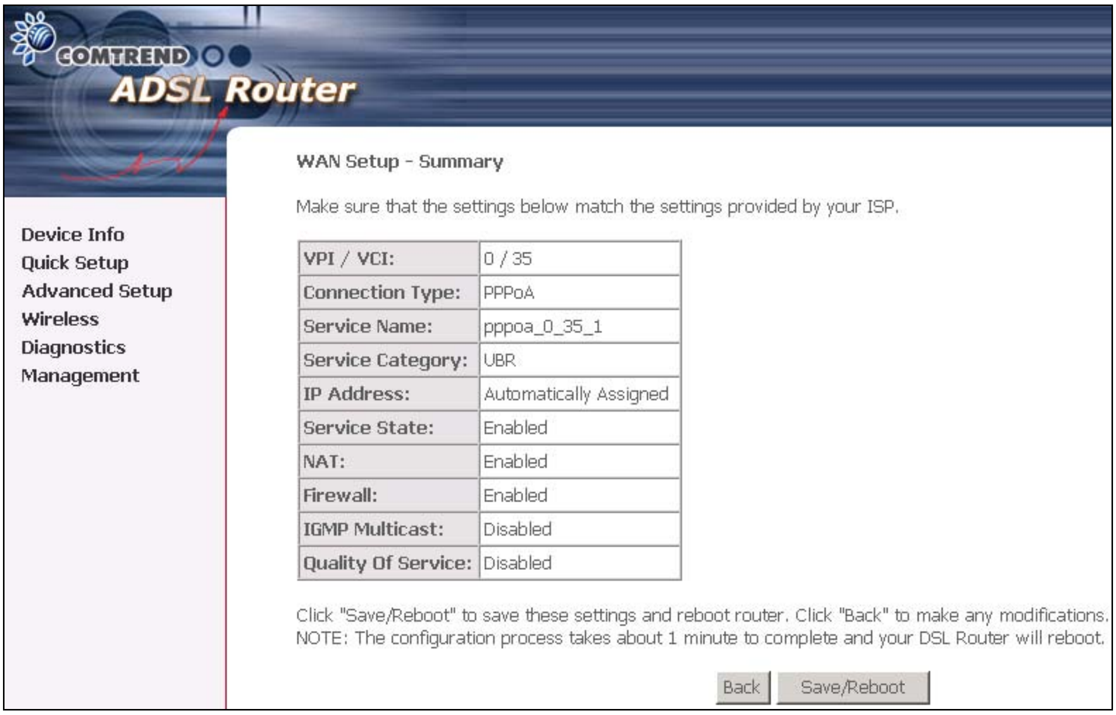
Wireless -- Setup

Enable Wireless ☑

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

SSID: Comtrend

5. Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

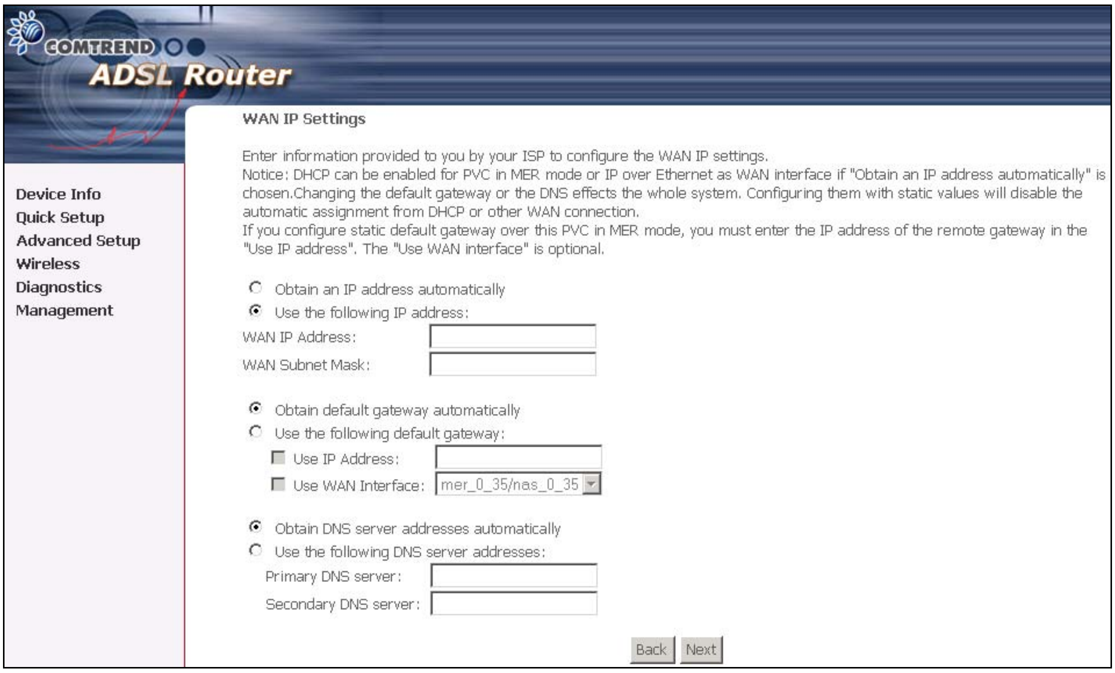
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

6. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5372 is ready for operation and the LEDs display as described in the LED description tables.

5.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index provided by the ISP and click **Next**.
3. Select the MAC Encapsulation Routing (MER) radio button, and click **Next**. The following screen appears.



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects 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". The "Use WAN interface" is optional.

○ Obtain an IP address automatically
● Use the following IP address:
WAN IP Address:
WAN Subnet Mask:

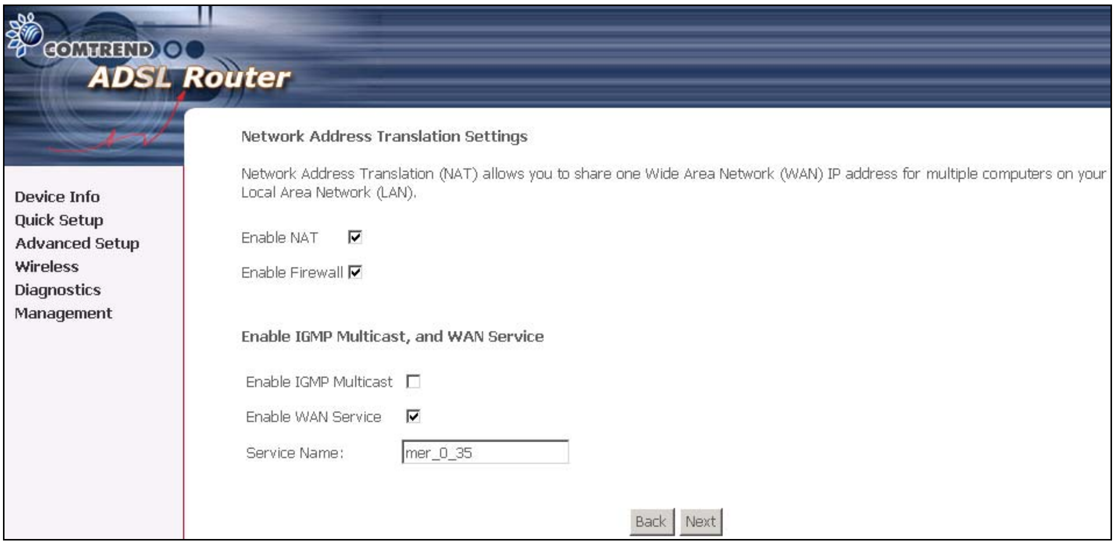
● Obtain default gateway automatically
○ Use the following default gateway:
□ Use IP Address:
□ Use WAN Interface: mer_0_35/nas_0_35

● Obtain DNS server addresses automatically
○ Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

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

Notice: DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS effects 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". The "Use WAN interface" is optional.
The ISP should provide the values that must be entered in the entry fields.

4. Click **Next** to display the following screen.



Network Address Translation Settings

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

Enable NAT ☑

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: mer_0_35

Enable NAT checkbox: If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel. The default setting for Mer is enable.

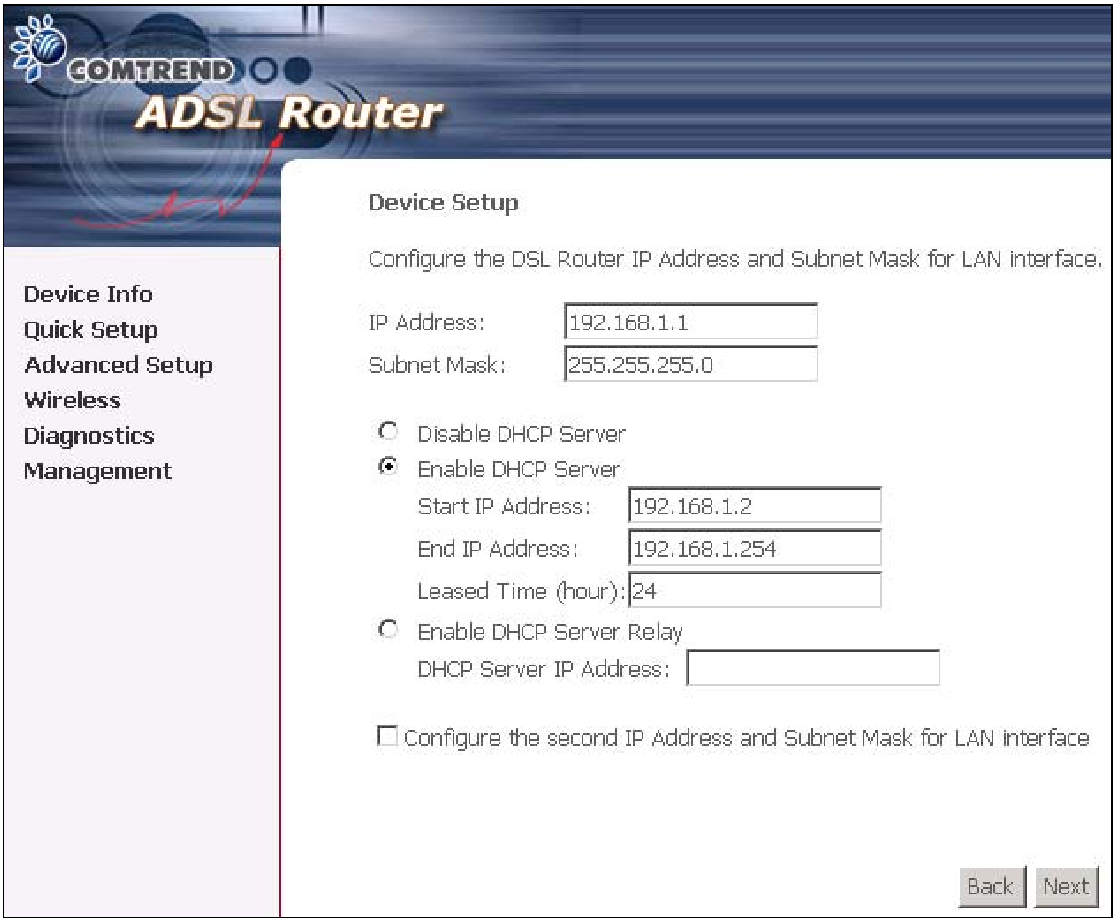
Enable Firewall checkbox: If the firewall checkbox is selected, the firewall submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Firewall submenu will not be displayed on the left main panel. The default setting for Mer is enable.

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 the checkbox to enable the WAN (ADSL) service. If this item is not selected, you will not be able to use the ADSL service. The default setting for Mer is enable.

Service Name: This is User-defined.

5. Upon completion, click **Next**. The following screen appears.



Device Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

○ Enable DHCP Server Relay

DHCP Server IP Address:

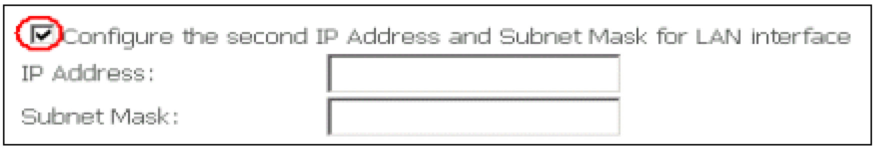
□ Configure the second IP Address and Subnet Mask for LAN interface

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the router’s default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

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



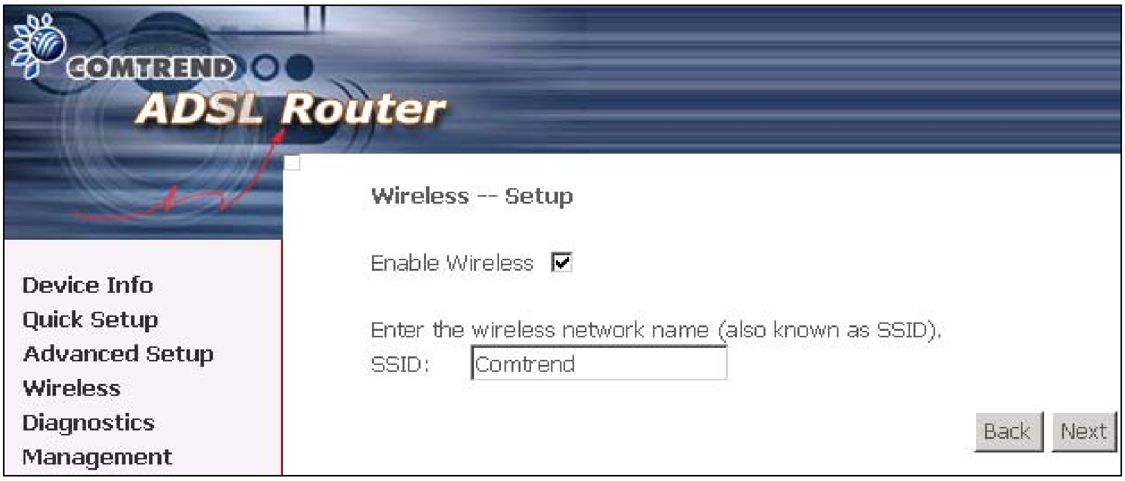
☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

6. After entering your settings, select **Next** to display the following screen. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

7. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



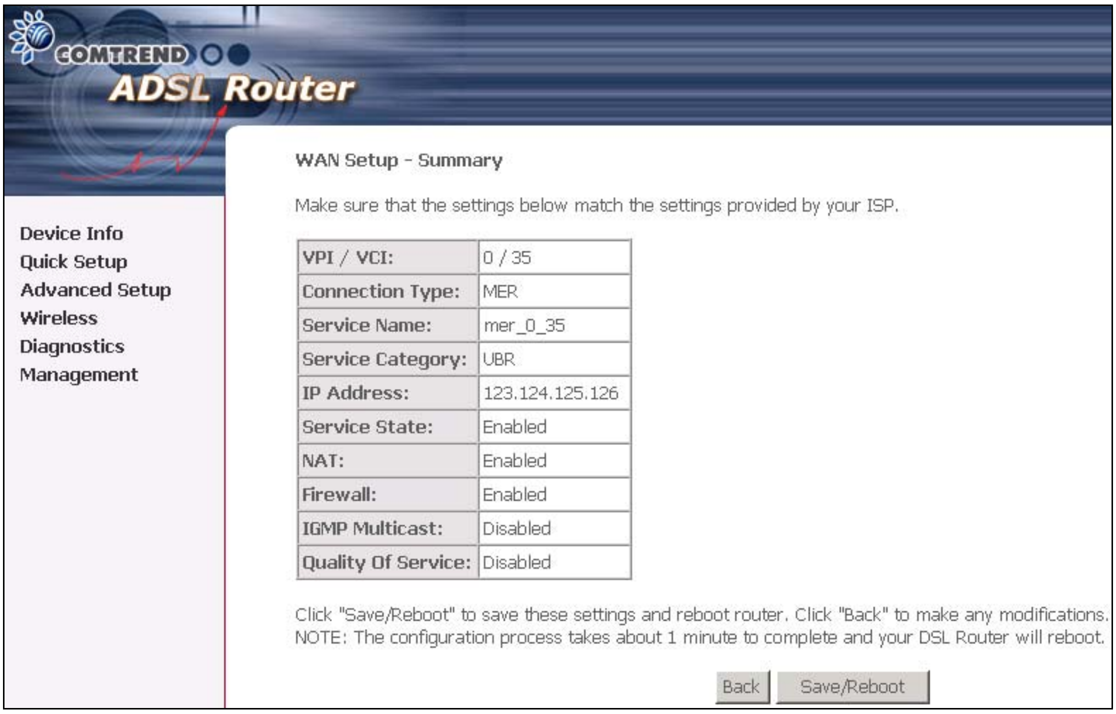
Wireless -- Setup

Enable Wireless ☑

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

SSID: Comtrend

The following screen will be displayed.



WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	MER
Service Name:	mer_0_35
Service Category:	UBR
IP Address:	123.124.125.126
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

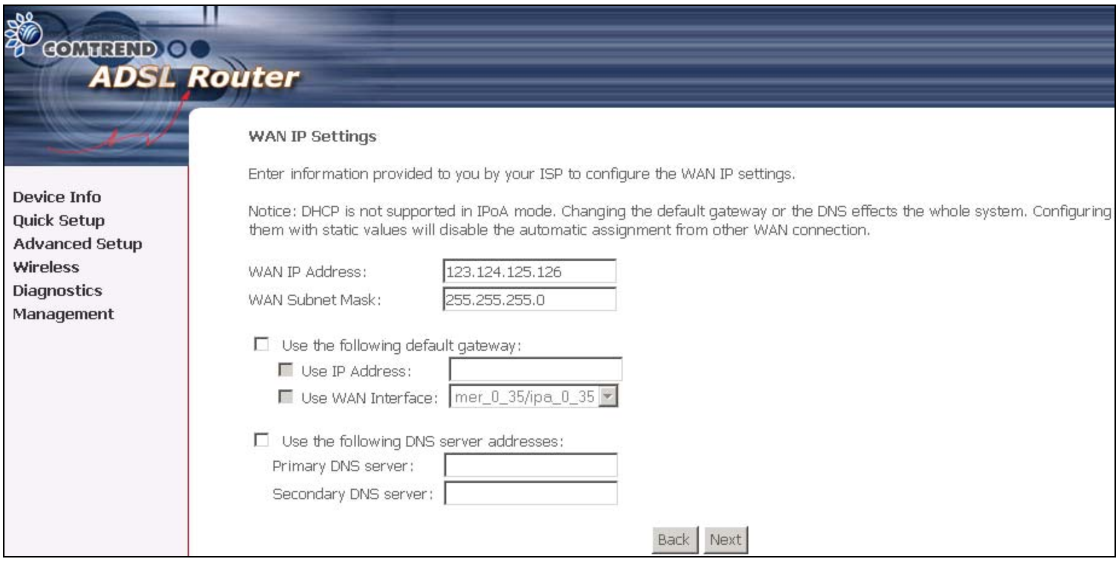
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5372 is ready for operation and the LEDs display as described in the LED description tables.

5.2.3 IP Over ATM

To configure IP Over ATM,

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**. The following screen appears.



WAN IP Settings

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

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

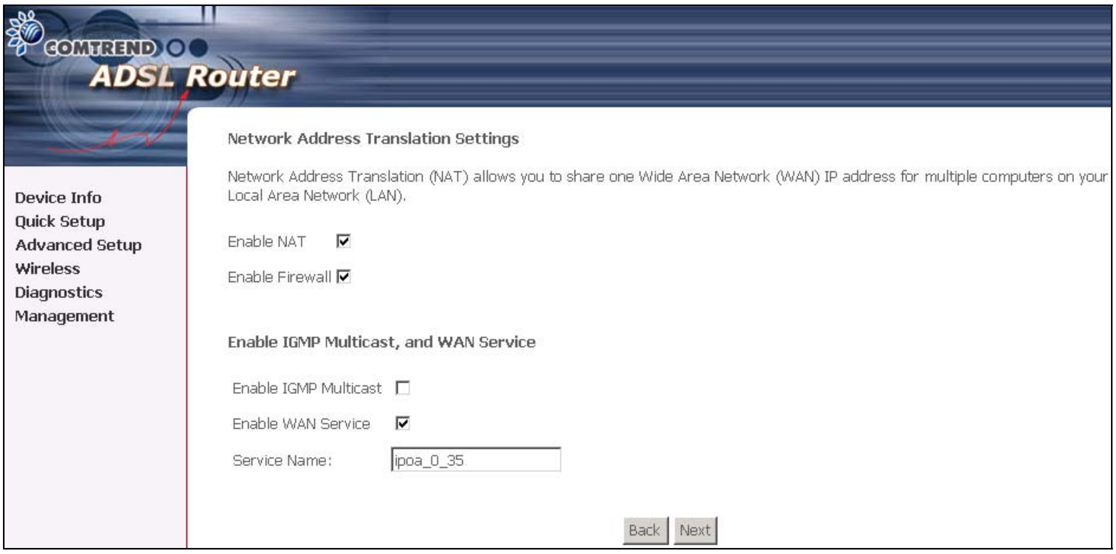
WAN IP Address: 123.124.125.126
WAN Subnet Mask: 255.255.255.0

☐ Use the following default gateway:
☐ Use IP Address:
☐ Use WAN Interface: mer_0_35/ipa_0_35

☐ Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

Notice that 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 the ISP.

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



Network Address Translation Settings

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

Enable NAT ☑

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☑

Service Name: ipoa_0_35

Enable NAT checkbox

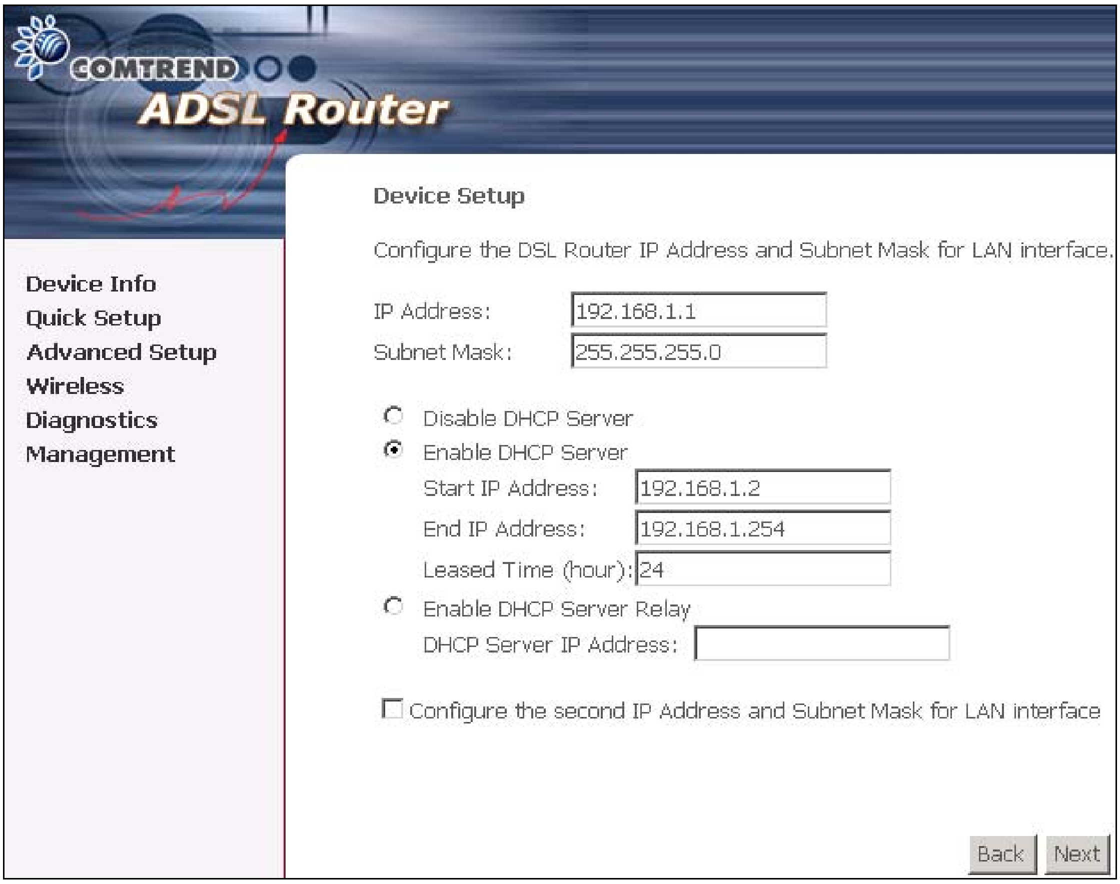
If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel. The default setting for IPoA is enable.

Enable Firewall checkbox

If the firewall checkbox is selected, the firewall submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Firewall submenu will not be displayed on the left main panel. The default setting for IPoA is enable.

Enable WAN Service: Tick the checkbox to enable the WAN (ADSL) service. If this item is not selected, you will not be able to use the ADSL service. The default setting for IPoA is enable.

6. Click **Next** to display the following screen. The Device Setup page allows the user to configure the LAN interface IP address and DHCP server if the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.



Device Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

○ Enable DHCP Server Relay

DHCP Server IP Address:

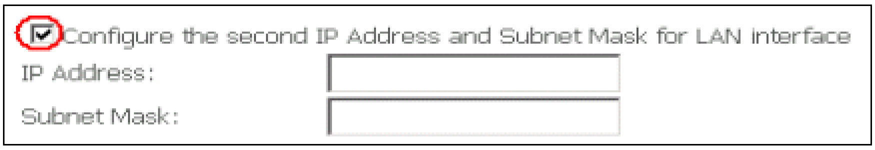
□ Configure the second IP Address and Subnet Mask for LAN interface

The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the router's default IP address is 192.168.1.1 and the default private address range provided by ISP server in the router is 192.168.1.2 through 192.168.1.254.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

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



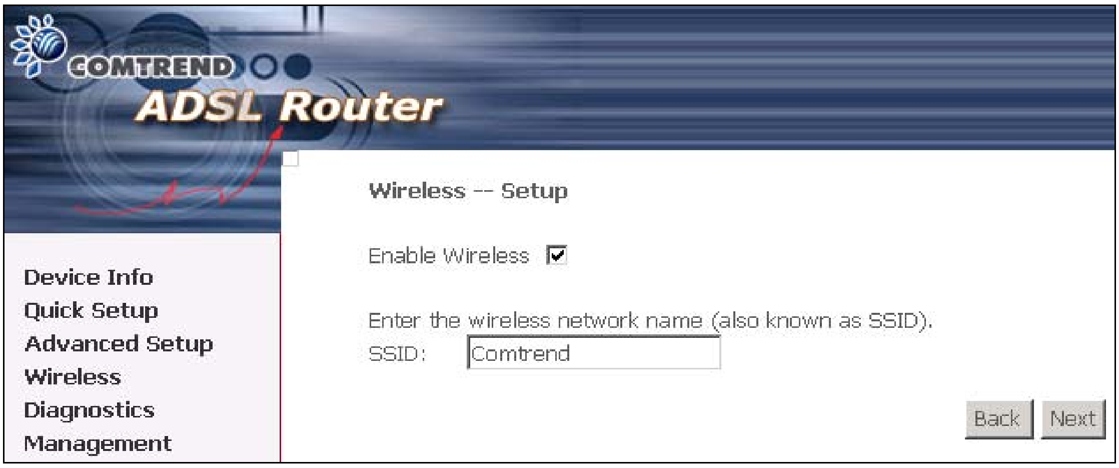
☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

7. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

8. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



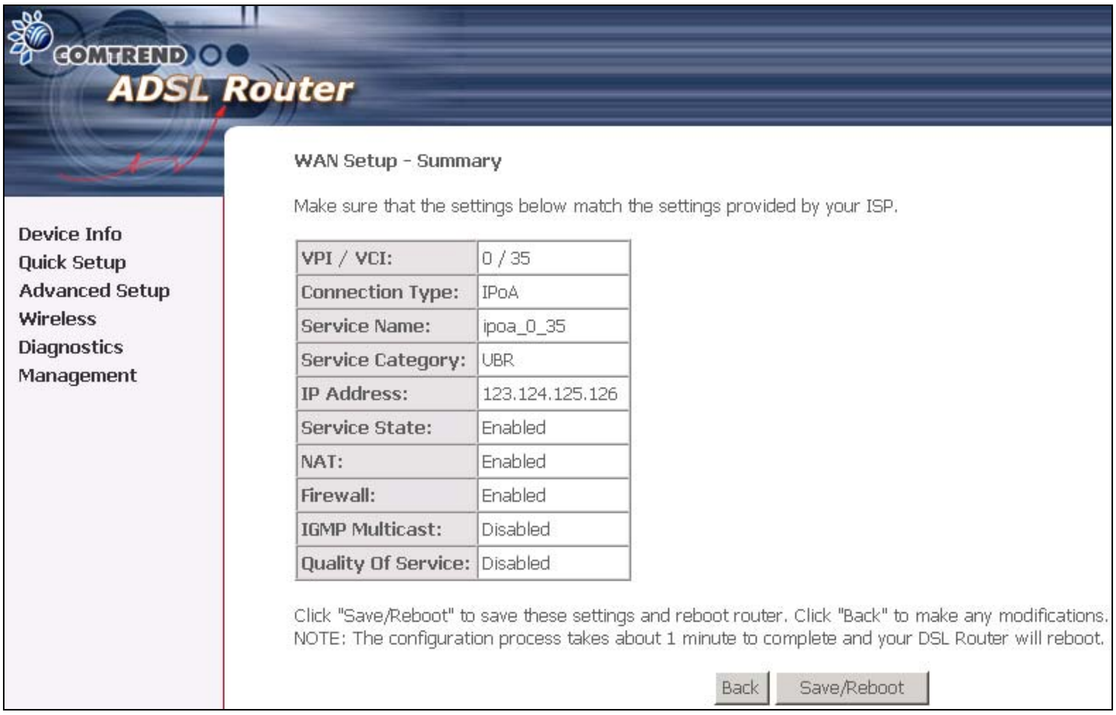
Wireless -- Setup

Enable Wireless ☑

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

SSID: Comtrend

The following screen will be displayed.



WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_35
Service Category:	UBR
IP Address:	123.124.125.126
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

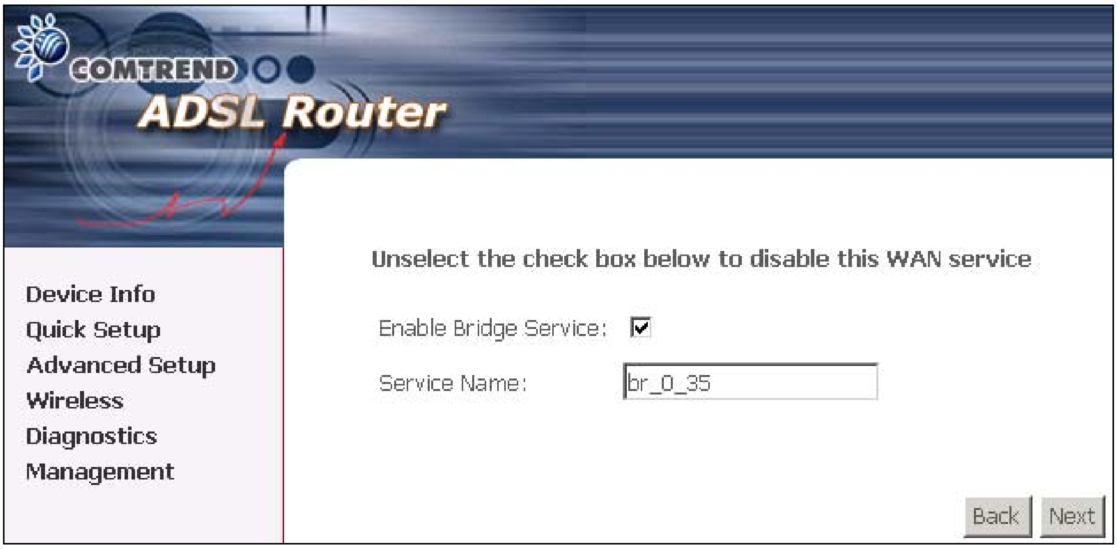
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

8. After clicking **Save/Reboot**, the router will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-5372 is ready for operation and the LEDs display as described in the LED description tables.

5.2.4 Bridging

Select the bridging mode. To configure Bridging, do the following.

1. Select Quick Setup and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type in the VPI and VCI values provided by the ISP and click Next.
4. Select the Bridging radio button and click **Next**. The following screen appears. To use the bridge service, tick the checkbox, Enable Bridge Service, and enter the service name.

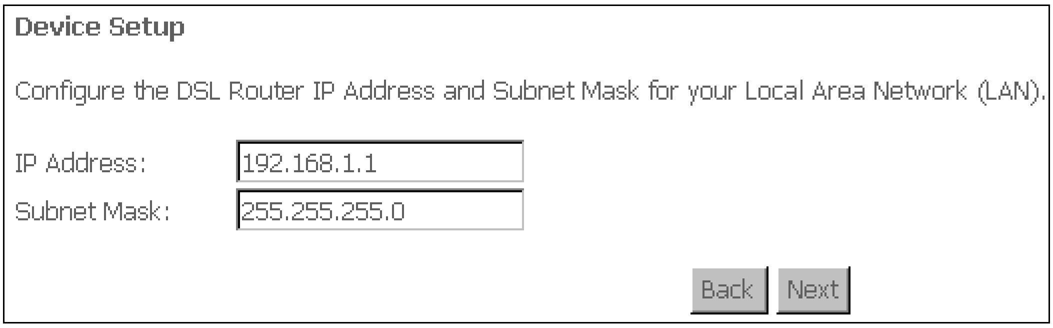


Unselect the check box below to disable this WAN service

Enable Bridge Service: ☑

Service Name: br_0_35

5. Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the ADSL router. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the ADSL router.



Device Setup

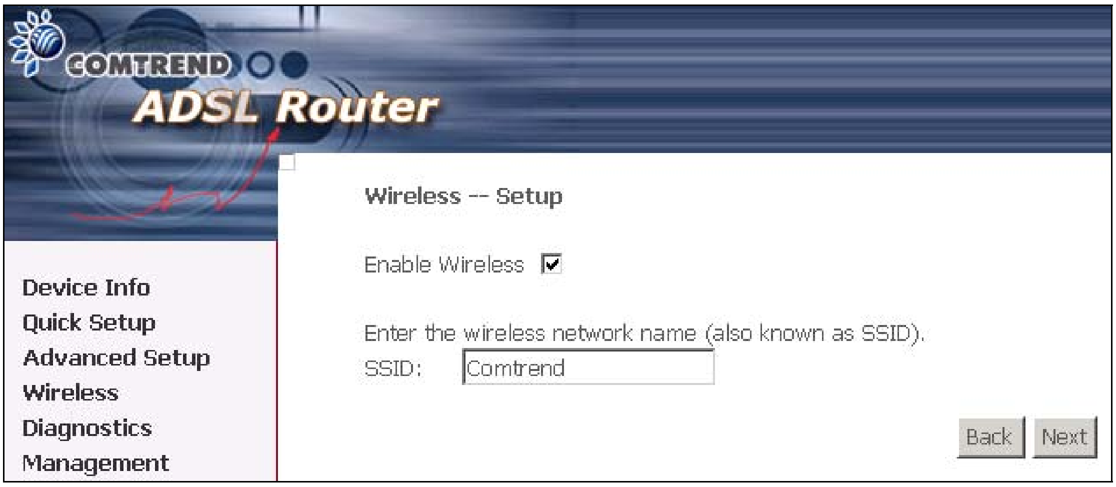
Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN).

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

6. Click next

7. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



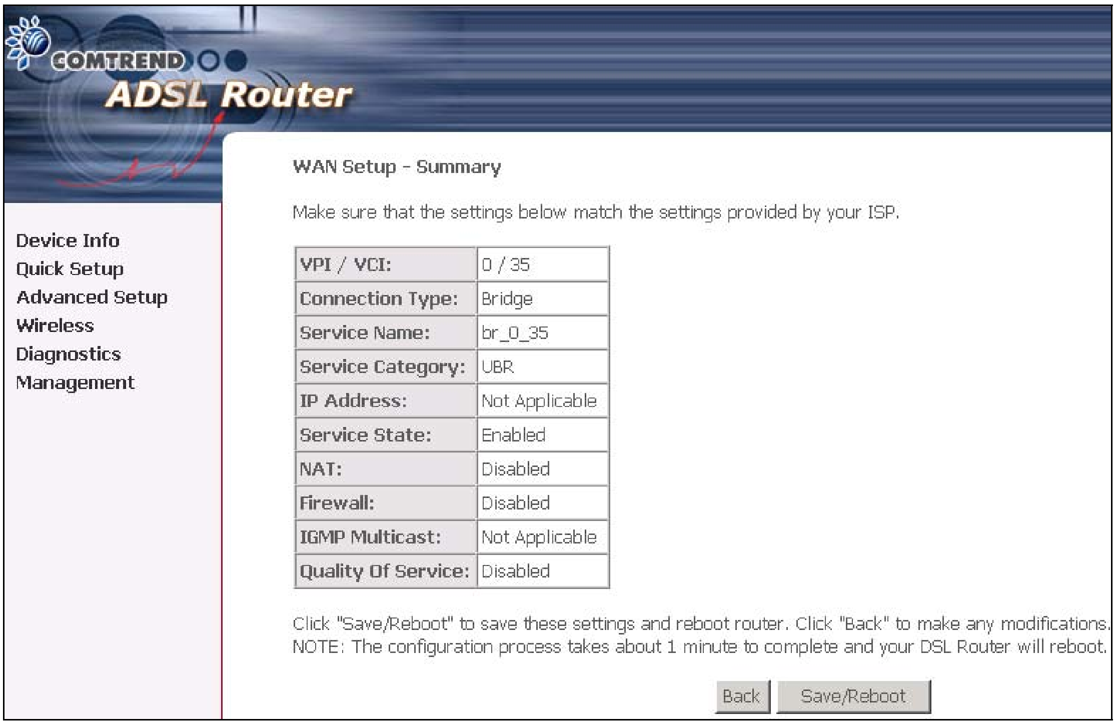
Wireless -- Setup

Enable Wireless ☑

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

SSID: Comtrend

The following screen will be displayed.



WAN Setup - Summary

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

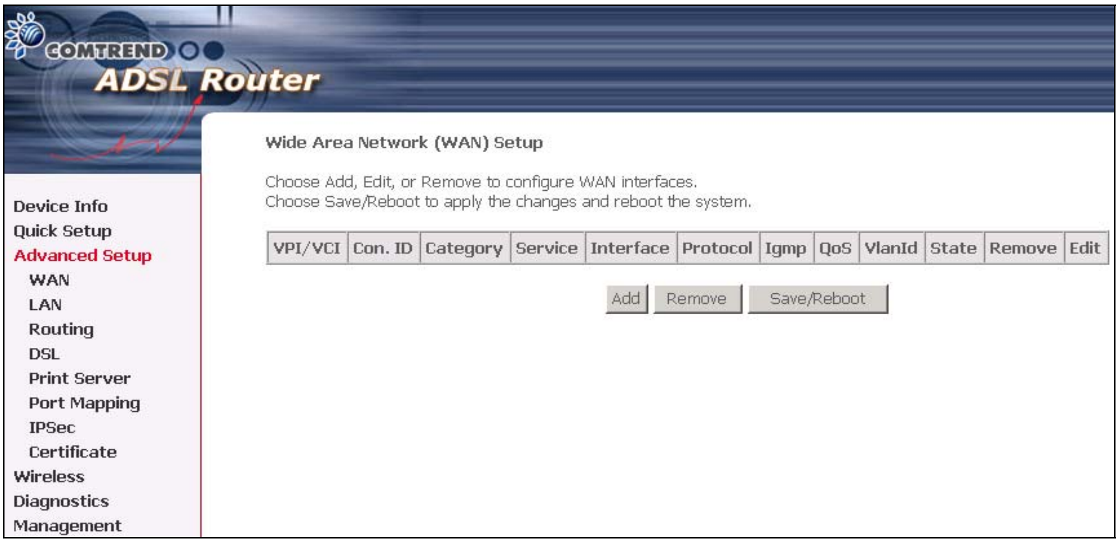
VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

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

The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

Chapter 6 Advanced Setup

This chapter explains: WAN, LAN, Routing, DSL and Port Mapping…...

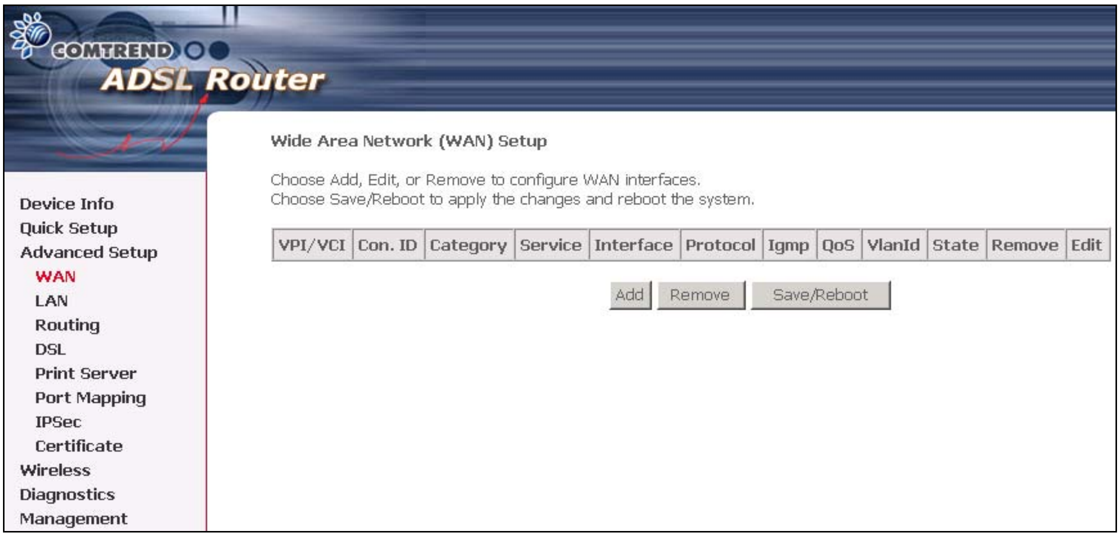


Wide Area Network (WAN) Setup

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

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit

6.1 WAN



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	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit

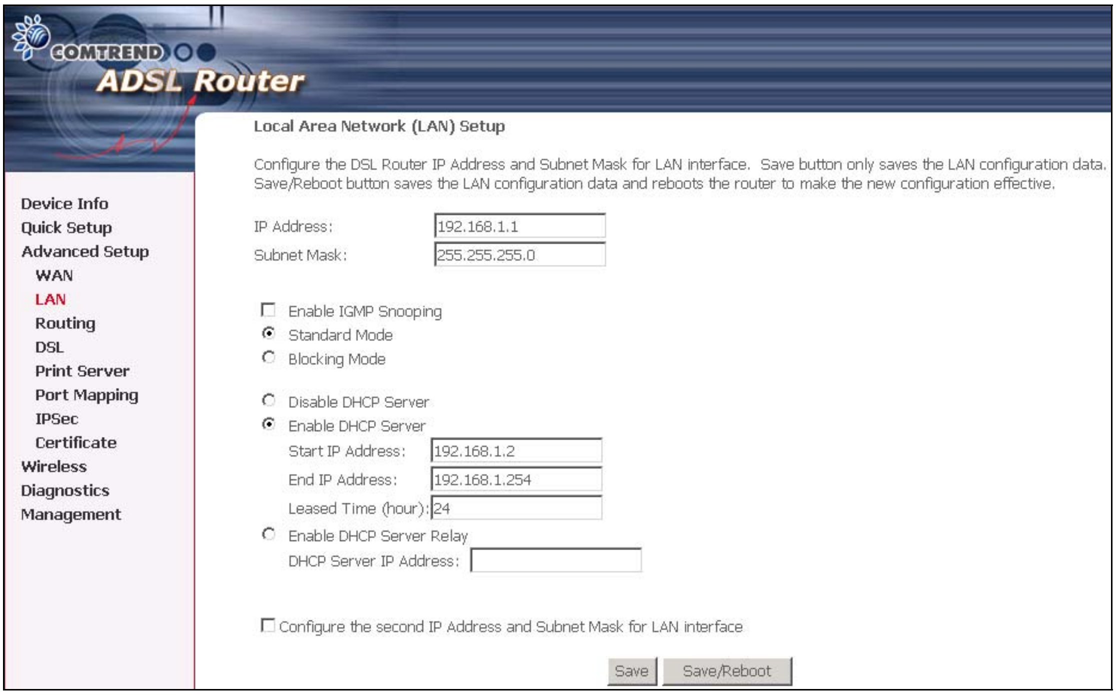
VlanID	• This function means one can add an 802.1Q VLAN tag on PPPoE/MER or Bridge mode. It means the packets are sent to WAN and a specific VlanID (802.1Q tag) will be added in the Ethernet header. The VlanID shows which 802.1Q tag will be added.

For further information on WAN, please reference section: 4.1, Page 19.

6.2 LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: Enter the IP address for the LAN port.
Subnet Mask: Enter the subnet mask for the LAN port.



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

□ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
○ Enable DHCP Server Relay
DHCP Server IP Address:

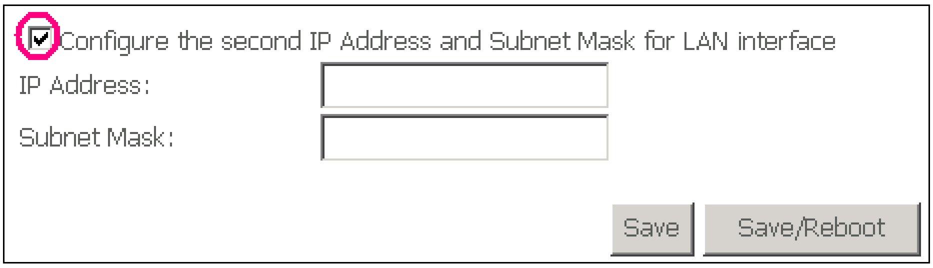
□ Configure the second IP Address and Subnet Mask for LAN interface

Enable IGMP Snooping: Enable /Disable the function that is IGMP Snooping.

Standard Mode: In standard mode, as in all prior releases, multicast traffic will flood to all bridge ports when there is no client subscribes to any multicast group – even when IGMP snooping is enabled.

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

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



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

IP Address:

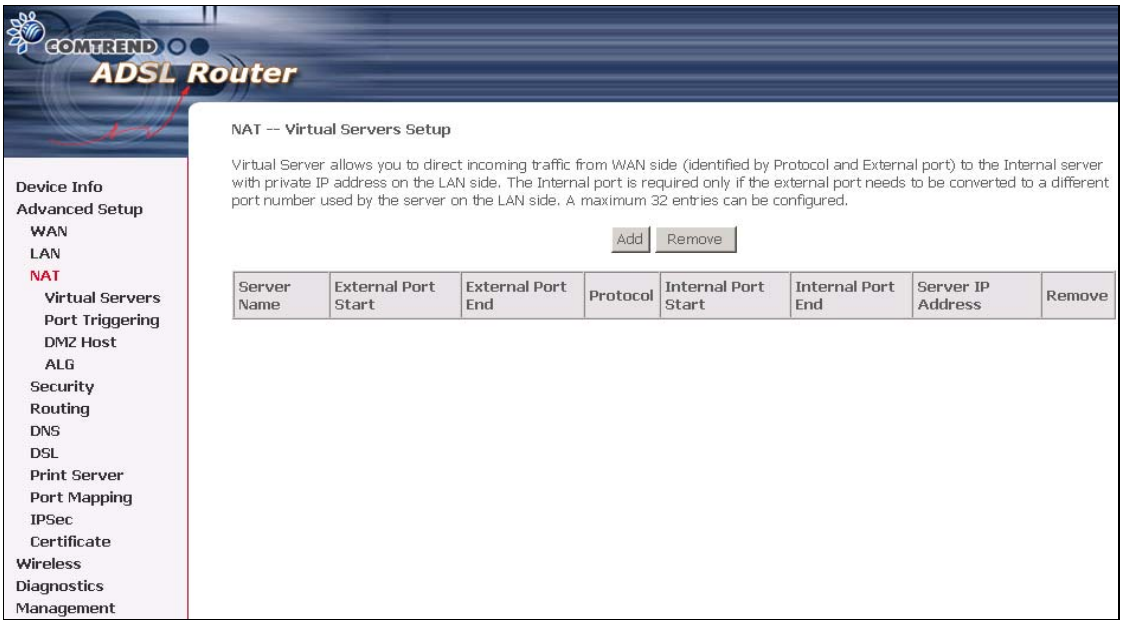
Subnet Mask:

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

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

6.3 NAT

To display the NAT function, you need to enable the NAT feature in the WAN Setup.



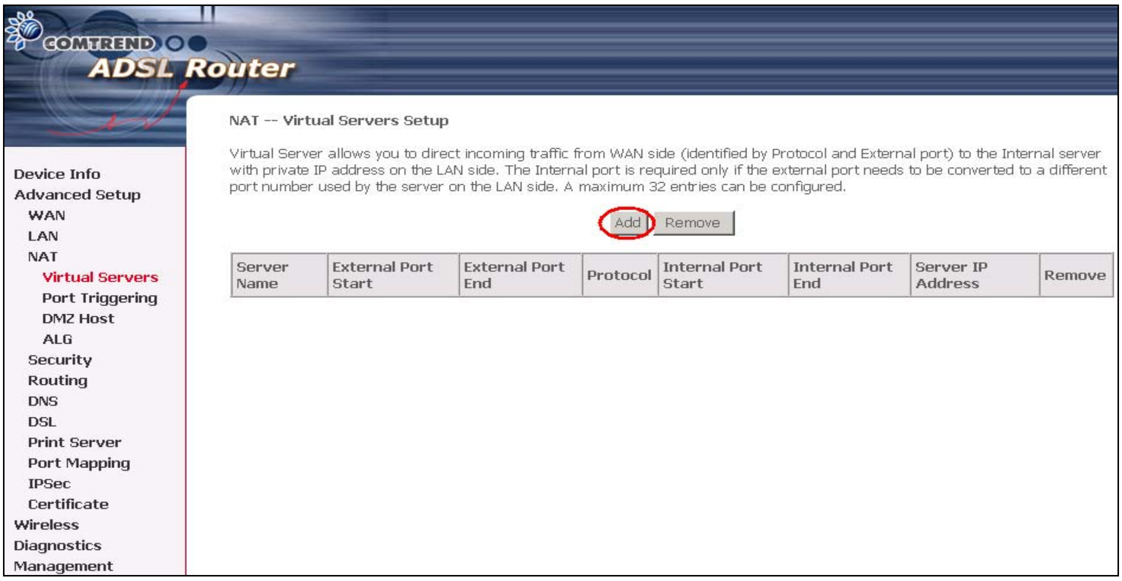
NAT -- Virtual Servers Setup

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove

6.3.1 Virtual Servers

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

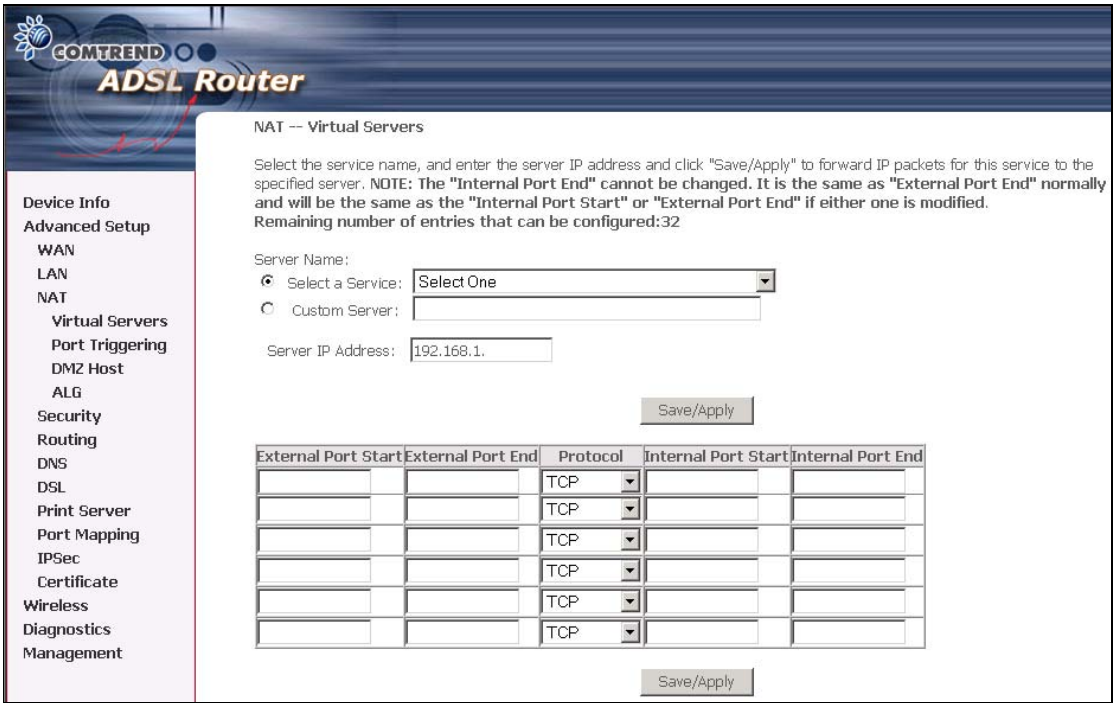


NAT -- Virtual Servers Setup

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

Remaining number of entries that can be configured:32

Server Name:

● Select a Service: Select One

○ Custom Server:

Server IP Address: 192.168.1.

Save/Apply

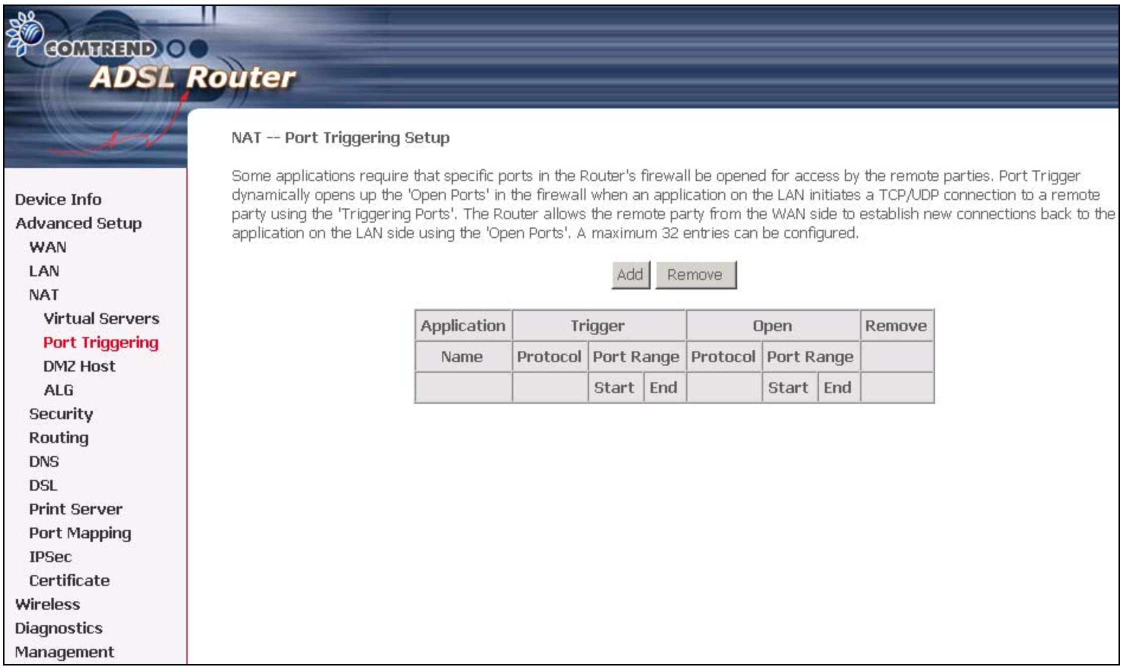
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Save/Apply

Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

6.3.2 Port Triggering

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

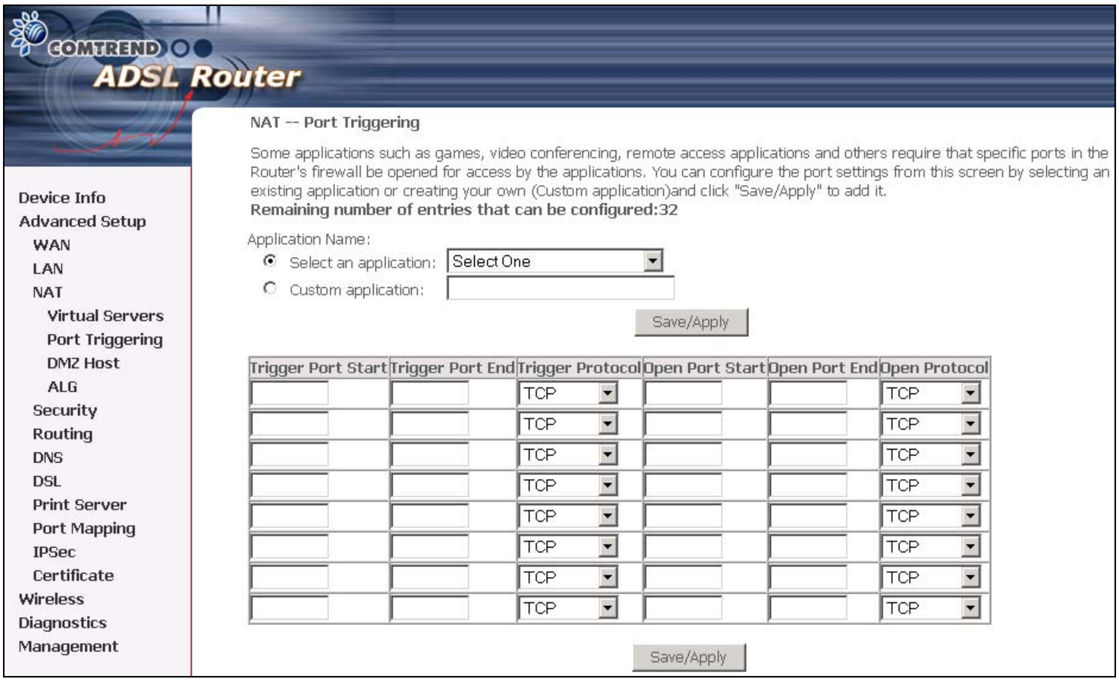


NAT -- Port Triggering Setup

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

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

To add a Trigger Port, simply click the Add button. The following will be displayed.



NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Application Name:

● Select an application: Select One

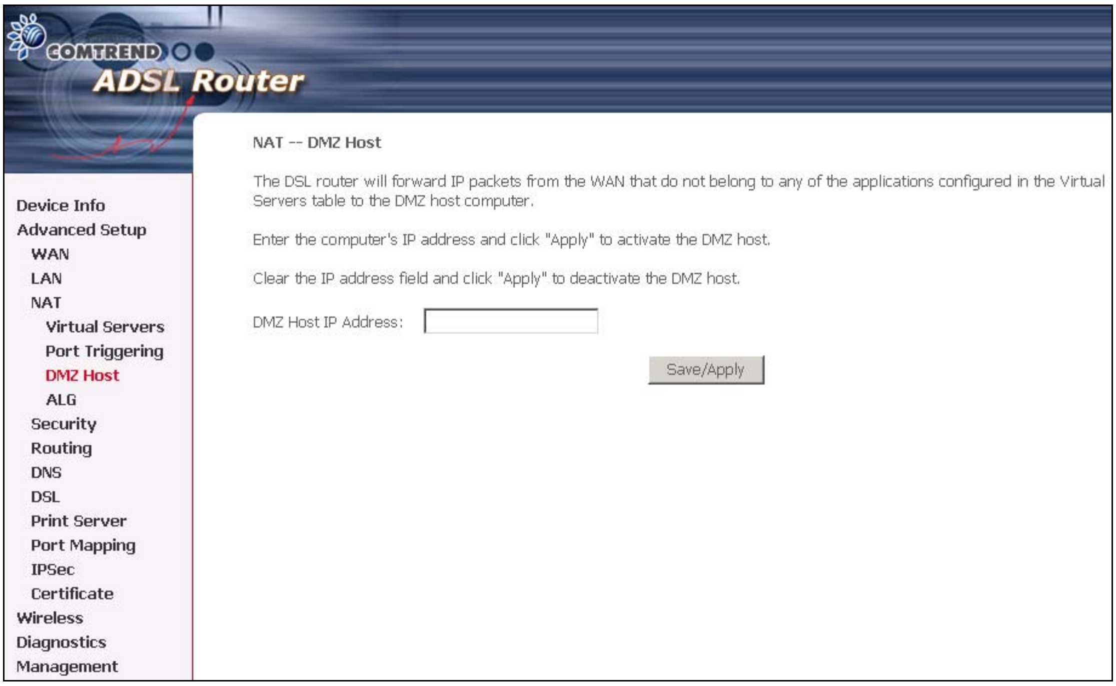
○ Custom application:

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

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	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

6.3.3 DMZ Host

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



NAT -- DMZ Host

The 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.

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

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

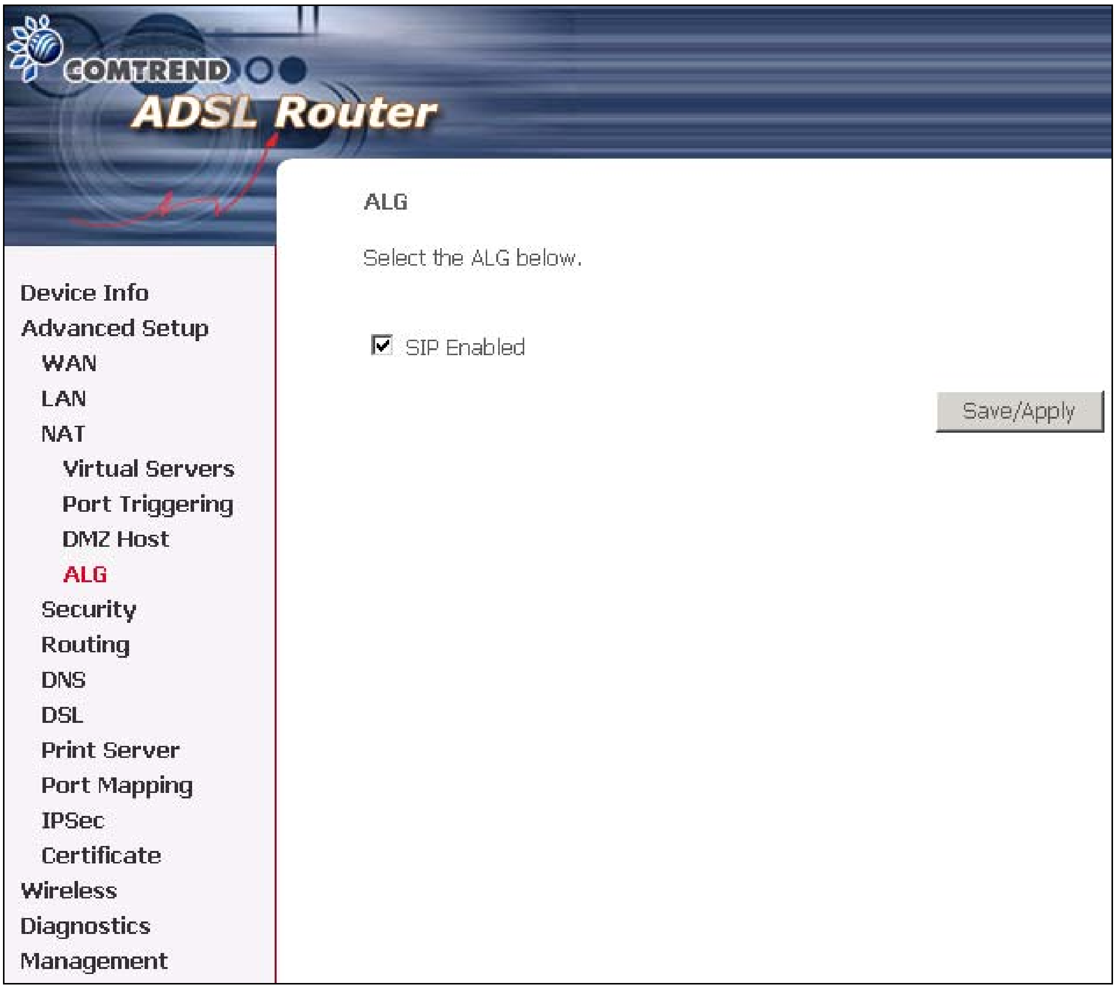
DMZ Host IP Address:

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

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

6.3.4 ALG

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



ALG

Select the ALG below.

☑ SIP Enabled

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

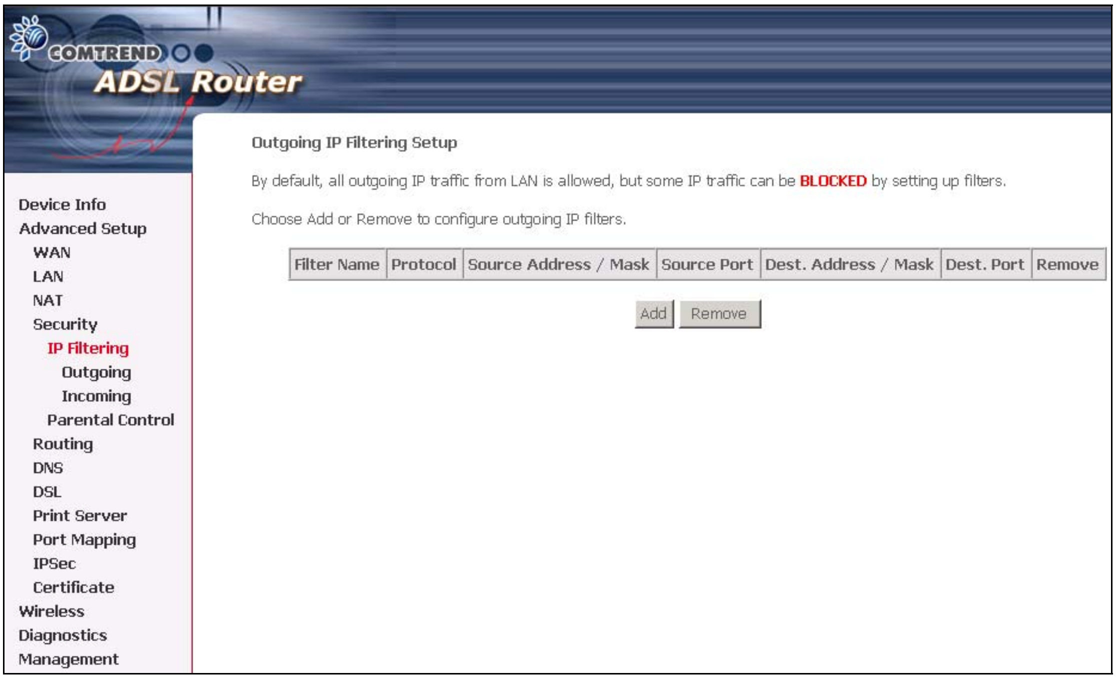
6.4 Security

To display the Security function, you need to enable the firewall feature in the WAN Setup.

6.4.1 IP Filtering

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

Outgoing



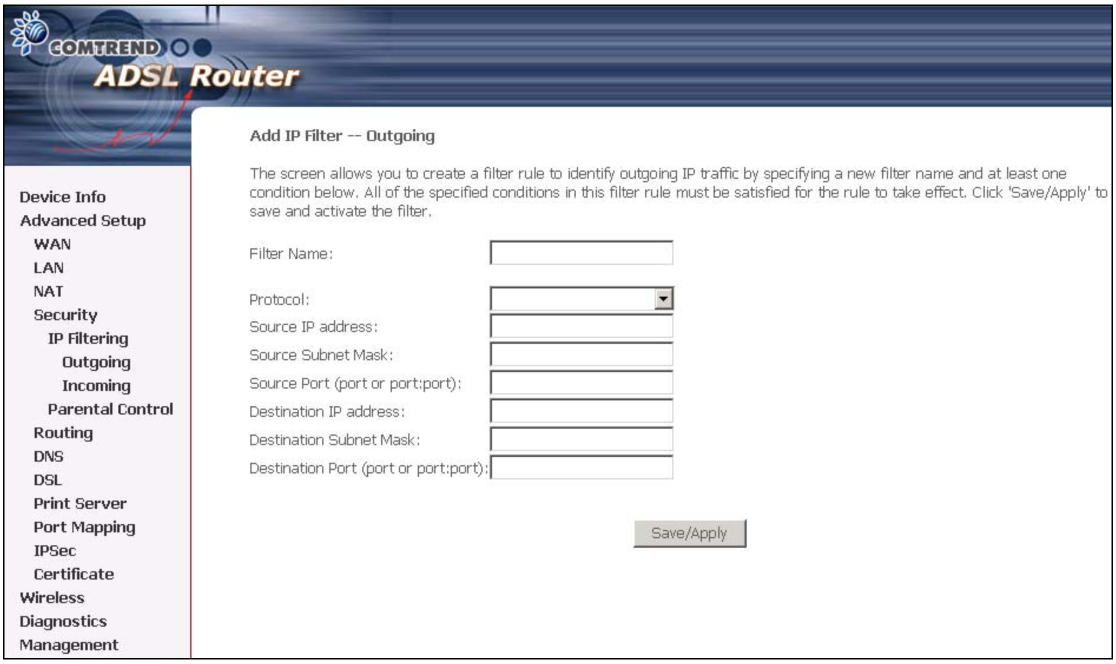
Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, simply click the Add button. The following screen will be displayed.



Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

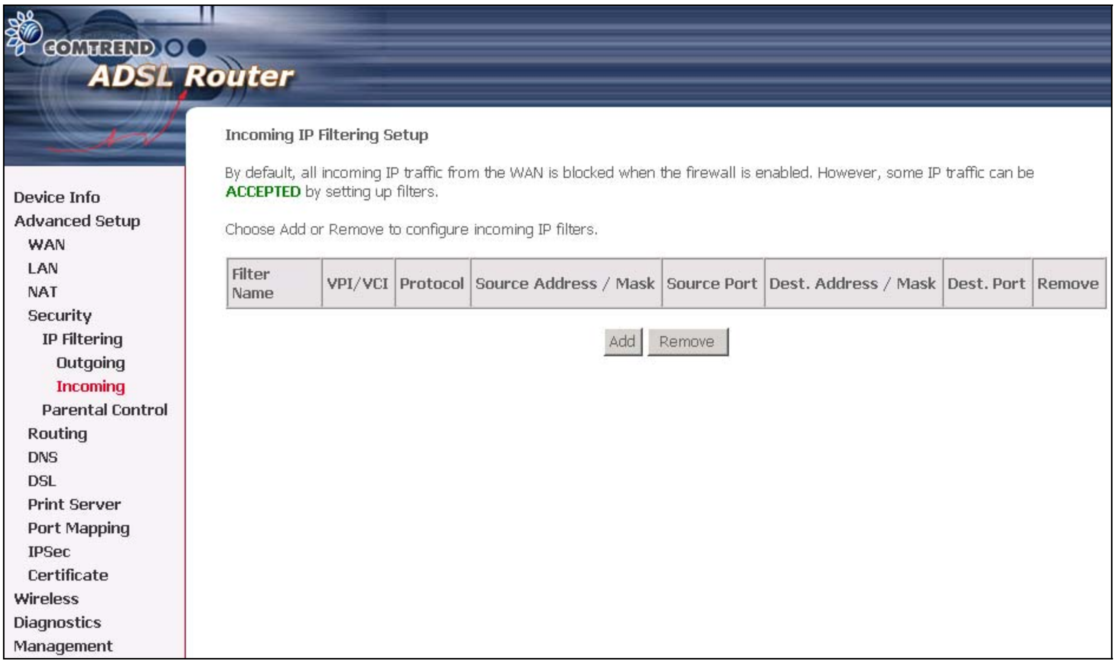
Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Filter Name	Type a name for the filter rule.
Protocol	User can select from: 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.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.

Incoming



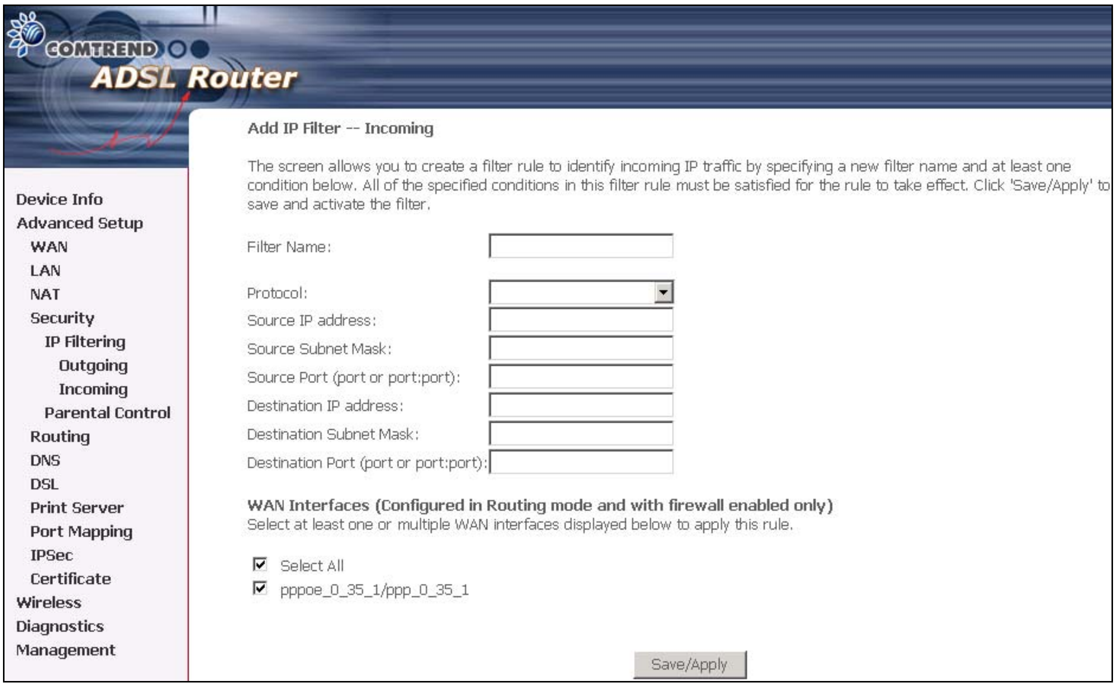
Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, simply click the Add button. The following screen will be displayed.



Add IP Filter -- Incoming

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

Filter Name:	
Protocol:	
Source IP address:	
Source Subnet Mask:	
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

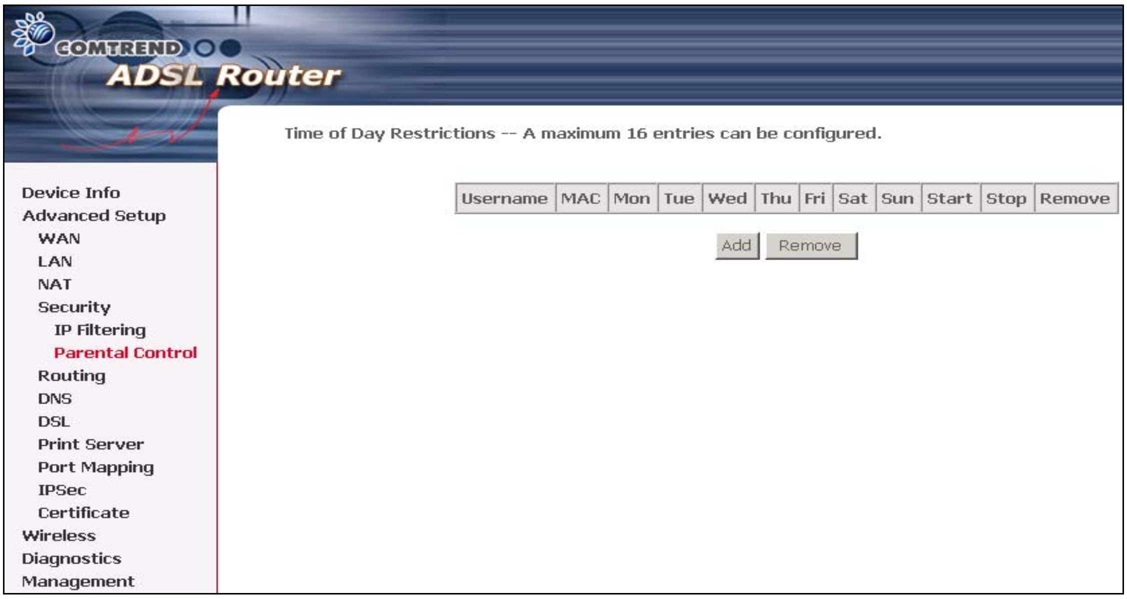
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All
☑ pppoe_0_35_1/ppp_0_35_1

To configure the parameters, please reference **Outgoing** table above.

6.4.2 Parental Control

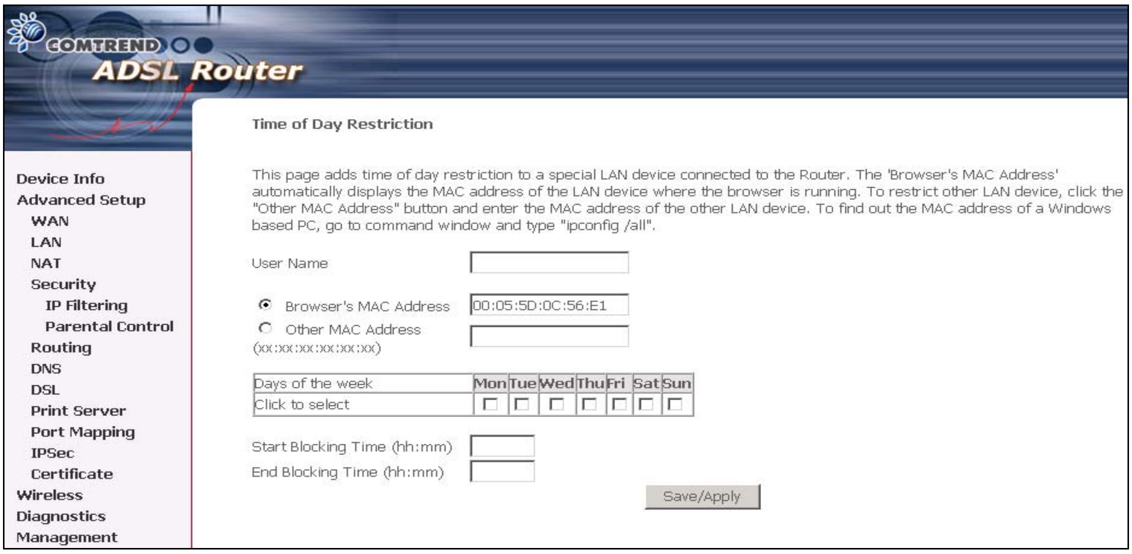
Parental control: allows parents, schools, and libraries to set access times for Internet use.



Time of Day Restrictions -- A maximum 16 entries can be configured.

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

To add a parental control, simply click the Add button. The following screen will be displayed.



Time of Day Restriction

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

User Name

● Browser's MAC Address 00:05:5D:0C:56:E1

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

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

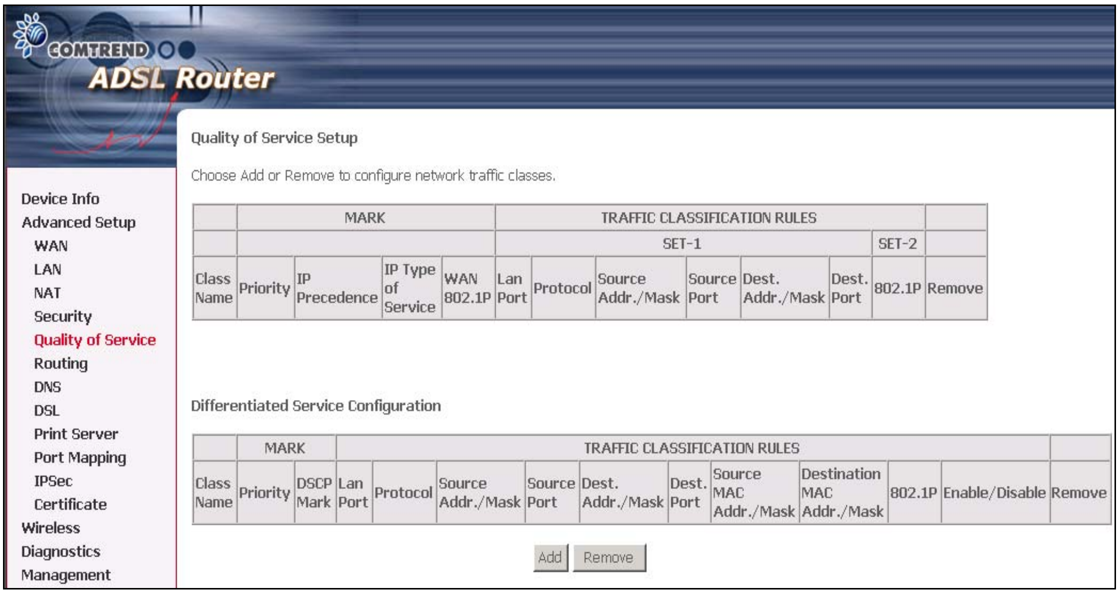
Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Username:	Input Internet access user name
MAC:	Set the MAC address to access the Internet
Mon, Tue, Wed, Thu, Fri, Sat, Sun:	Set which days that will have block restrictions to Internet access
Start, End Blocking Time:	Set Internet block start and stop time

6.5 Quality of Service

To display the QoS function, you need to enable the QoS feature in the WAN Setup.



Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

	MARK				TRAFFIC CLASSIFICATION RULES							
					SET-1						SET-2	
Class Name	Priority	IP Precedence	IP Type of Service	WAN 802.1P	Lan Port	Protocol	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	802.1P	Remove

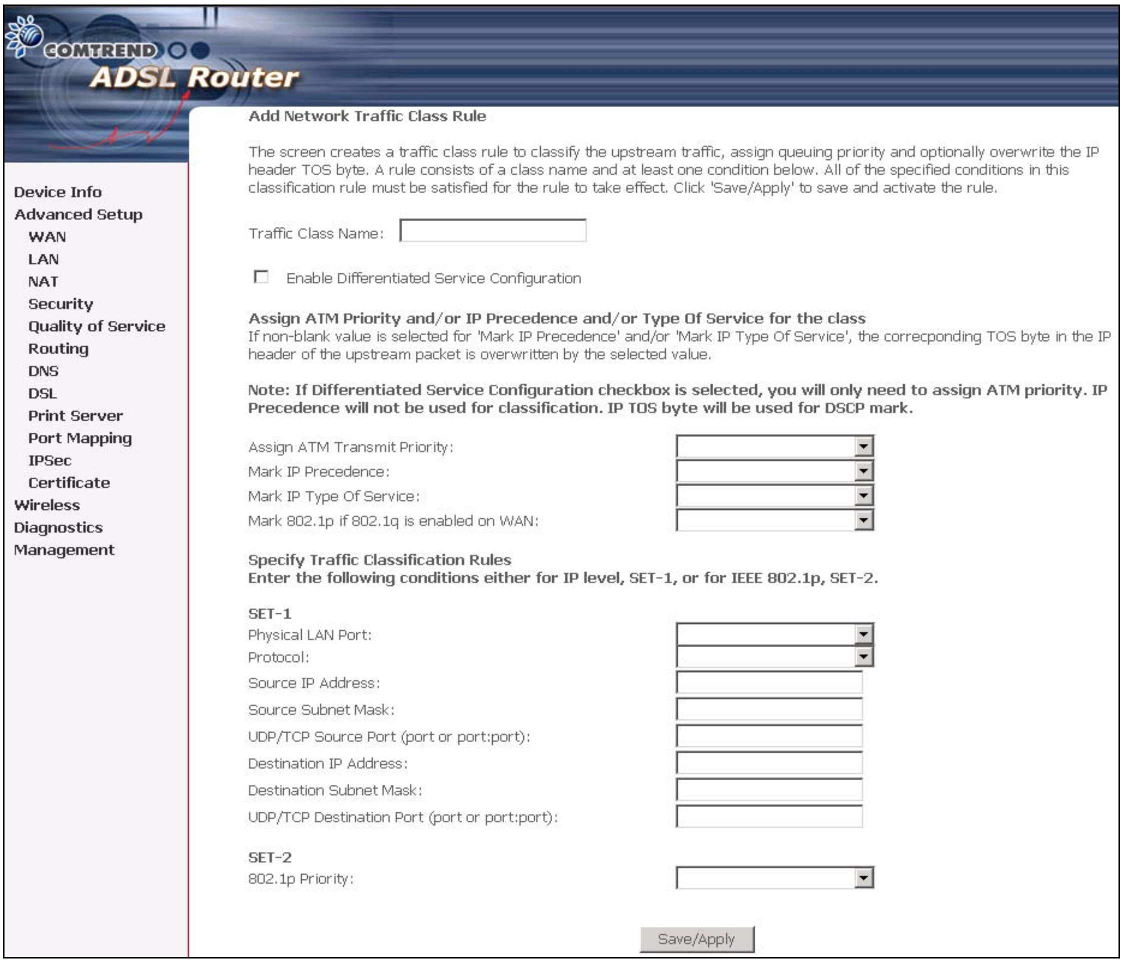
Differentiated Service Configuration

	MARK		TRAFFIC CLASSIFICATION RULES									
Class Name	Priority	DSCP Mark	Lan Port	Protocol	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Enable/Disable	Remove

Choose Add to configure network traffic classes.

The following screen will be displayed:

See below



Add Network Traffic Class Rule

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

Traffic Class Name:

□ Enable Differentiated Service Configuration

Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.

Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.

Assign ATM Transmit Priority:
Mark IP Precedence:
Mark IP Type Of Service:
Mark 802.1p if 802.1q is enabled on WAN:

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

SET-1
Physical LAN Port:
Protocol:
Source IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):

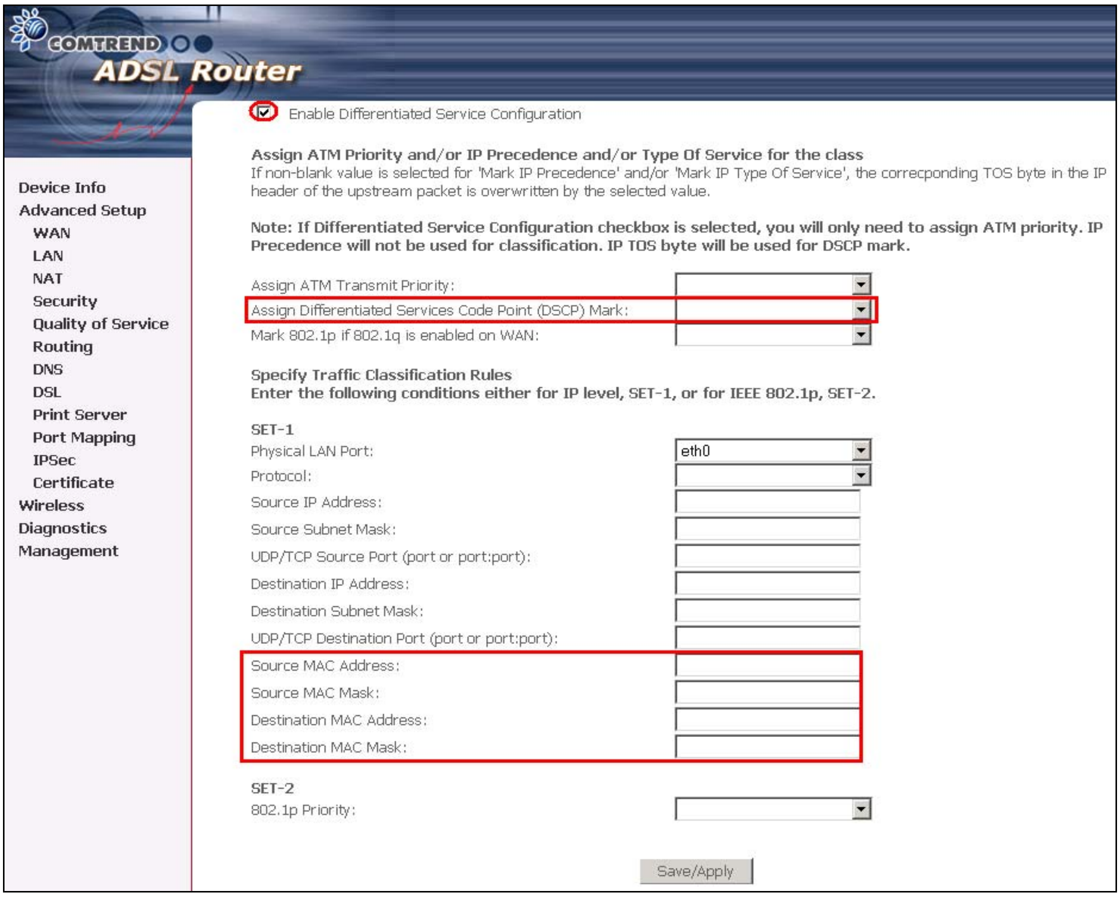
SET-2
802.1p Priority:

The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.	
Traffic Class Name	Enter name for traffic class.
Enable Differentiated Service Configuration	Enable Differentiated Service Configuration if required.

Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value. **Note:** If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value. **Note:** If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.
Assign Differentiated Services Code Point (DSCP) Mark	Choose the required DSCP value. Default value is "000000".
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7.
Specify Traffic Classification Rules Enter the following conditions either for physical LAN/Wireless port or for IP level, SET-1, or for IEEE 802.1p, SET-2	
SET-1	
Physical LAN Port	User can select from: ENET, ENET(1-4), USB, Wireless or Wireless_Guest.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.

Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
SET-2	
802.1p Priority	Select between 0-7.
Traffic Class Name	Enter name for traffic class
Priority	Select Low, Medium or High.
IP Precedence	Select between 0-7. The lower the digit shows the higher the priority
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Physical LAN Port	User can select from: ENET, ENET(1-4), USB, Wireless or Wireless_Guest.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number.
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

If the **Enable Differentiated Service Configuration** box is ticked (i.e. selected) the following screen will be displayed:



☑ Enable Differentiated Service Configuration

Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class
If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.

Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.

Assign ATM Transmit Priority:	
Assign Differentiated Services Code Point (DSCP) Mark:	
Mark 802.1p if 802.1q is enabled on WAN:	

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

SET-1

Physical LAN Port:	eth0
Protocol:	
Source IP Address:	
Source Subnet Mask:	
UDP/TCP Source Port (port or port:port):	
Destination IP Address:	
Destination Subnet Mask:	
UDP/TCP Destination Port (port or port:port):	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

SET-2

802.1p Priority:	

The additional Items are explained here.

Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
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.

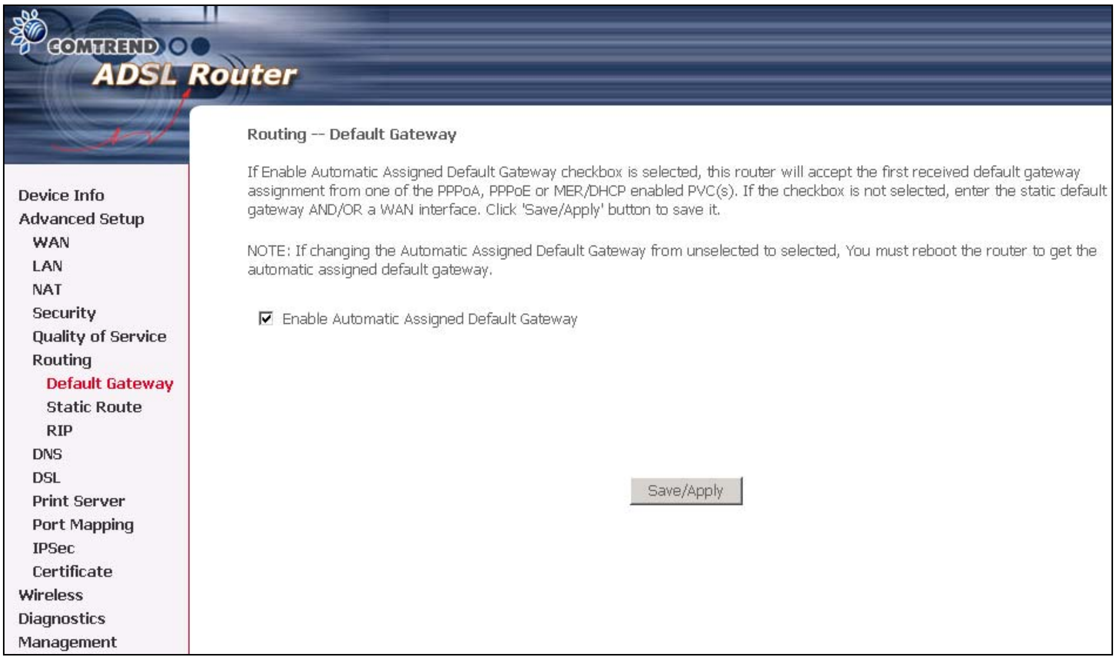
6.6 Routing

The Routing dialog box allows you to configure Default gateway, Static Route and RIP.

6.6.1 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: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.



Routing -- Default Gateway

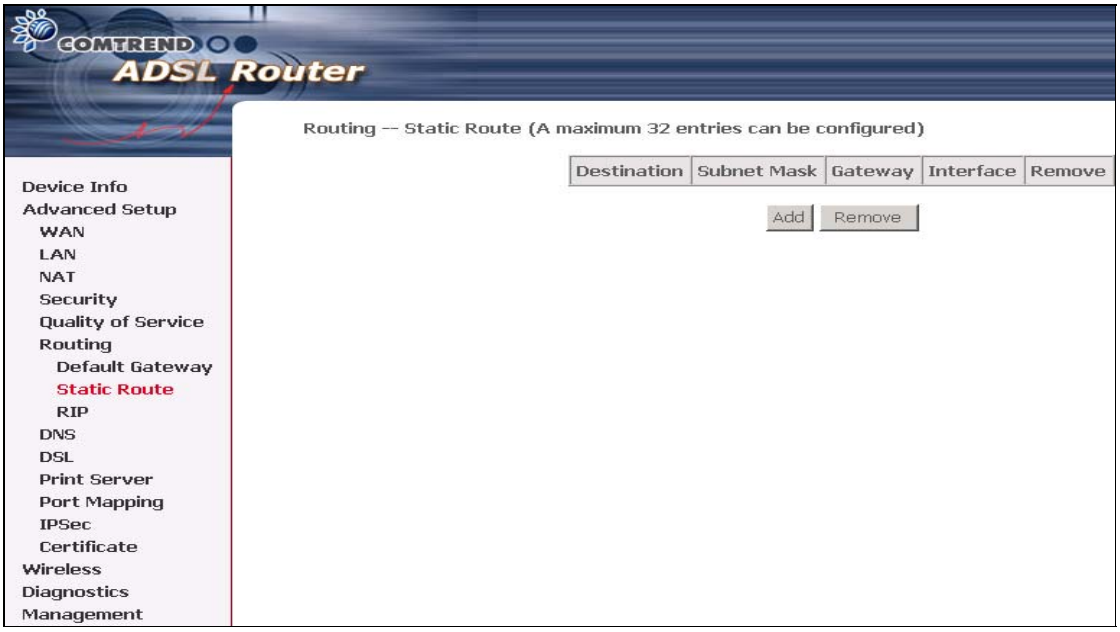
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

6.6.2 Static Route

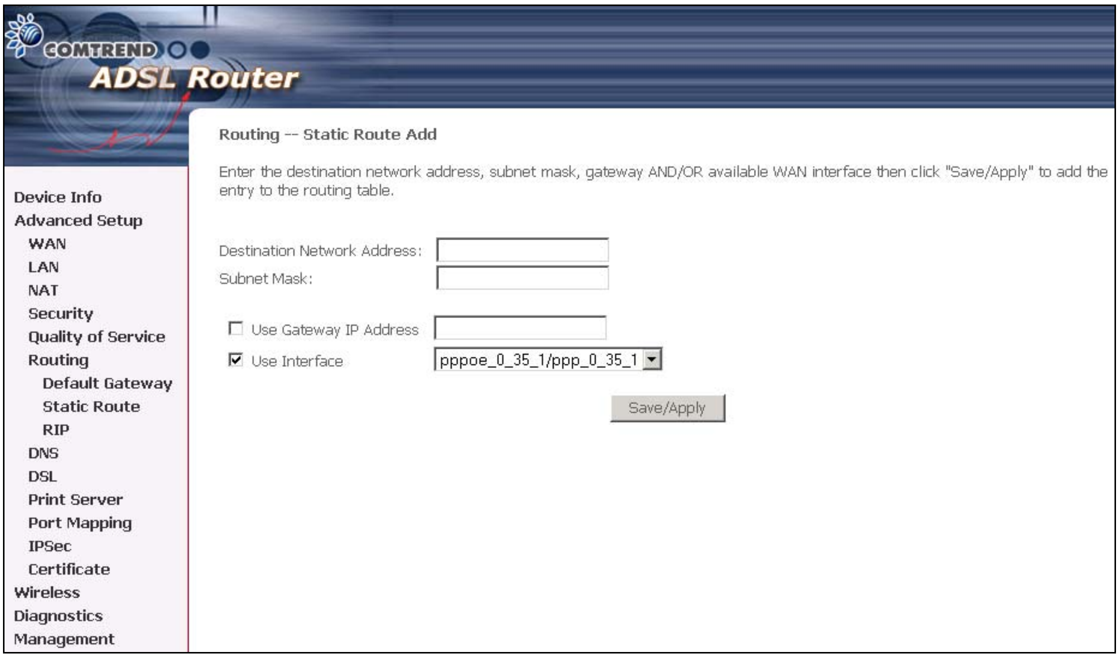
Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.



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

Destination	Subnet Mask	Gateway	Interface	Remove

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.



Routing -- Static Route Add

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

Destination Network Address:

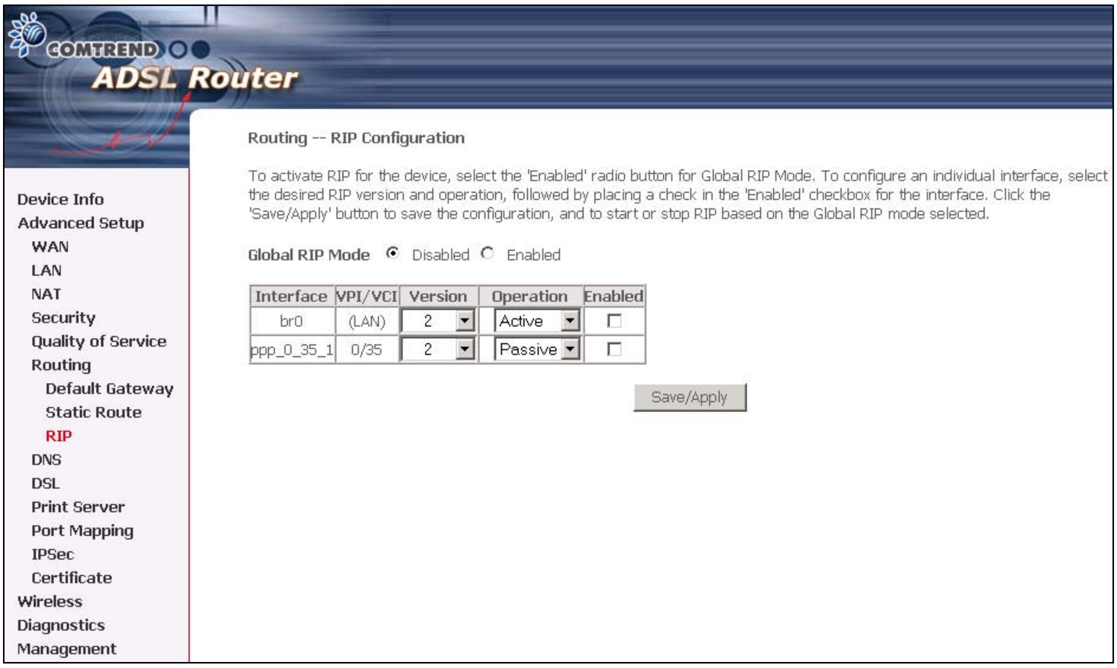
Subnet Mask:

☐ Use Gateway IP Address

☑ Use Interface pppoe_0_35_1/ppp_0_35_1

6.6.3 RIP

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



Routing -- RIP Configuration

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

Global RIP Mode ● Disabled ○ Enabled

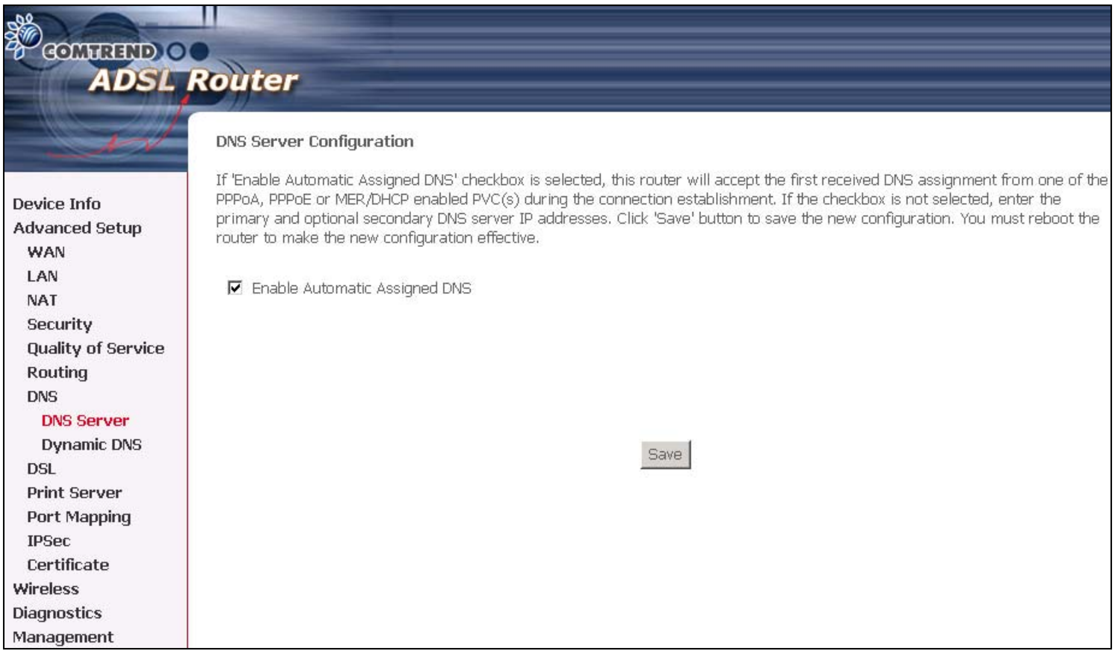
Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	□
ppp_0_35_1	0/35	2	Passive	□

Note: This screenshot is based on PPPoE encapsulation.

6.7 DNS

6.7.1 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.



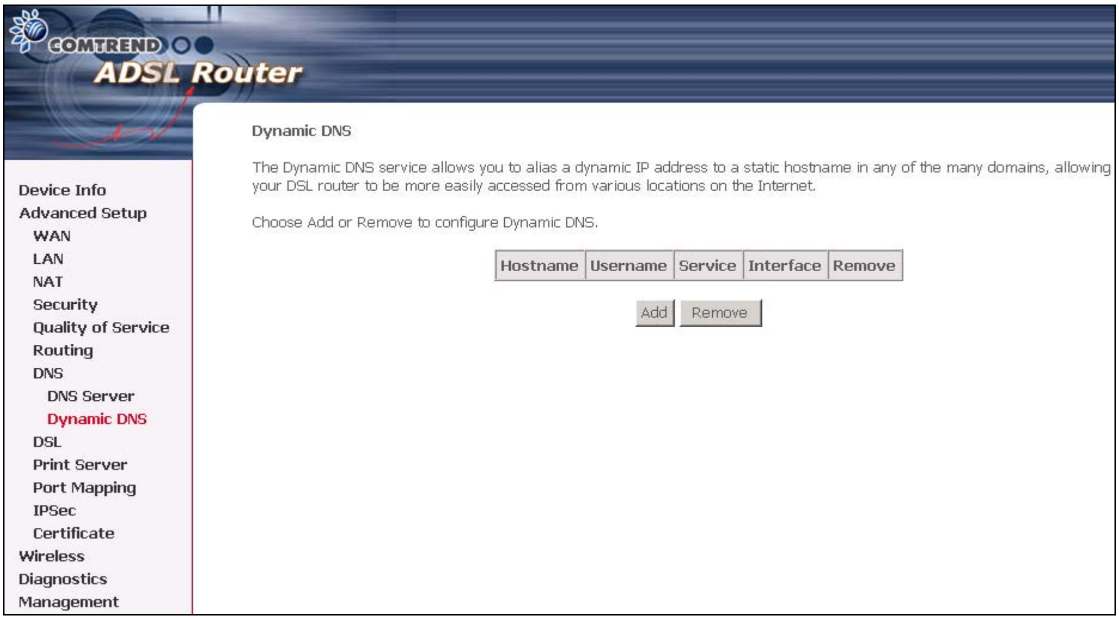
DNS Server Configuration

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.

☑ Enable Automatic Assigned DNS

6.7.2 Dynamic DNS

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



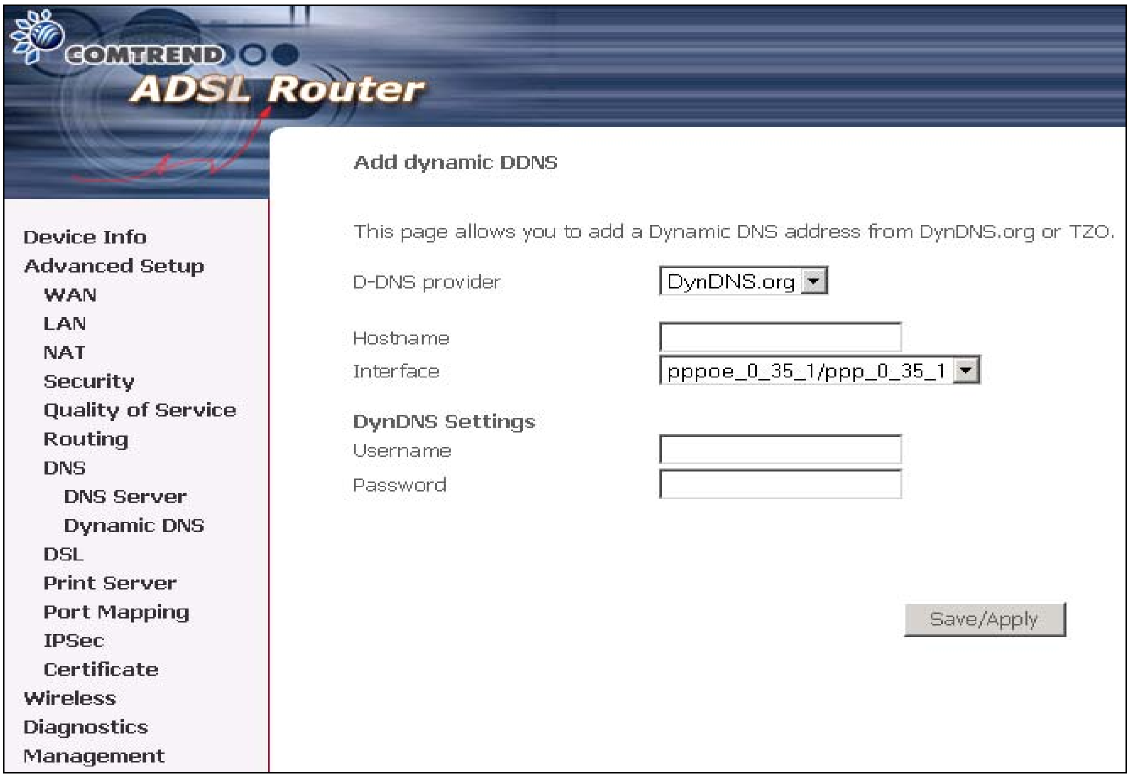
Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

To add a dynamic DNS service, simply click the Add button. The following screen will be displayed:



Add dynamic DDNS

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

D-DNS provider DynDNS.org

Hostname

Interface pppoe_0_35_1/ppp_0_35_1

DynDNS Settings

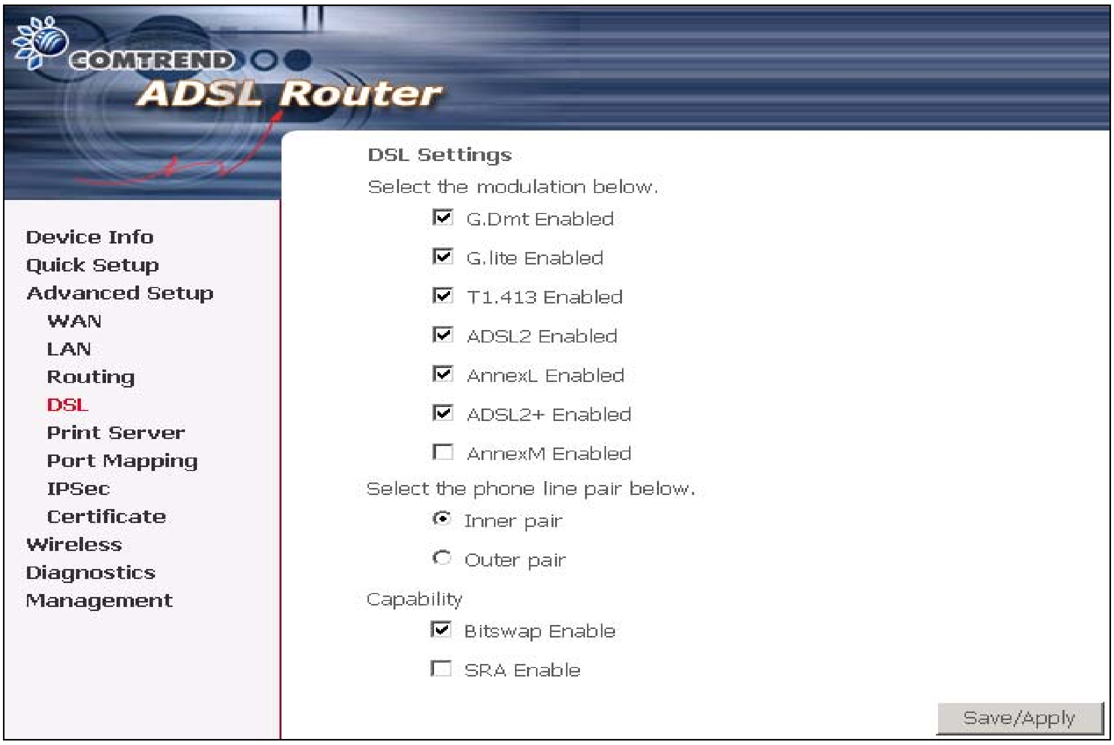
Username

Password

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

6.8 DSL

To access the DSL settings, first click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

□ AnnexM Enabled

Select the phone line pair below.

● Inner pair

○ Outer pair

Capability

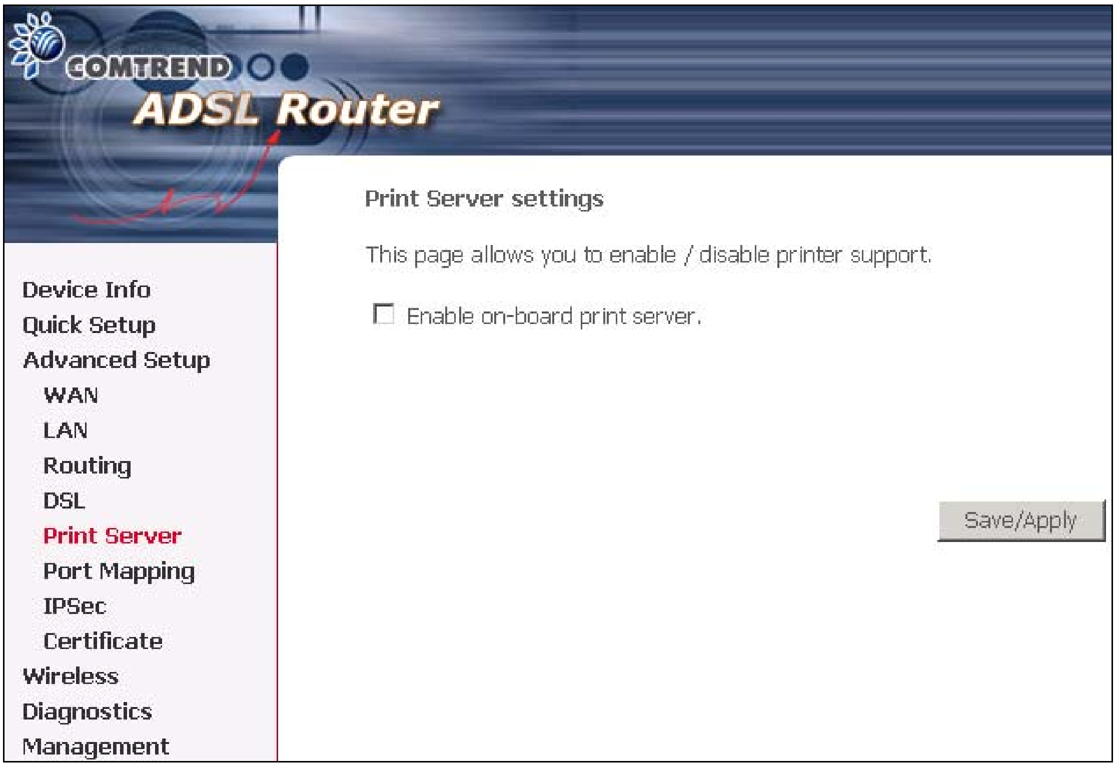
☑ Bitswap Enable

□ SRA Enable

Option	**Description**
Auto Mode (G.dmt, G.lite or T1.413)	Sets the system auto-sense between G.Dmt, G.lite, or T1.413
G.dmt/G.lite	Sets G.Dmt/G.lite if you want the system to use either G.Dmt or G.lite mode.
T1.413	Sets the T1.413 if you want the system to use only T1.413 mode.
ADSL2 Enabled	The device can support the functions of the ADSL2.
AnnexL Enabled	The device can support/enhance the long loop test.
ADSL2+ Enabled	The device can support the functions of the ADSL2+.
AnnexM	Covers a higher “upstream” data rate version, by making use of some of the downstream channels.
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswaping function
SRA Enable	Allows seamless rate adaptation

6.9 Print Server

The CT-5372 is equipped with one high-speed USB2.0 host connection.
With software support, users can connect USB devices such as a printer and hard disc to the CT-5372. For this software release, printer server is supported.



Print Server settings

This page allows you to enable / disable printer support.

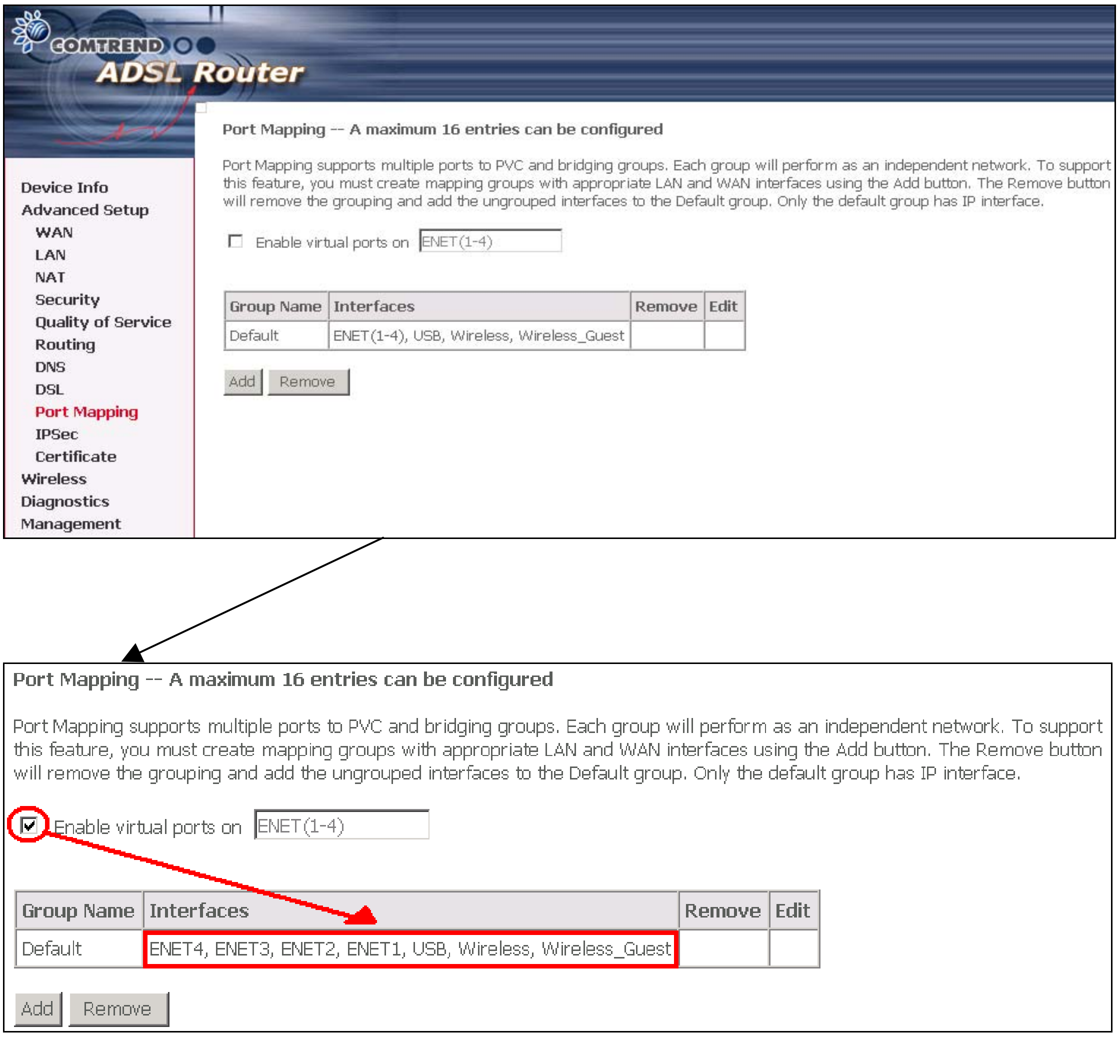
☐ Enable on-board print server.

Please refer to Appendix A for an Example.

6.10 Port Mapping

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.



Port Mapping -- A maximum 16 entries can be configured

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

☐ Enable virtual ports on ENET(1-4)

Group Name	Interfaces	Remove	Edit
Default	ENET(1-4), USB, Wireless, Wireless_Guest		

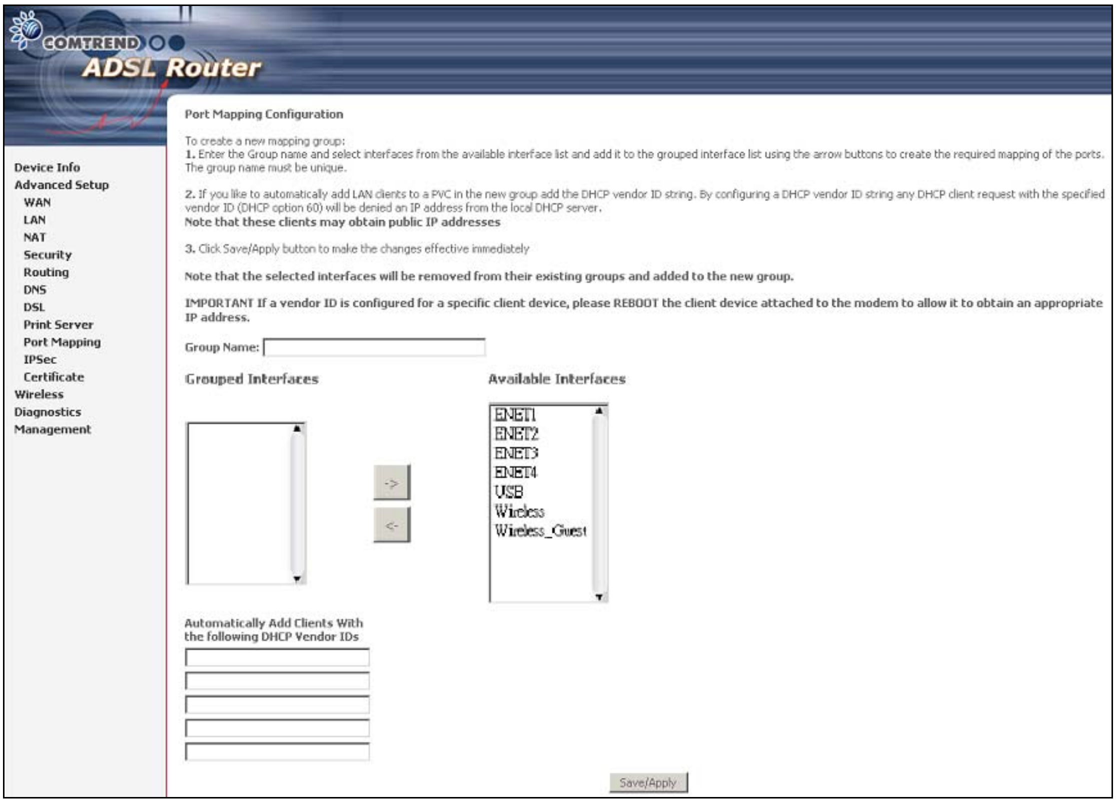
Port Mapping -- A maximum 16 entries can be configured

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

☑ Enable virtual ports on ENET(1-4)

Group Name	Interfaces	Remove	Edit
Default	ENET4, ENET3, ENET2, ENET1, USB, Wireless, Wireless_Guest		

To add a port mapping group, simply click the Add button.



Port Mapping Configuration

To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses

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

Note that the selected interfaces will be removed from their existing groups and added to the new group.

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

Group Name:

Grouped Interfaces

Available Interfaces
ENET1
ENET2
ENET3
ENET4
USB
Wireless
Wireless_Guest

Automatically Add Clients With the following DHCP Vendor IDs

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

Automatically Add Clients With the Following DHCP Vendor IDs:
Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video).
The Lan interfaces are ETH1, ETH2, ETH3, ETH4, Wireless and USB.
Port mapping configuration are:
1. Default : ENET1, ENET2, ENET3, ENET4, Wireless, Wireless_Guest and USB.
2. Video: nas_0_36, nas_0_37 and nas_0_38. The DHCP vendor ID is "Video".

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

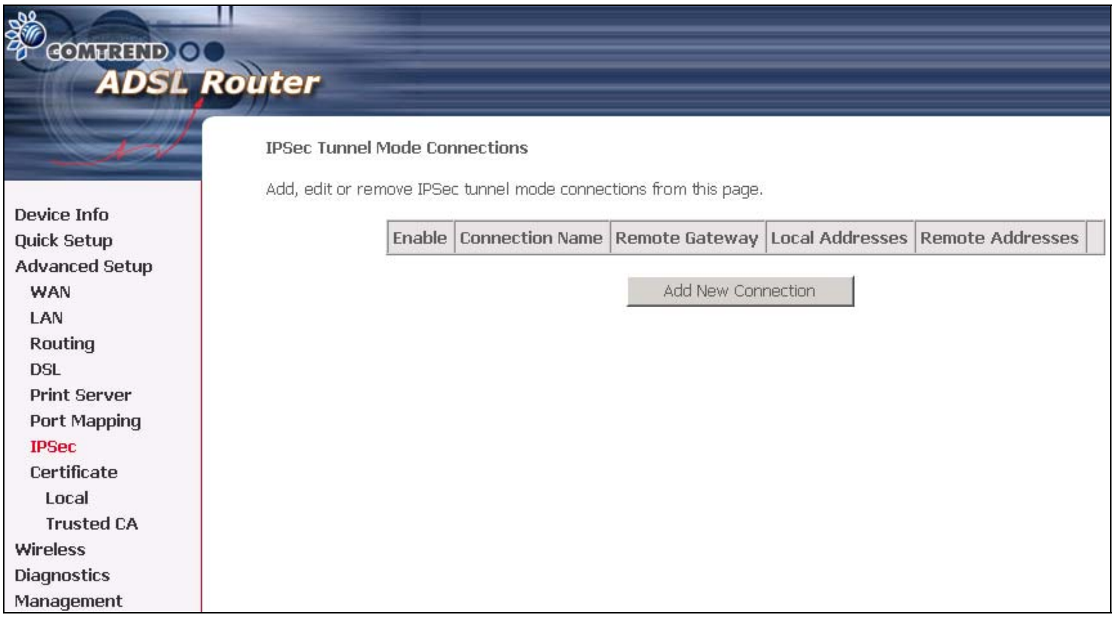
If the setup-box was connected with interface "ENET1" and send a dhcp request with vendor id "Video", CPE's dhcp server will forward this request to ISP's dhcp server.

And CPE will change the portmapping configuration automatically. The portmapping configuration will become:

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

6.11 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page. By clicking Add New Connection, you can add a new IPSec termination rule.

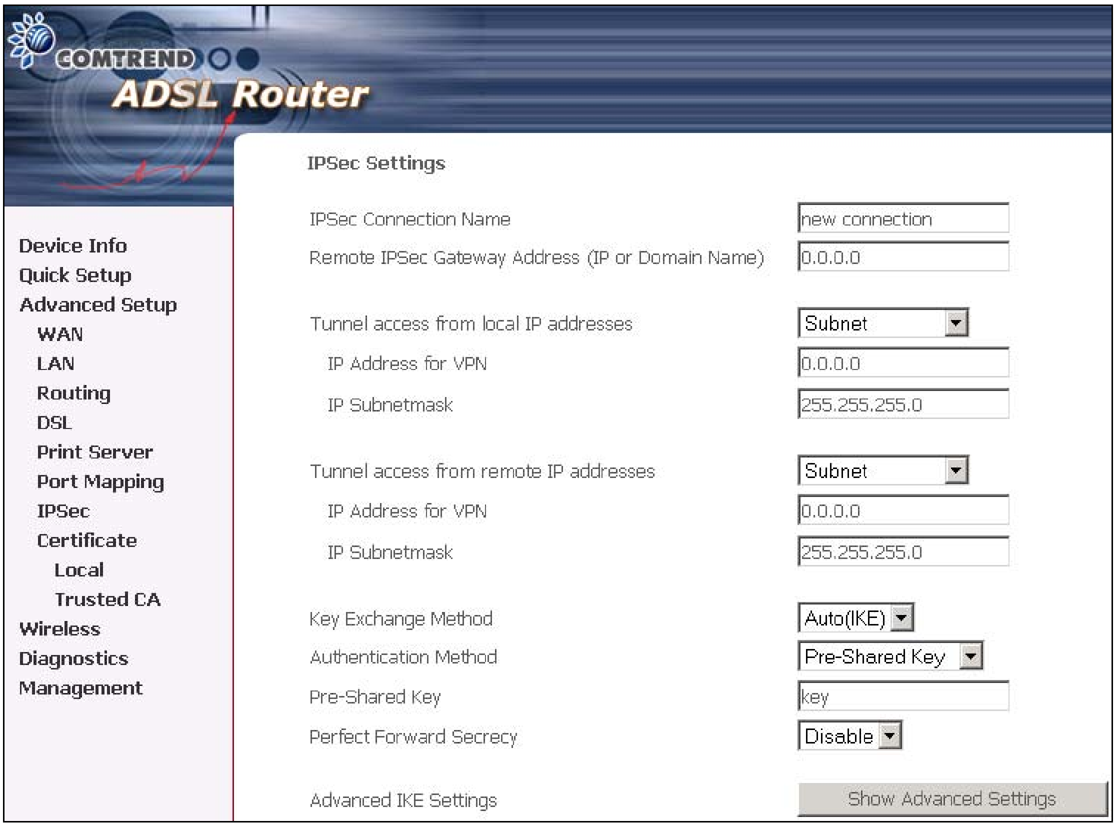


IPSec Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses

The following screen will be displayed.

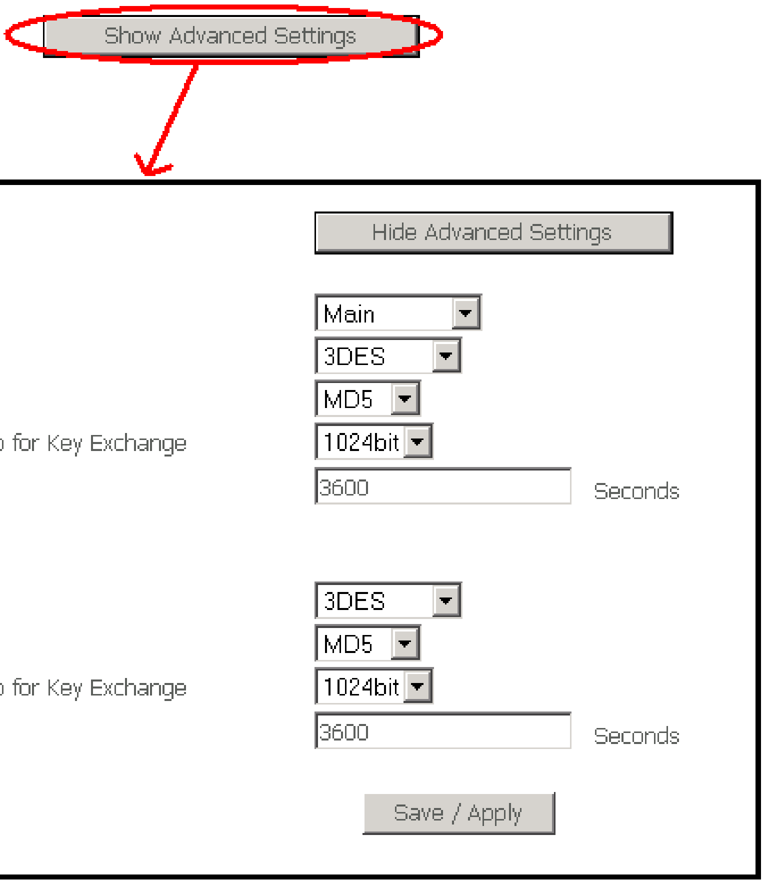


IPSec Settings

IPSec Connection Name	new connection
Remote IPSec Gateway Address (IP or Domain Name)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

IPSec Connection Name	User-defined label
Remote IPSec Gateway Address (IP or Domain Name)	The IP address of remote tunnel Gateway, and you can use numeric address and domain name
Tunnel access from local IP addresses	It chooses methods that specify the acceptable host IP on the local side. It has single and subnet.
IP Address for VPN	If you choose "single", please entry the host IP address for VPN. If you choose "subnet", please entry the subnet information for VPN.
Tunnel access from remote IP addresses	It chooses methods that specify the acceptable host IP on the remote side. It has single and subnet.
IP Address for VPN	If you choose "single", please input the host IP address for VPN. If you choose "subnet", please input the subnet information for VPN.
Key Exchange Method	It has two modes. One is auto and the other is manual.
Authentication Method	It has either pre-shared key or x.509.
Pre-Shared Key	Input Pre-shared key
Perfect Forward Secrecy	Enable/disable the method that is Perfect Forward Secrecy.
Advanced IKE Settings	On IPSec Auto mode, you need to choose the setting of two phases. Click the button then choose which modes, Encryption Algorithm, Integrity Algorithm, Select Diffie-Hellman Group for Key Exchange, key time on different phases.

The following is displayed if the **Show Advanced Settings** button is clicked.



Advanced IKE Settings

Phase 1

Mode: Main

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Phase 2

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

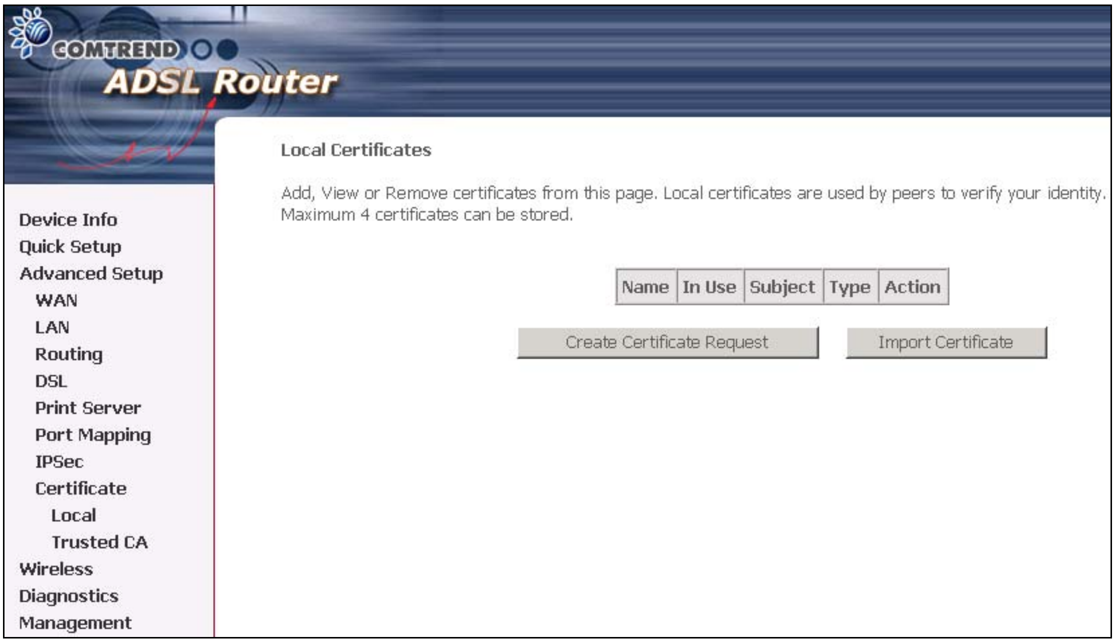
Advanced IKE Settings

Phase 1	
Mode	Defines the exchange mode for phase 1 when racoon is the initiator. It also means the acceptable exchange mode when racoon is responder. The first exchange mode is what racoon uses when it is the initiator.
Encryption Algorithm	Specify the encryption algorithm used for the phase 1 negotiation. This directive must be defined. *Algorithm* is one of following: **des**, **3des**, **aes-128(192, 256)** for Oakley.
Integrity Algorithm	Define the hash algorithm used for the phase 1. *Algorithm* is one of following: **md5, sha1** for Oakley.

Select Diffie-Hellman Group for Key Exchange	Define the group used for the Diffie-Hellman exponentiations. This directive must be defined. *group* is one of following: **modp768**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144**, **modp8192.** When you want to use aggressive mode, you must define the same DH group in each proposal.
Key Life Time	Define lifetime of the phase 1 SA proposal.
Phase 2	
Encryption Algorithm	Specify the encryption algorithm used for the phase 2 negotiation. This directive must be defined. A*lgorithm* is one of following: **des**, **3des**, **aes-128(192, 256)** for Oakley
Integrity Algorithm	Define the hash algorithm used for the phase 2. A*lgorithm* is one of following: **md5, sha1** for Oakley
Select Diffie-Hellman Group for Key Exchange	Define the group of Diffie-Hellman exponentiations. If you do not require PFS then you can omit this directive. Any proposal will be accepted if you do not specify one.
Key Life Time	Define how long an IPsec-SA will be used, in time units. Any proposal will be accepted, and no attribute(s) will be proposed to the peer if you do not specify it(them).

6.12 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 on the certificate, indicating that these signers have verified that the owner information of this certificate is correct.

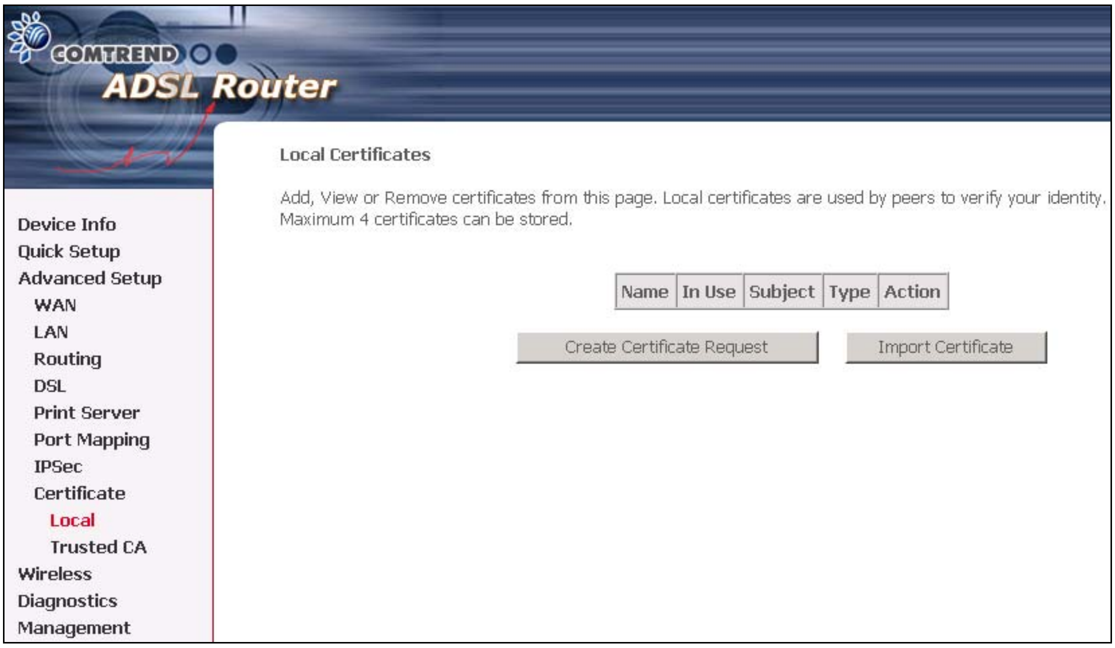


Local Certificates

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

Name	In Use	Subject	Type	Action

6.12.1 Local



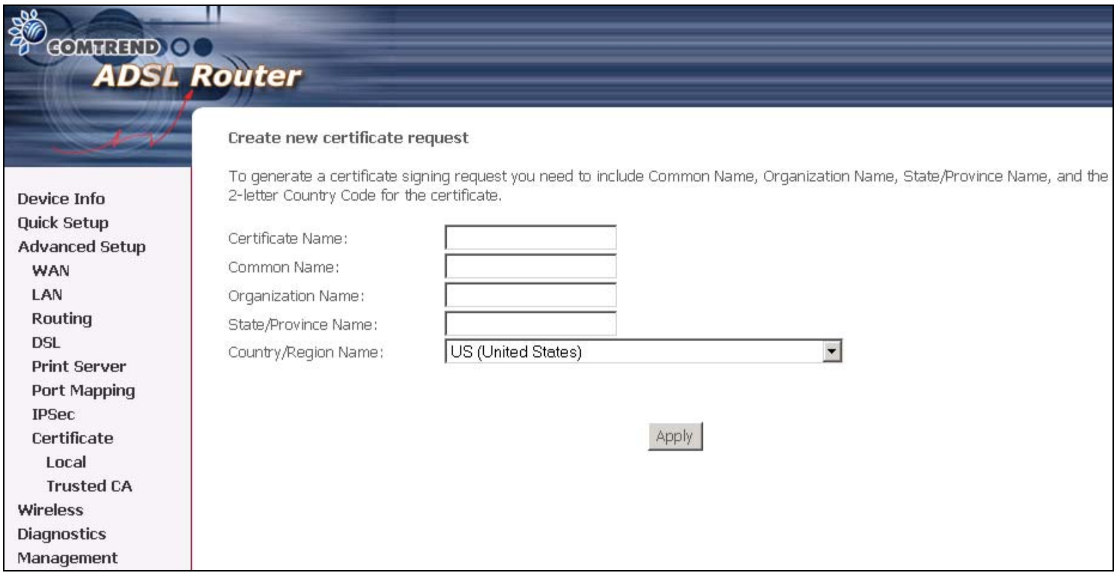
Local Certificates

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

Name	In Use	Subject	Type	Action

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. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.

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



Create new certificate request

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

Certificate Name:

Common Name:

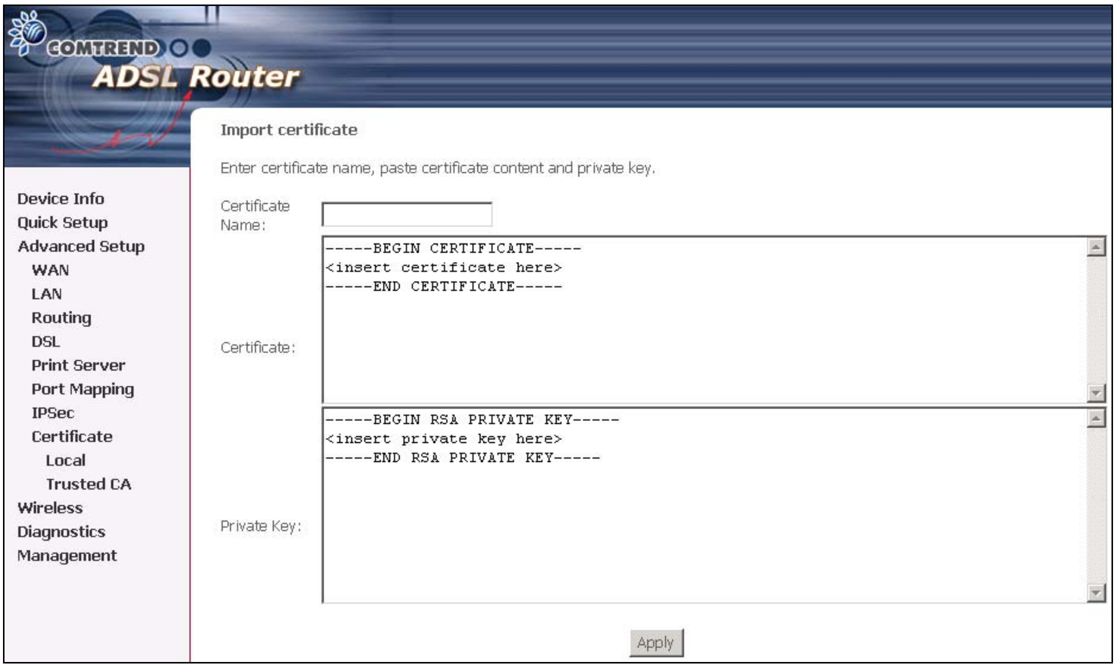
Organization Name:

State/Province Name:

Country/Region Name: US (United States)

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

This page is used to paste the certificate content and the private key provided by your vendor/ISP/ITSP.



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

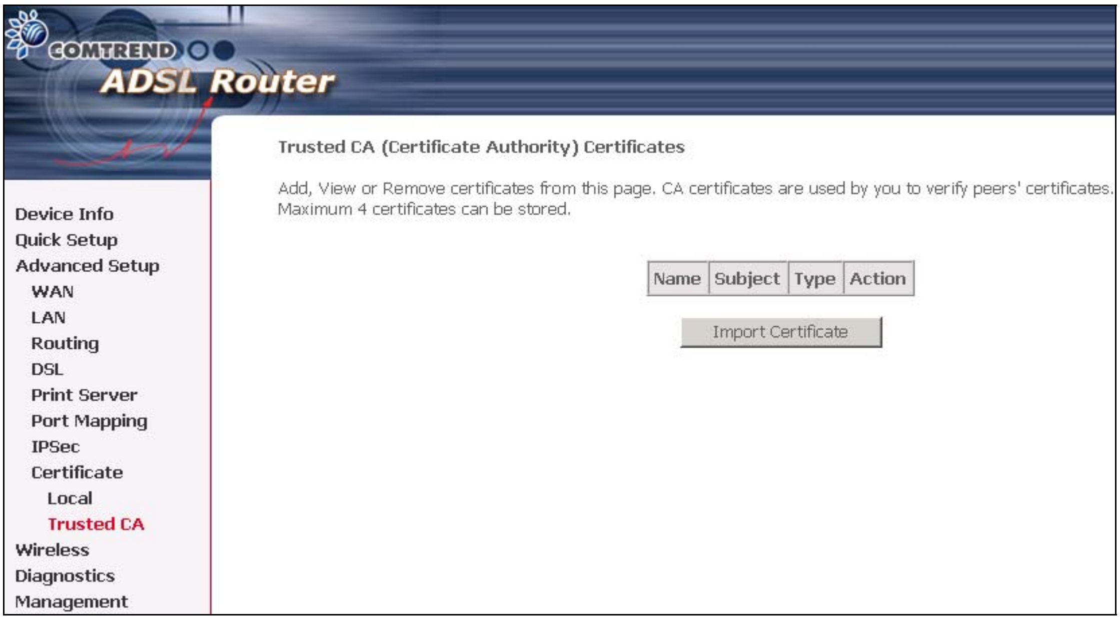
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

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

6.12.2 Trusted CA

CA is the abbreviation for Certificate Authority. CA 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 to do encryption/decryption. Its purpose is to sign and issue certificates; in order to prove the owner information of that certificate is correct.

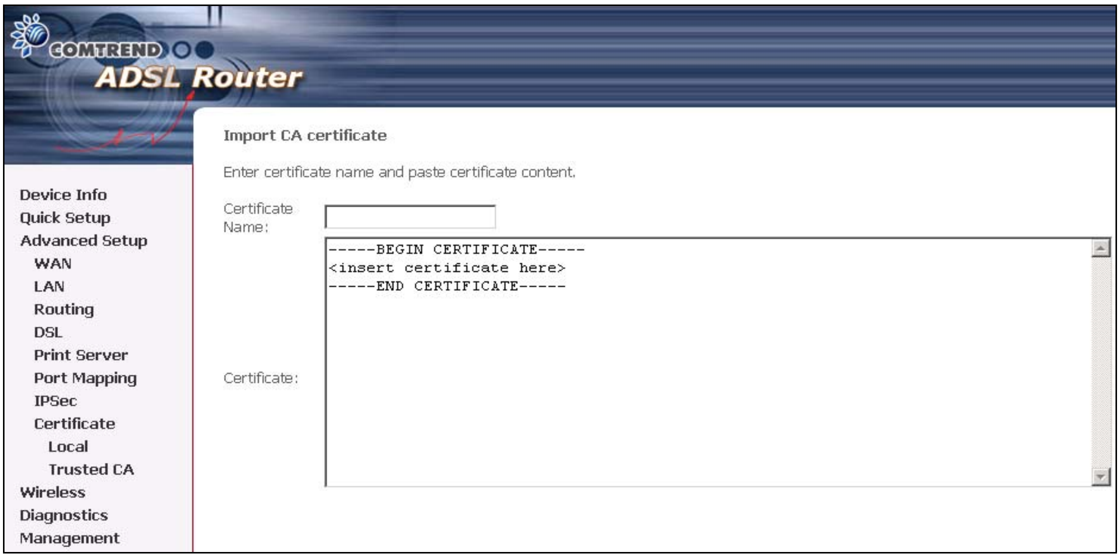


Trusted CA (Certificate Authority) Certificates

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

Name	Subject	Type	Action

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



Import CA certificate

Enter certificate name and paste certificate content.

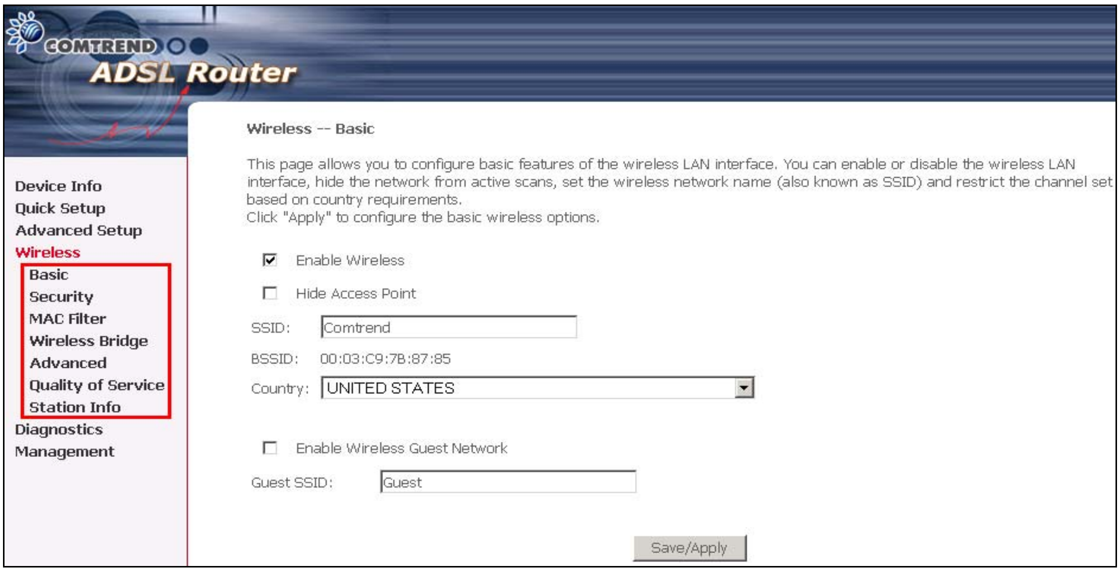
Certificate Name:

Certificate:

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

Chapter 7 Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

SSID: Comtrend

BSSID: 00:03:C9:7B:87:85

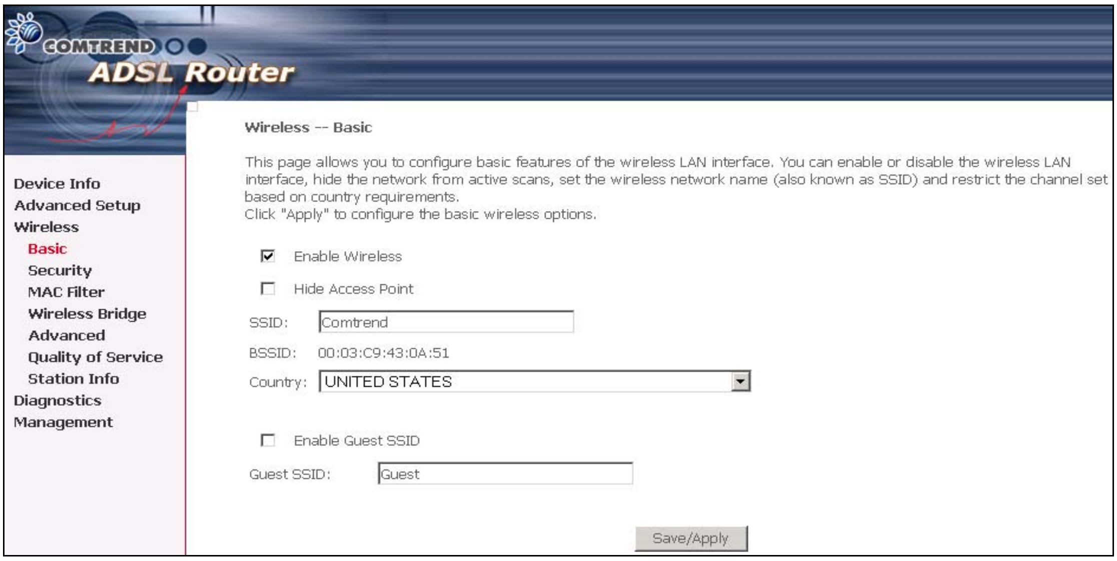
Country: UNITED STATES

□ Enable Wireless Guest Network

Guest SSID: Guest

7.1 Wireless Basic Screen

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



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

SSID: Comtrend

BSSID: 00:03:C9:43:0A:51

Country: UNITED STATES

□ Enable Guest SSID

Guest SSID: Guest

Option	**Description**
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect ADSL router access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: ● US= worldwide ● Japan=1-14 ● Jordan= 10-13 ● Israel= 1-13
Enable Guest SSID	CT-5372 supports multiple SSIDs. Guest SSID is not visible. The wireless hosts are able to scan main SSID only.

Guest SSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.

7.1.1 Security

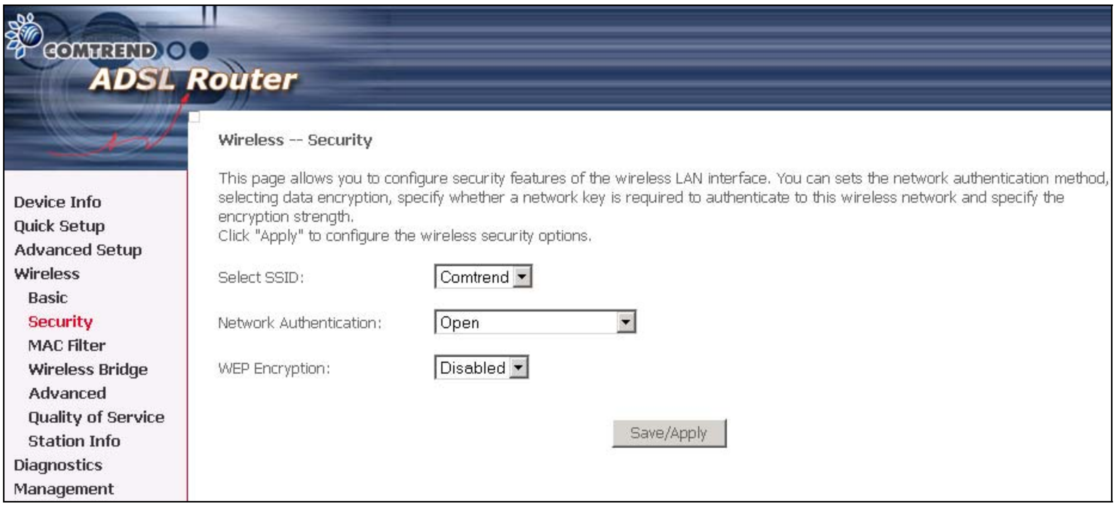
Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption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

802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

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

The following screen appears when Security is selected. The Security page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click **Apply** to configure the wireless security options.



Wireless -- Security

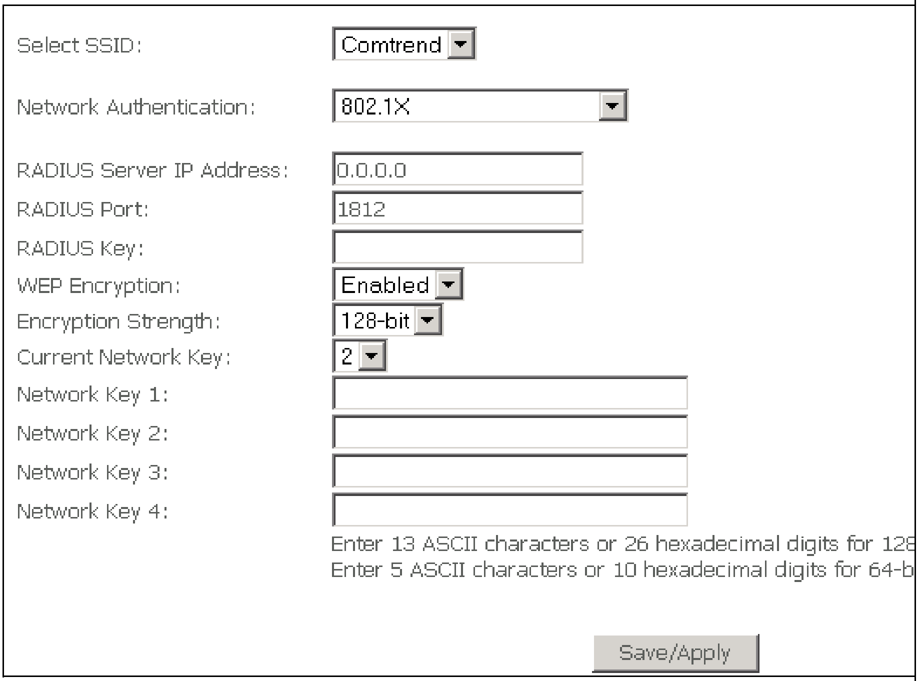
This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

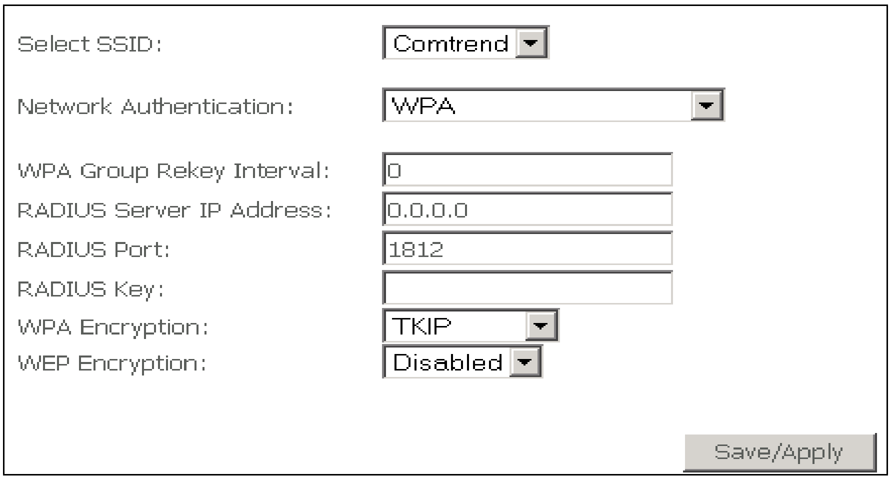
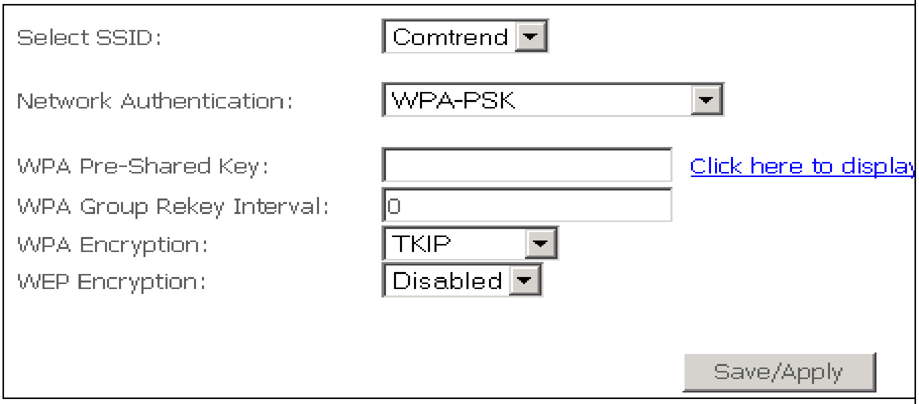
Select SSID: Comtrend

Network Authentication: Open

WEP Encryption: Disabled

Option	Description
Select SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.

Network Authentication	It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications. Different authentication type pops up different settings requests. Choosing **802.1X**, enter RADIUS Server IP address, RADIUS Port, and RADIUS key. Also, enable WEP Encryption and the Encryption Strength. Select SSID: Comtrend Network Authentication: 802.1X RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WEP Encryption: Enabled Encryption Strength: 128-bit Current Network Key: 2 Network Key 1: Network Key 2: Network Key 3: Network Key 4: Enter 13 ASCII characters or 26 hexadecimal digits for 128 Enter 5 ASCII characters or 10 hexadecimal digits for 64-b Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys. Choosing **WPA**, you must enter WPA Group Rekey Interval.

	 Select SSID: Comtrend Network Authentication: WPA WPA Group Rekey Interval: 0 RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WPA Encryption: TKIP WEP Encryption: Disabled Save/Apply Choosing **WPA-PSK**, you must enter WPA Pre-Shared Key and Group Rekey Interval.  Select SSID: Comtrend Network Authentication: WPA-PSK WPA Pre-Shared Key: Click here to display WPA Group Rekey Interval: 0 WPA Encryption: TKIP WEP Encryption: Disabled Save/Apply
WEP Encryption	It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.
Encryption strength	A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-ASCII character or 10-hexadecimal character) or 128 8-bit (13-ASCII character or 26-hexadecimal character) key. If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key. The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.

7.1.2 MAC Filter

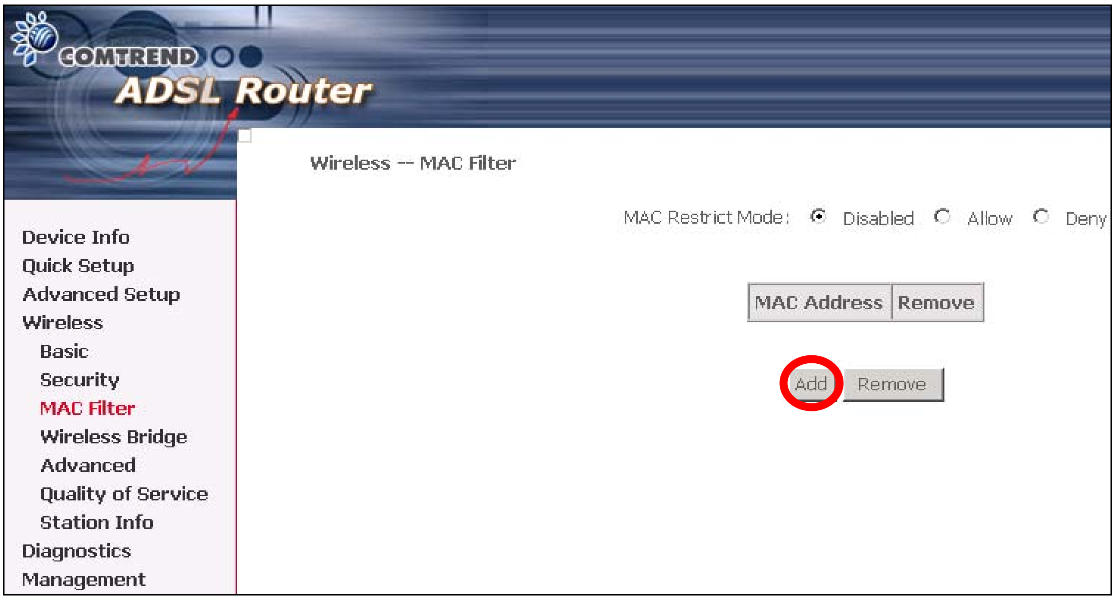
This MAC Filter page allows access to be restricted/allowed based on a MAC address. All NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its "allows" list.

Wi-Fi routers and access points that support MAC filtering let you specify a list of MAC addresses that may connect to the access point, and thus dictate what devices are authorized to access the wireless network. When a device is using MAC filtering, any address not explicitly defined will be denied access.

MAC Restrict mode: **Off**- disables MAC filtering; **Allow** – permits **access** for the specified MAC address; **deny**; reject access of the specified MAC address, then click the **SET** button.

To delete an entry**,** select the entry at the bottom of the screen and then click the **Remove** button, located on the right hand side of the screen.

To add a MAC entry, click **Add** and enter MAC address

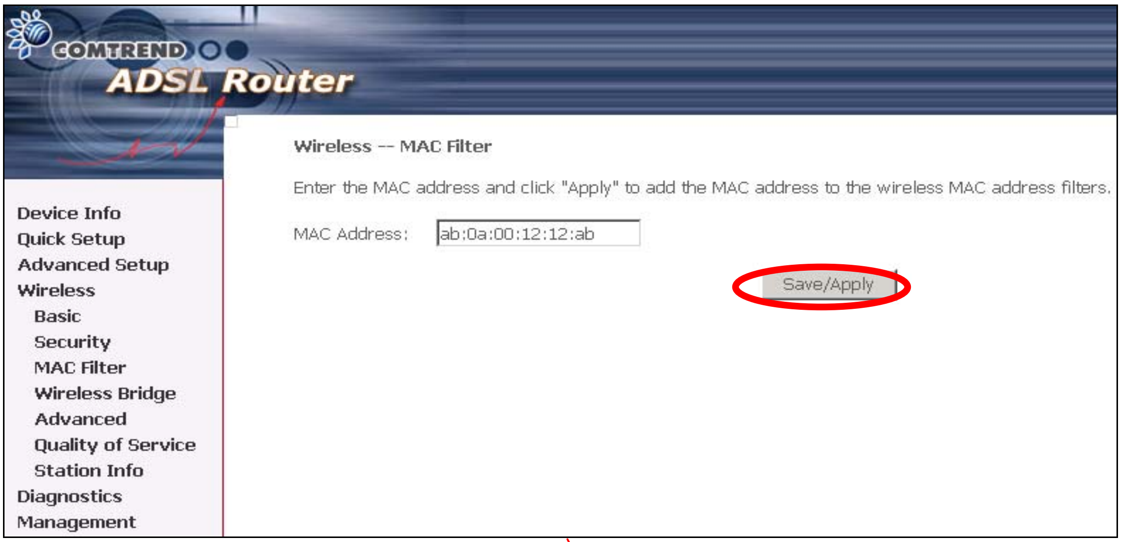


Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

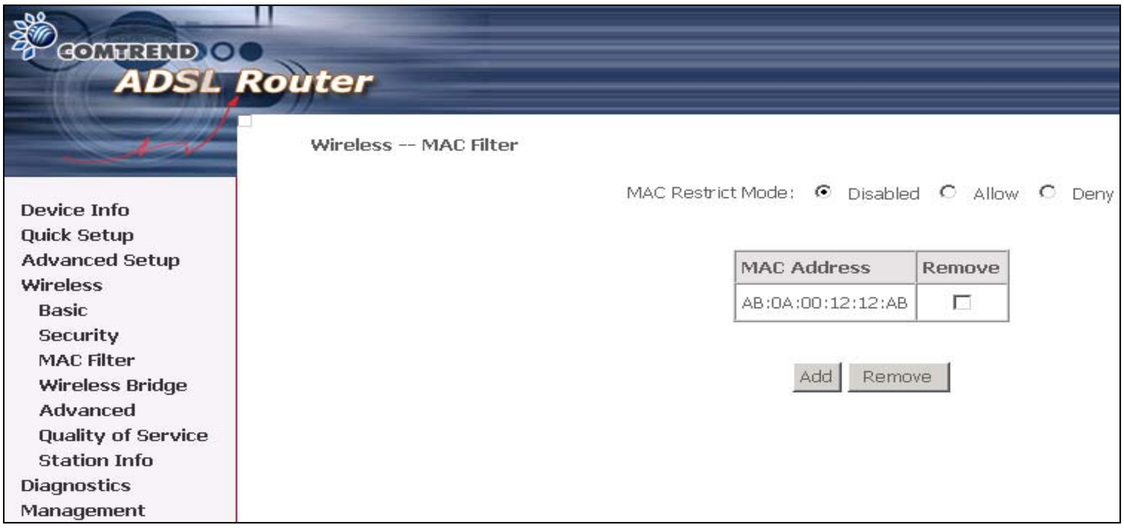
After choosing the Add button, the following screen appears. Enter the MAC address and click **Apply** to add the MAC address to the wireless MAC address filters.



Wireless -- MAC Filter

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

MAC Address: ab:0a:00:12:12:ab



Wireless -- MAC Filter

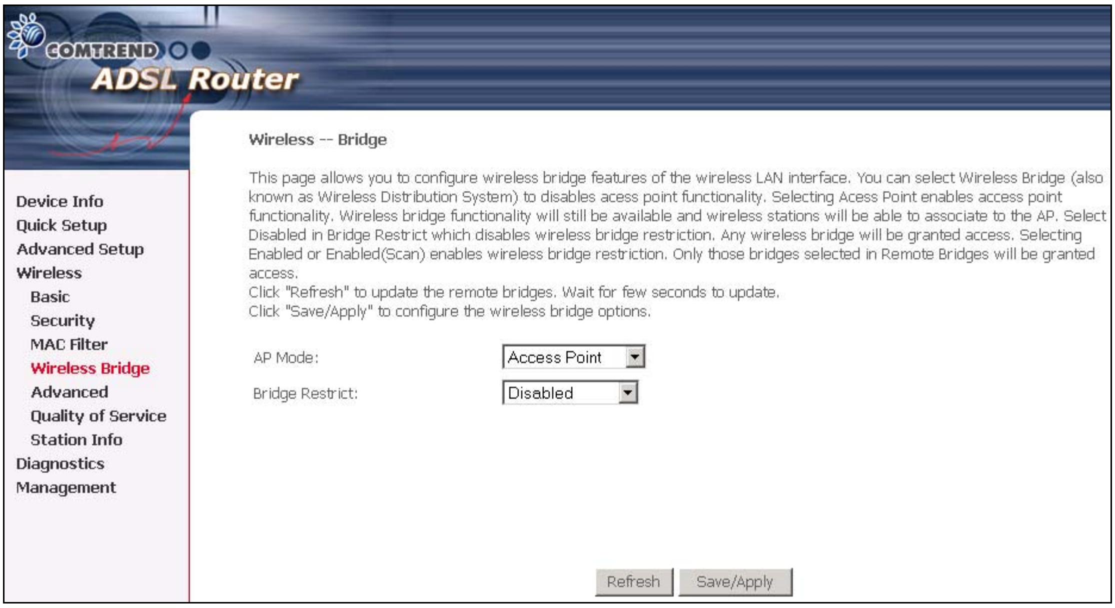
MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove
AB:0A:00:12:12:AB	□

Option	**Description**
MAC Restrict Mode	Radio buttons that allow settings of; Off: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to the access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60.

7.1.3 Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables acess point functionality. Selecting Acess Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

AP Mode: Access Point

Bridge Restrict: Disabled

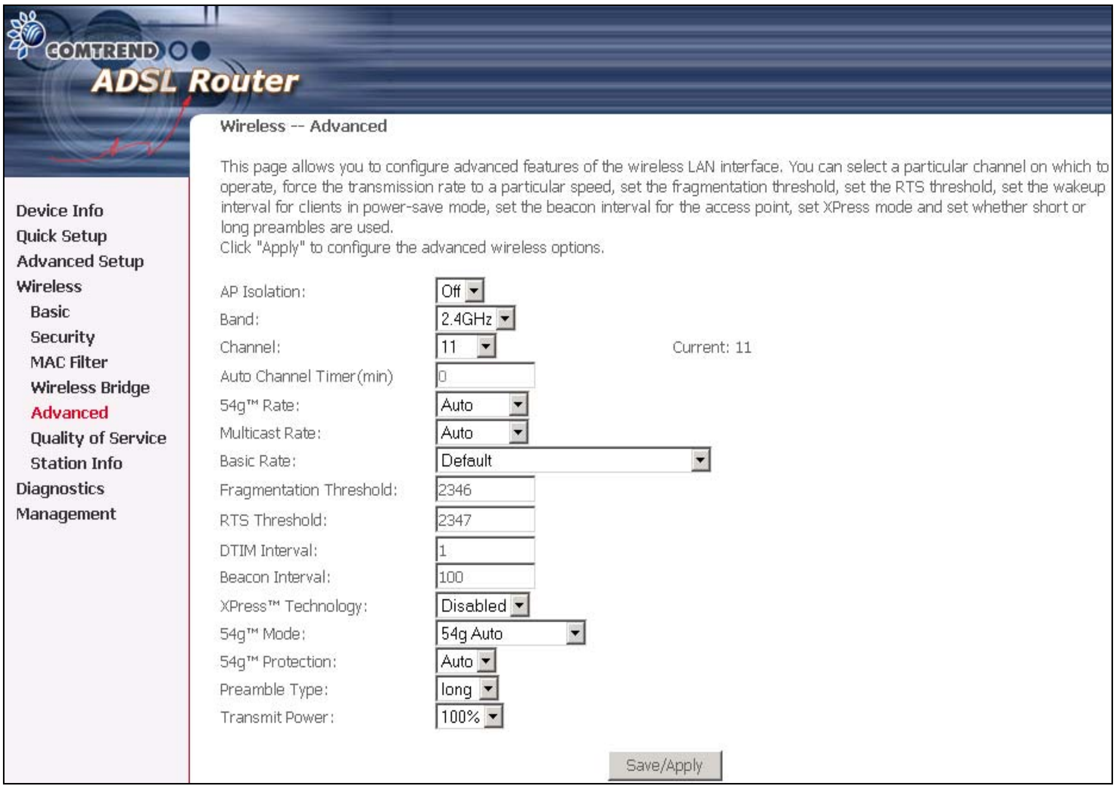
Option	Description
AP Mode	Access Point Wireless Bridge
Bridge Restrict	Enabled Enabled (Scan) Disabled

7.1.4 Advanced

The Advanced page allows you to configure advanced features of the wireless LAN interface.

You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

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



Wireless -- Advanced

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

AP Isolation: Off
Band: 2.4GHz
Channel: 11 Current: 11
Auto Channel Timer(min) 0
54g™ Rate: Auto
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
XPress™ Technology: Disabled
54g™ Mode: 54g Auto
54g™ Protection: Auto
Preamble Type: long
Transmit Power: 100%

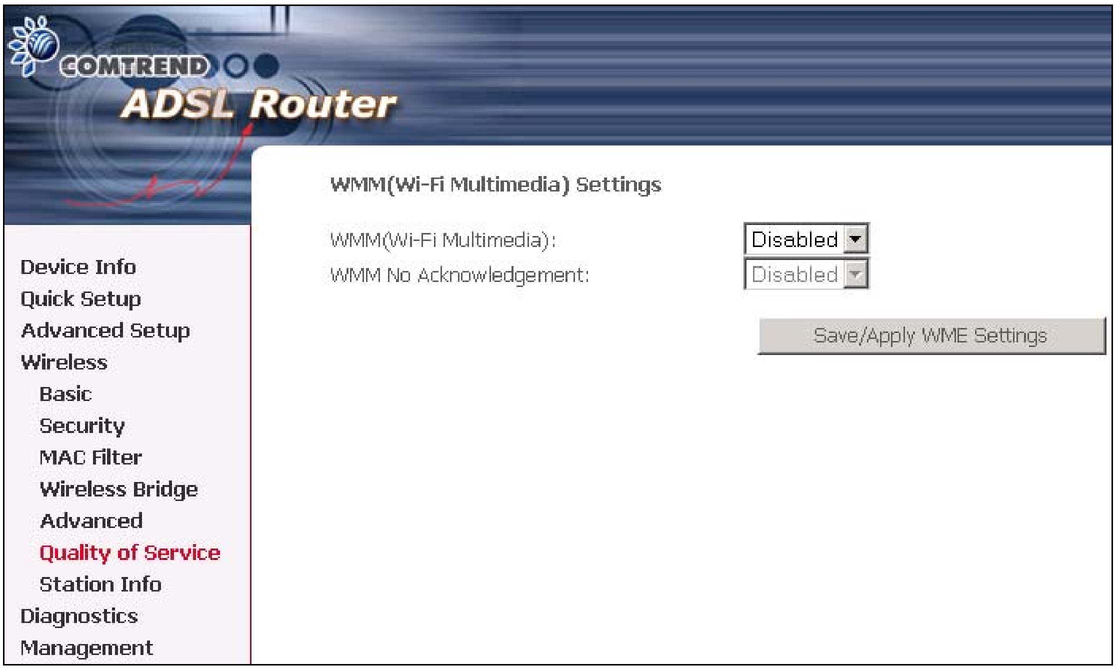
Option	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point will be able to connect to each other.

Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.

DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g ™ Mode	Set the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.

7.1.5 Quality of Service

WMM provides advanced quality of service (QoS) features for Wi-Fi networks to improve the end-user experience by prioritizing audio, video and voice traffic and optimizing the way shared network resources are allocated among competing applications.



WMM(Wi-Fi Multimedia) Settings

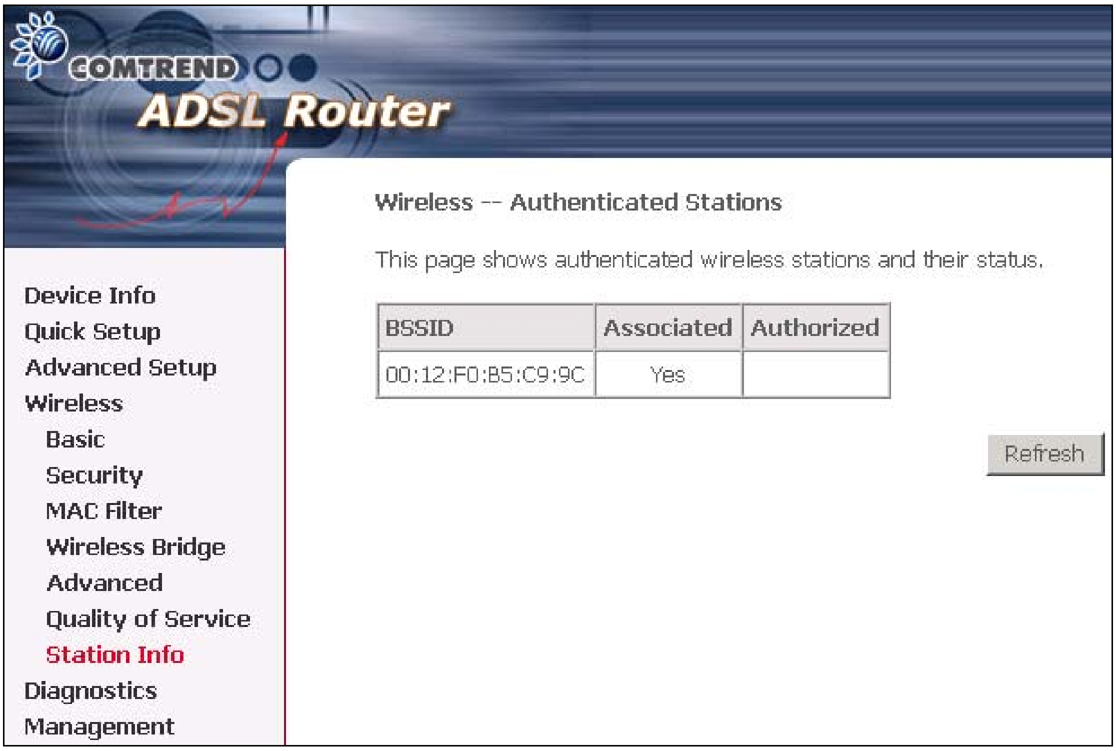
WMM(Wi-Fi Multimedia): Disabled

WMM No Acknowledgement: Disabled

If you want to enable Click on the drop down menu and select, then click the **Save/Apply WME Settings** button.

7.1.6 Station Info

This page shows authenticated wireless stations and their status.



Wireless -- Authenticated Stations

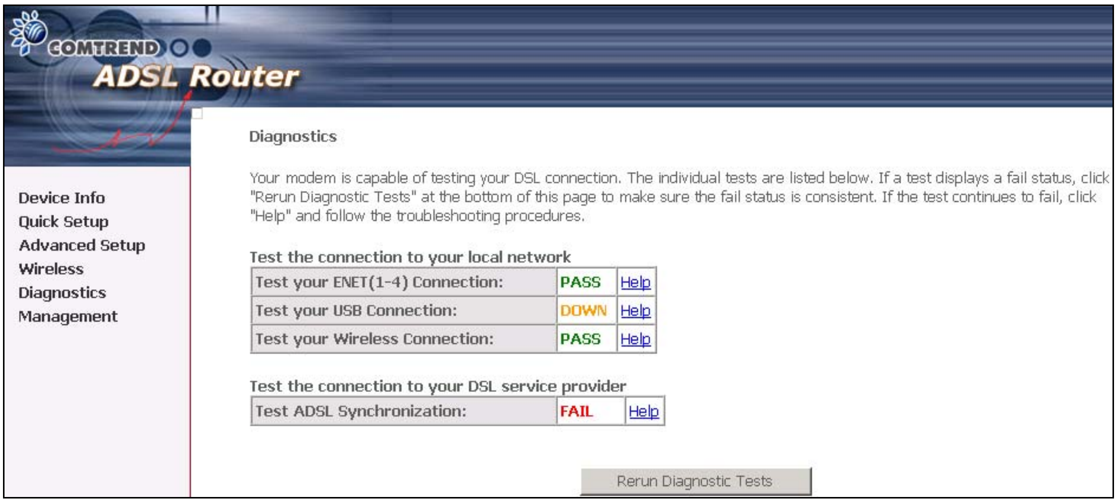
This page shows authenticated wireless stations and their status.

BSSID	Associated	Authorized
00:12:F0:B5:C9:9C	Yes	

BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

Chapter 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-5372 and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Diagnostics

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

Test the connection to your local network

Test your ENET(1-4) Connection:	PASS	Help
Test your USB Connection:	DOWN	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help

Test	Description
Ethernet Connection	**Pass:** indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A blinking or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful. **Fail:** Indicates that the DSL Router does not detect the Ethernet interface on your computer.
USB	This option is for future release.
ADSL Synchronization	**Pass:** Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid WAN LED on the router also indicates the detection of a DSL signal from the telephone company. **Fail:** indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The WAN LED will stop blinking (i.e. training) and the LED will stop illuminating (i.e. go blank).

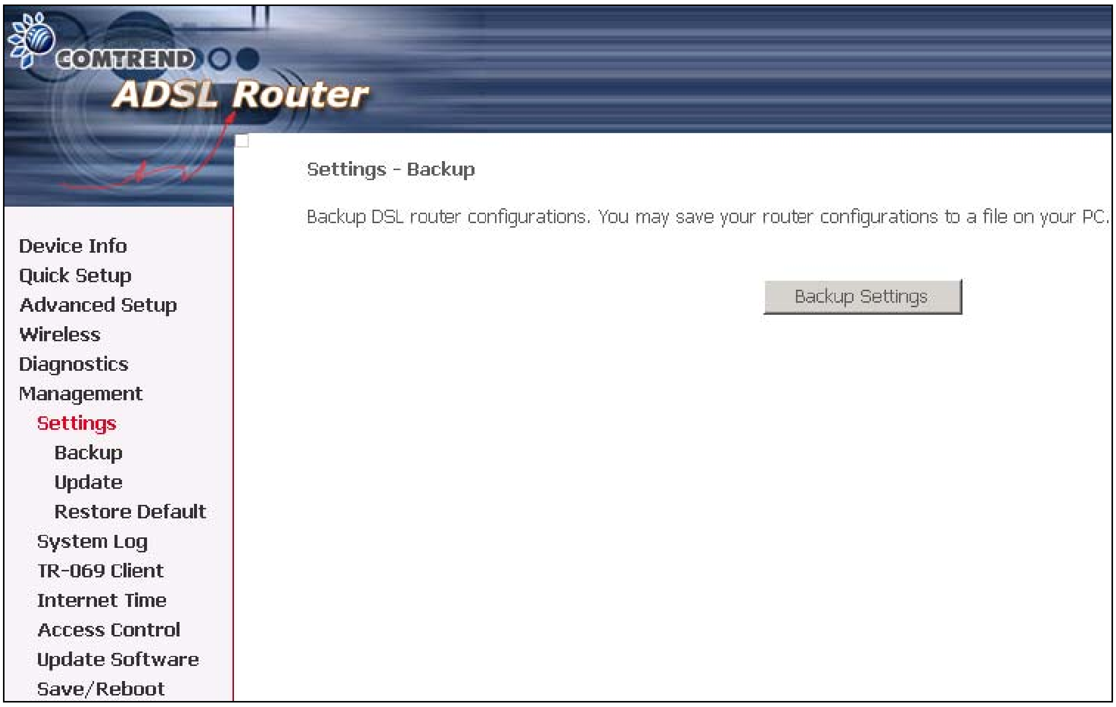
Chapter 9 Management

The Management section of the CT-5372 supports the following maintenance functions and processes:

- Settings
- System log
- TR-069 Client
- Internet Time
- Access Control
- Update software
- Save/Reboot

9.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.

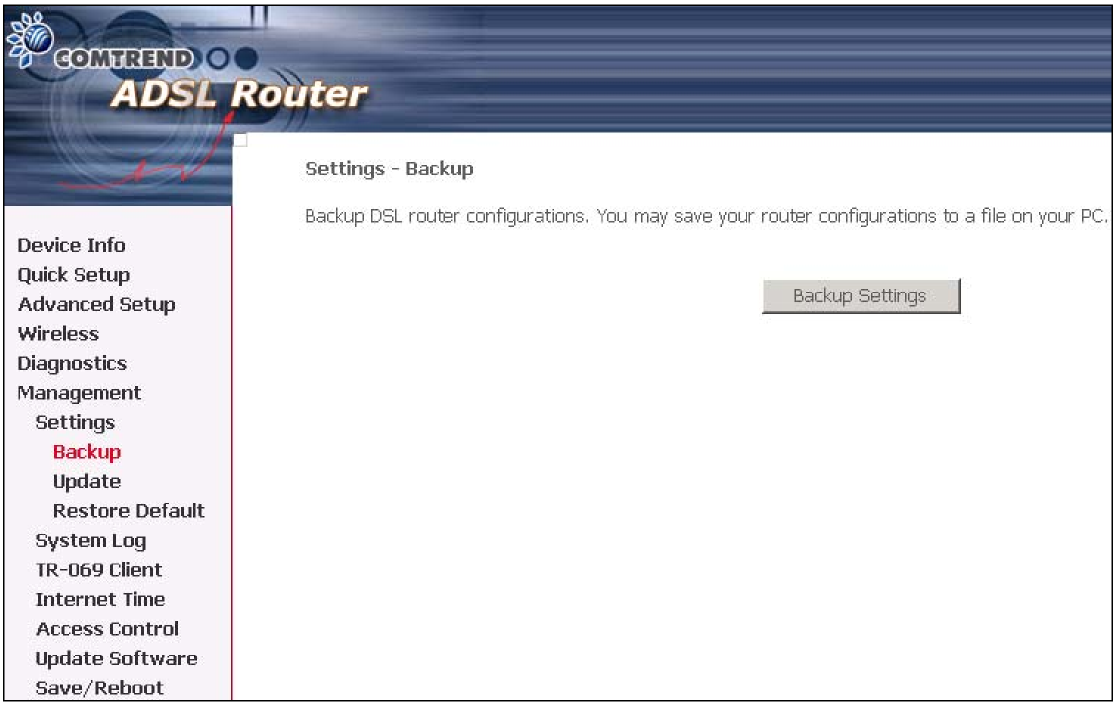


Settings - Backup

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

9.1.1 Configuration Backup

The Backup option under Management>Settings save your router configurations to a file on your PC. Click BACKUP Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings.** The file will then be saved to the assigned location.

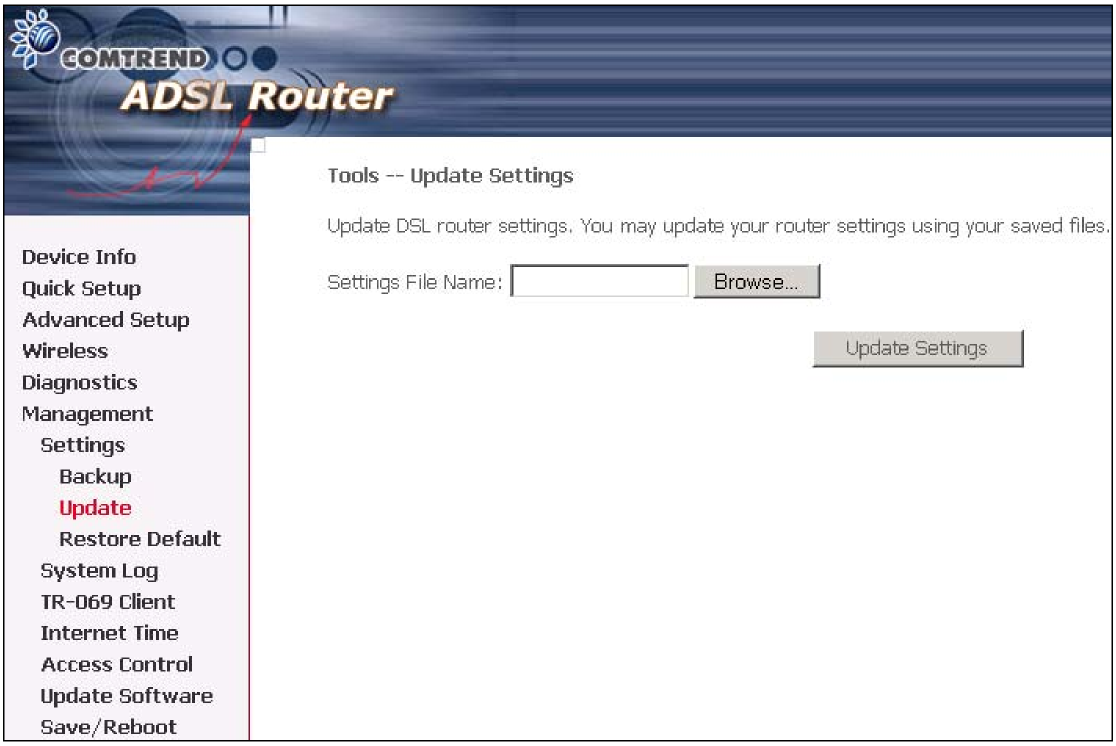


Settings - Backup

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

9.1.2 Tools – Update Settings

The Update option under Management>Settings update your router settings using your saved files.



Tools -- Update Settings

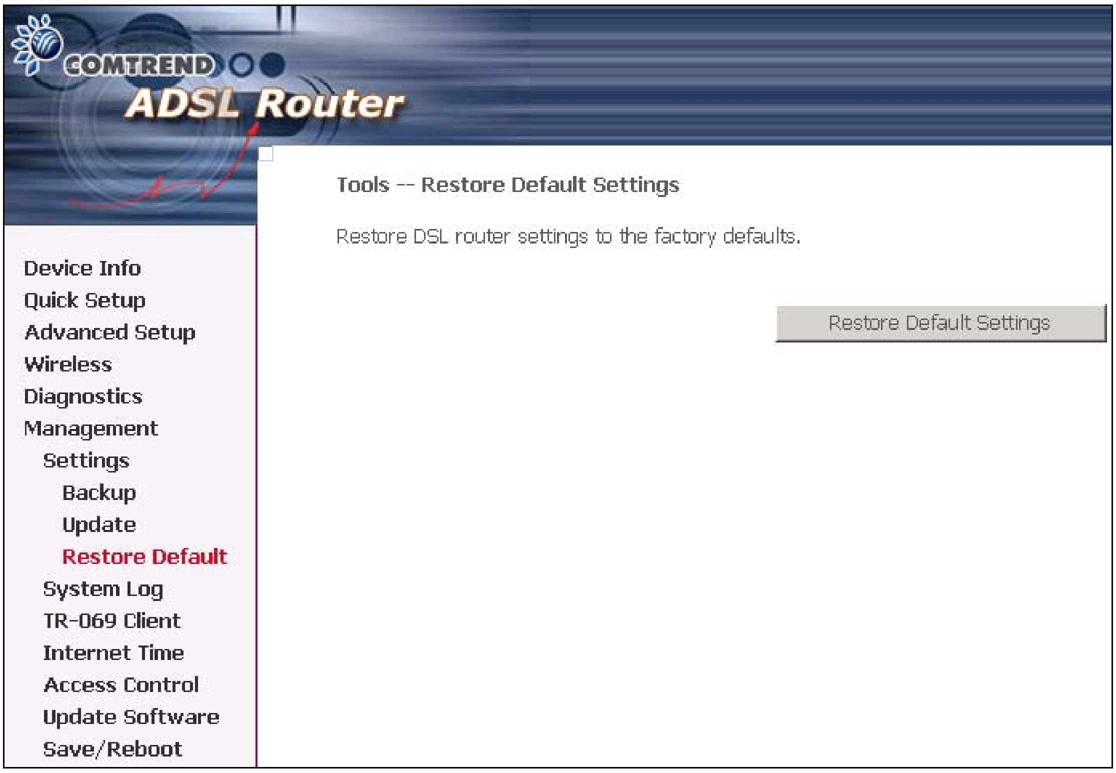
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name: [ ] Browse...

Update Settings

9.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

NOTE: This entry has the same effect as the hardware reset-to-default button. The CT-5372 board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration data saved on the flash memory.

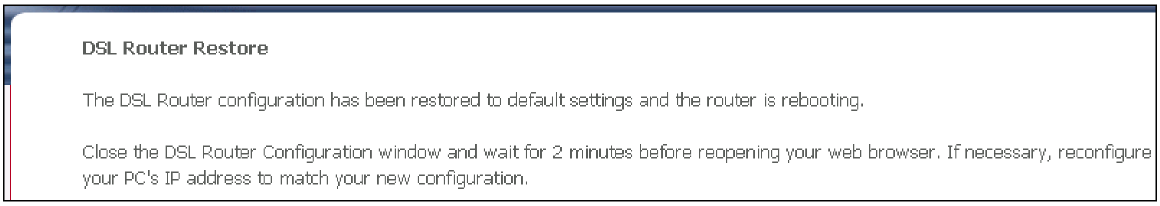
NOTE: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-5372.

Default settings

The CT-5372 default settings are

- LAN port IP= 192.168.1.1, subnet mask = 255.255.255.0
- Local user name: root
- Password: 12345
- Remote user name: support
- Remote user password: support

After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



DSL Router Restore

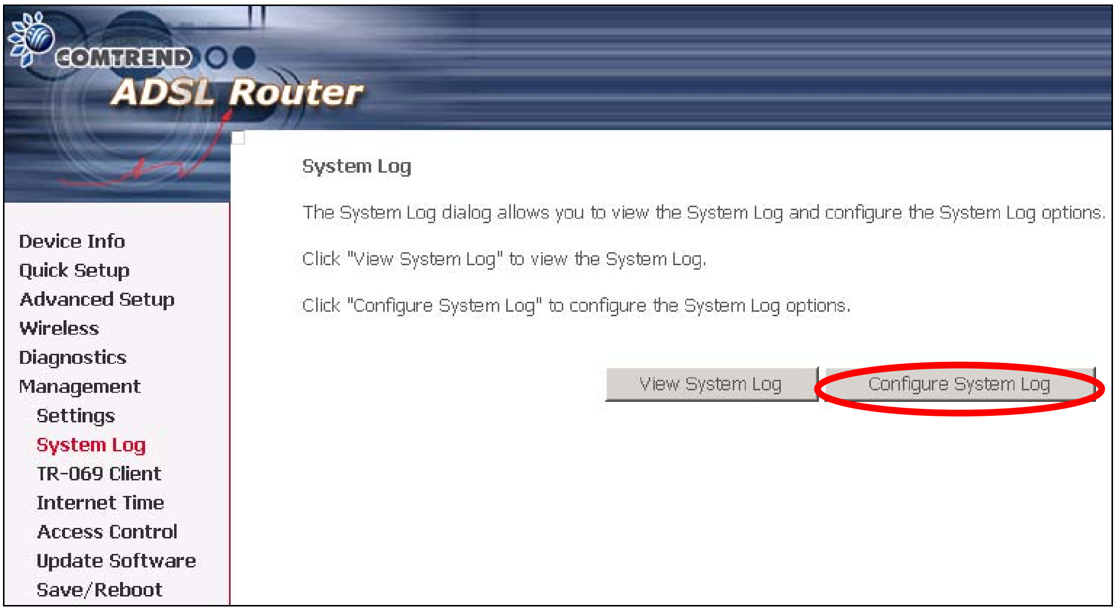
The DSL Router configuration has been restored to default settings and the router is rebooting.

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

9.2 System Log

The System Log option under Management>Settings allows you to view the system events log, or to configure the System Log options. The default setting of system log is disabled. Follow the steps below to enable and view the system log.

1. Click **Configure System Log** to display the following screen.



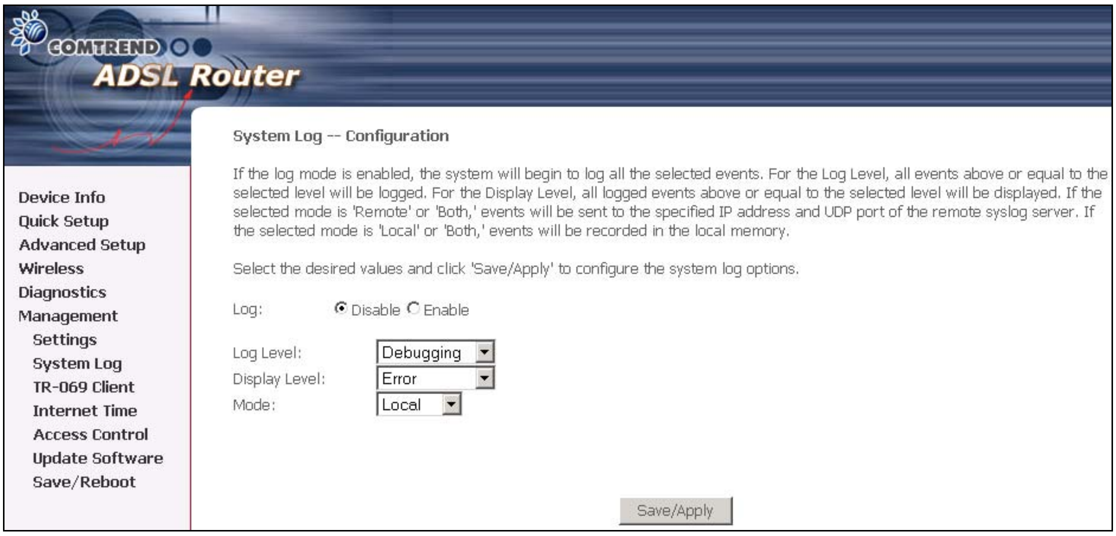
System Log

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

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

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

2. Select from the desired Log options described in the following table, and then click **Save/Apply**.



System Log -- Configuration

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

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

Log: ● Disable ○ Enable

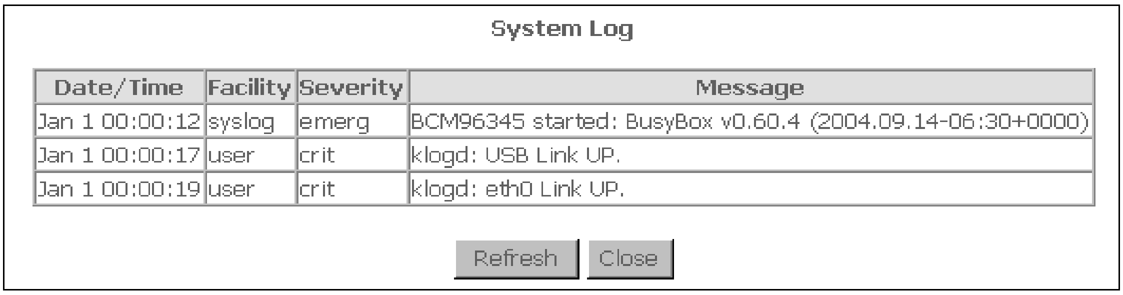
Log Level: Debugging

Display Level: Error

Mode: Local

Option	**Description**
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.
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-5372 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are ● 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** page 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 syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

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

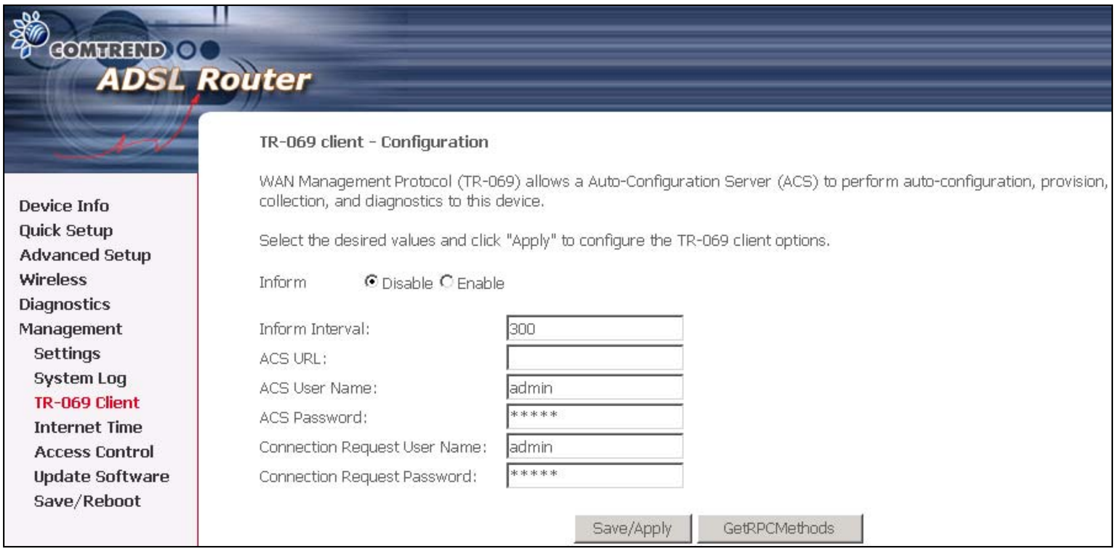


System Log

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

9.3 TR-069 Client

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



TR-069 client - Configuration

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

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

Inform ● Disable ○ Enable

Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	*****
Connection Request User Name:	admin
Connection Request Password:	*****

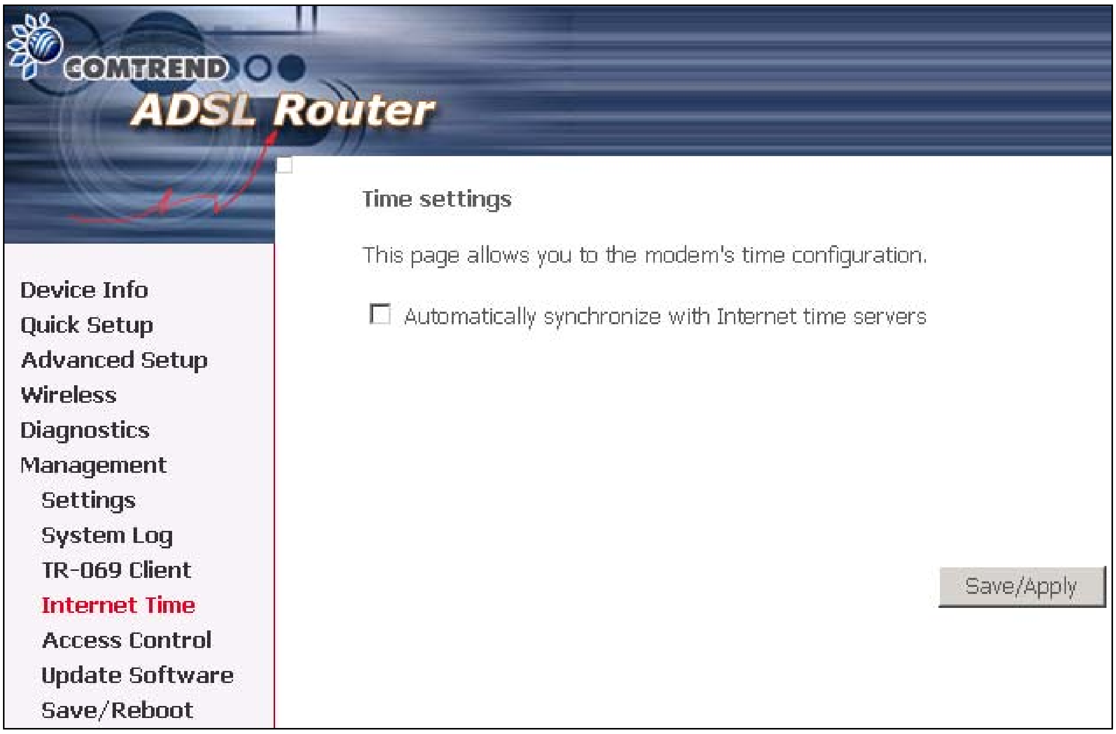
Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter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

User Name	Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. 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. Click this button to force the CPE to immediately establish a connection to the ACS.

9.4 Internet Time

The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet time servers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.

Note: This menu item will not be displayed if a Bridged PVC is configured.



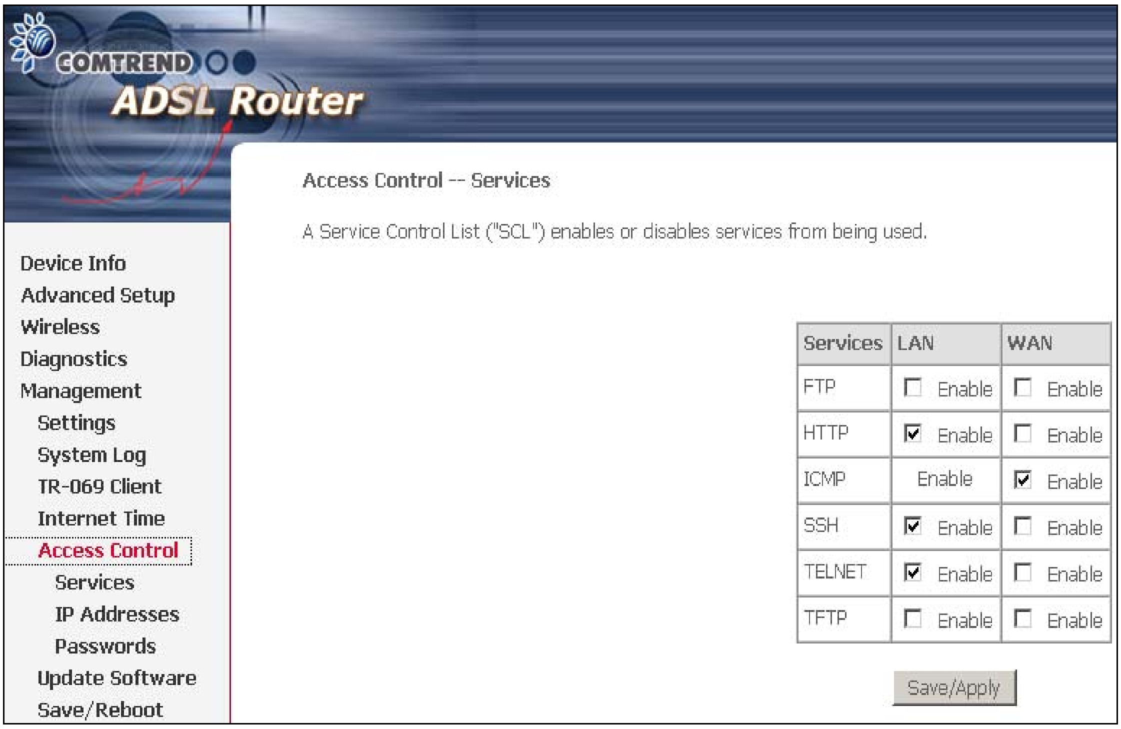
Time settings

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

□ Automatically synchronize with Internet time servers

9.5 Access Control

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



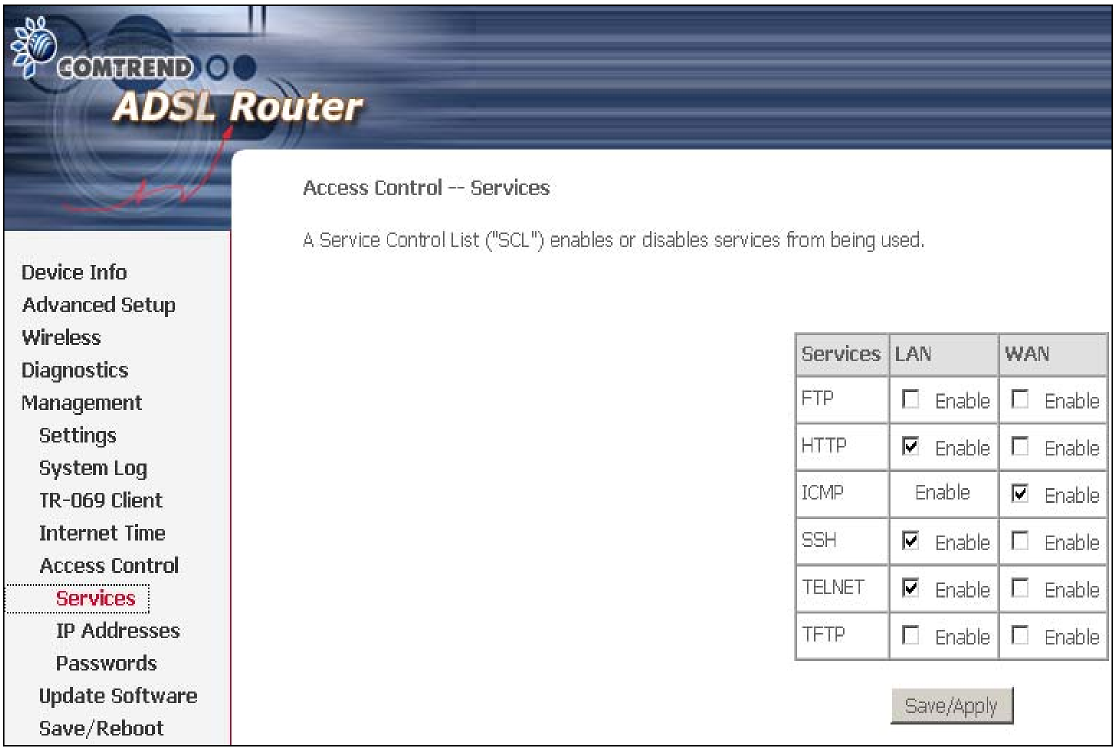
Access Control -- Services

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

Services	LAN	WAN
FTP	□ Enable	□ Enable
HTTP	☑ Enable	□ Enable
ICMP	Enable	☑ Enable
SSH	☑ Enable	□ Enable
TELNET	☑ Enable	□ Enable
TFTP	□ Enable	□ Enable

9.5.1 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**.



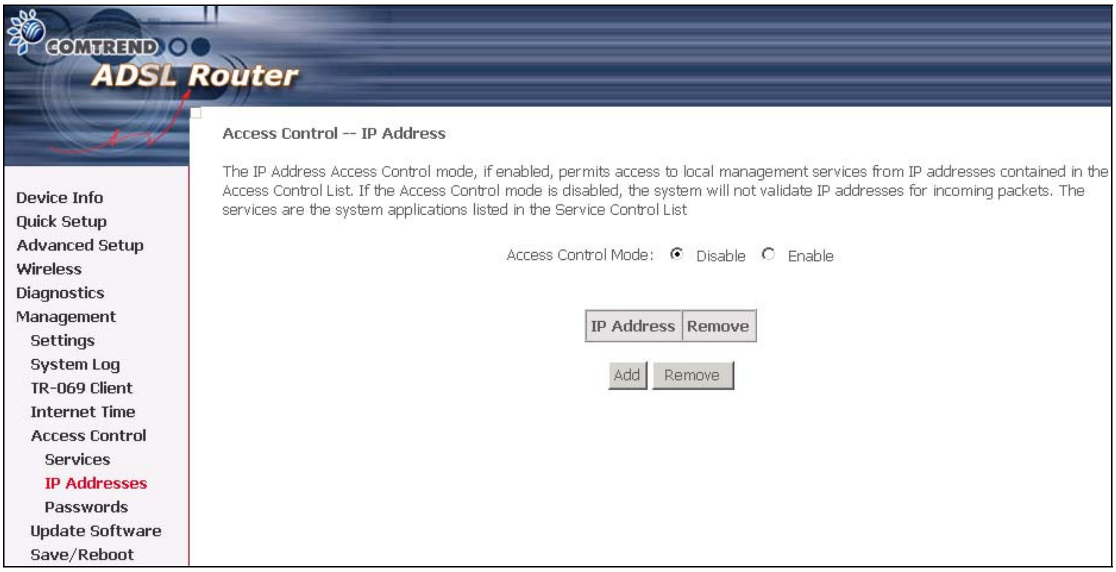
Access Control -- Services

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

Services	LAN	WAN
FTP	☐ Enable	☐ Enable
HTTP	☑ Enable	☐ Enable
ICMP	Enable	☑ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☐ Enable	☐ Enable

9.5.2 Access 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. Before 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.



Access Control -- IP Address

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

Access Control Mode: ● Disable ○ Enable

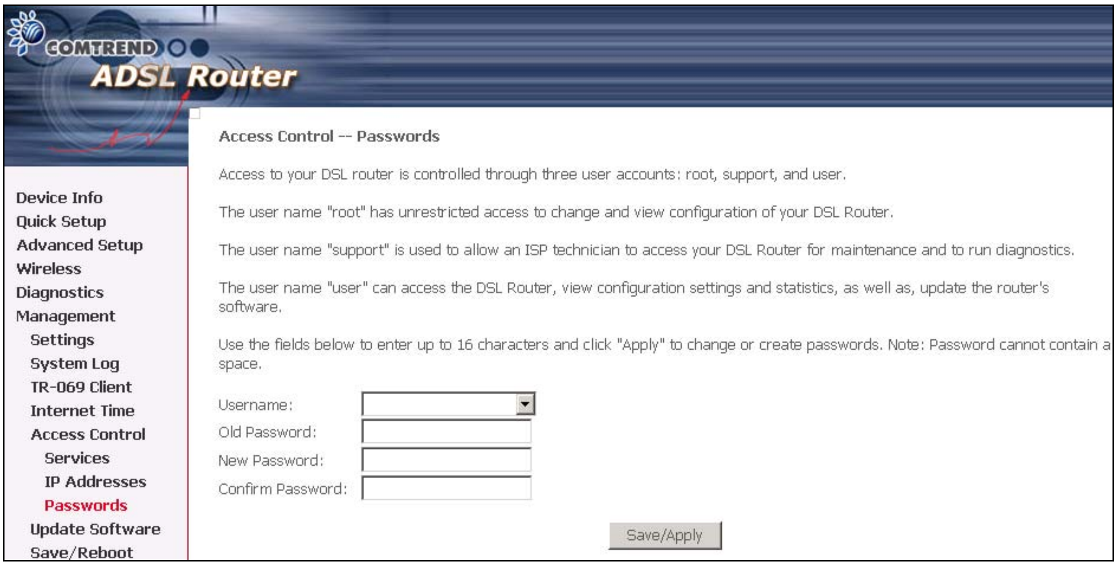
IP Address	Remove

9.5.3 Passwords

The Passwords option configures the access passwords for the router. Access to your DSL router is controlled through three user accounts: root, support, and user.

- “root” has unrestricted access to change and view configuration of your DSL Router.
- "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
- "user" can access the Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click Apply to change or create passwords.



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: root, support, and user.

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

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

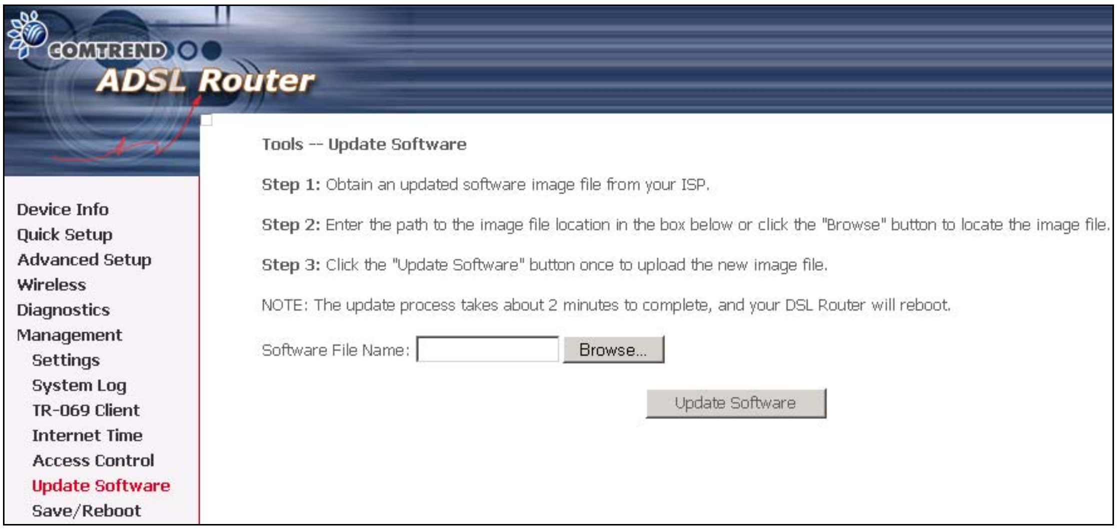
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

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

Username:
Old Password:
New Password:
Confirm Password:

9.6 Update software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.



Tools -- Update Software

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

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

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

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

Software File Name:

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

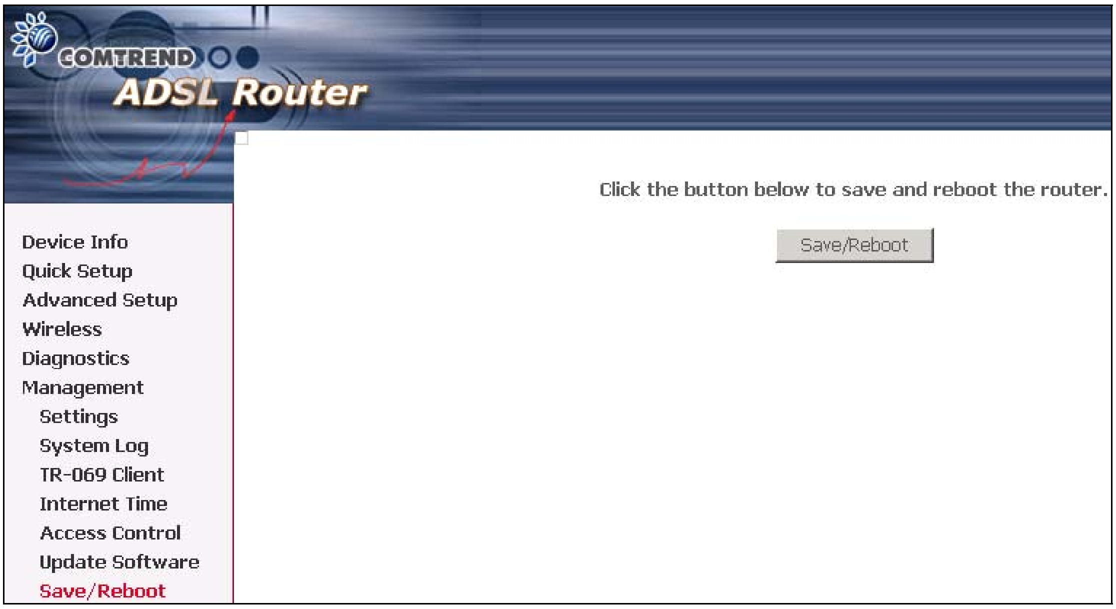
Step 2: Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

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

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

9.7 Save and Reboot

The Save/Reboot options saving the configurations and reboot the router. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



Click the button below to save and reboot the router.

Appendix A: Printer Server Configuration

1. Introduction

This application notes explain the steps of enabling the Printer Server function in CT-5372 DSL Router reference platforms.

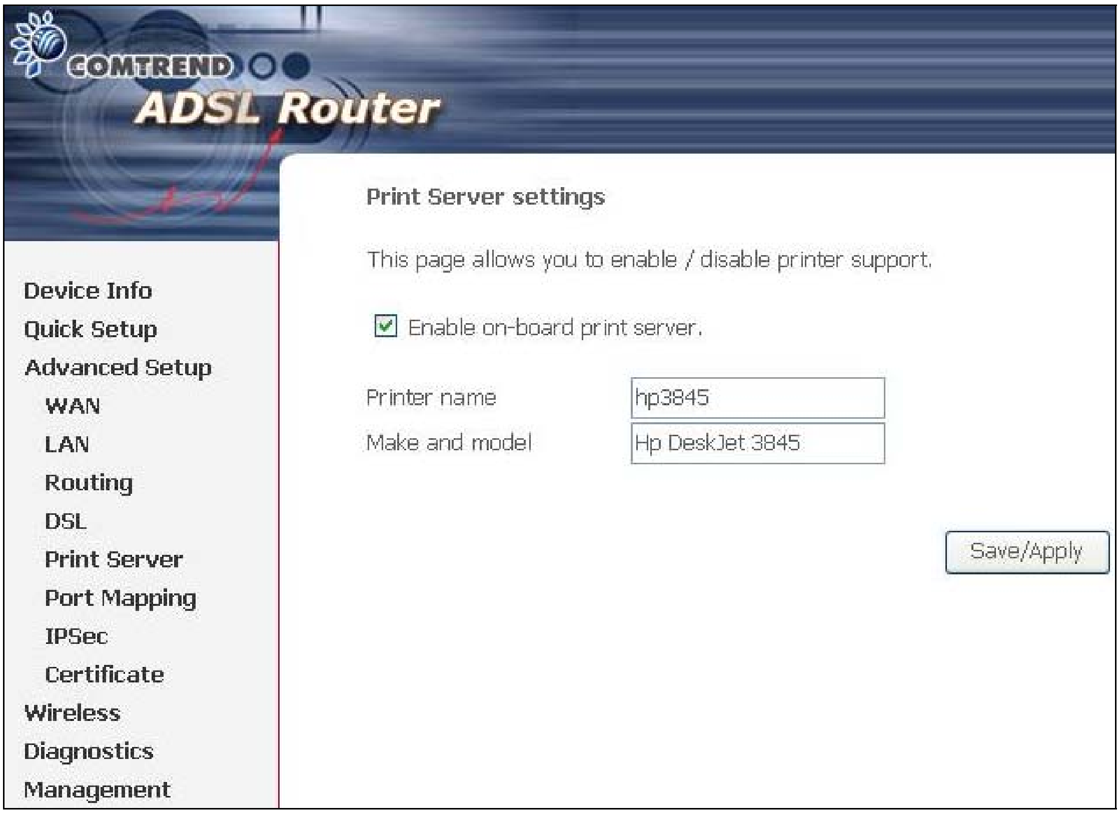
2. How to enable on-board Printer Server function

Following are the steps to enable the on-board Printer Server.

Step1: Enable Print Server from Modem Web GUI.

Check "**Enable on-board printer server**" and key in "**Printer name**", "**Make and model**"

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



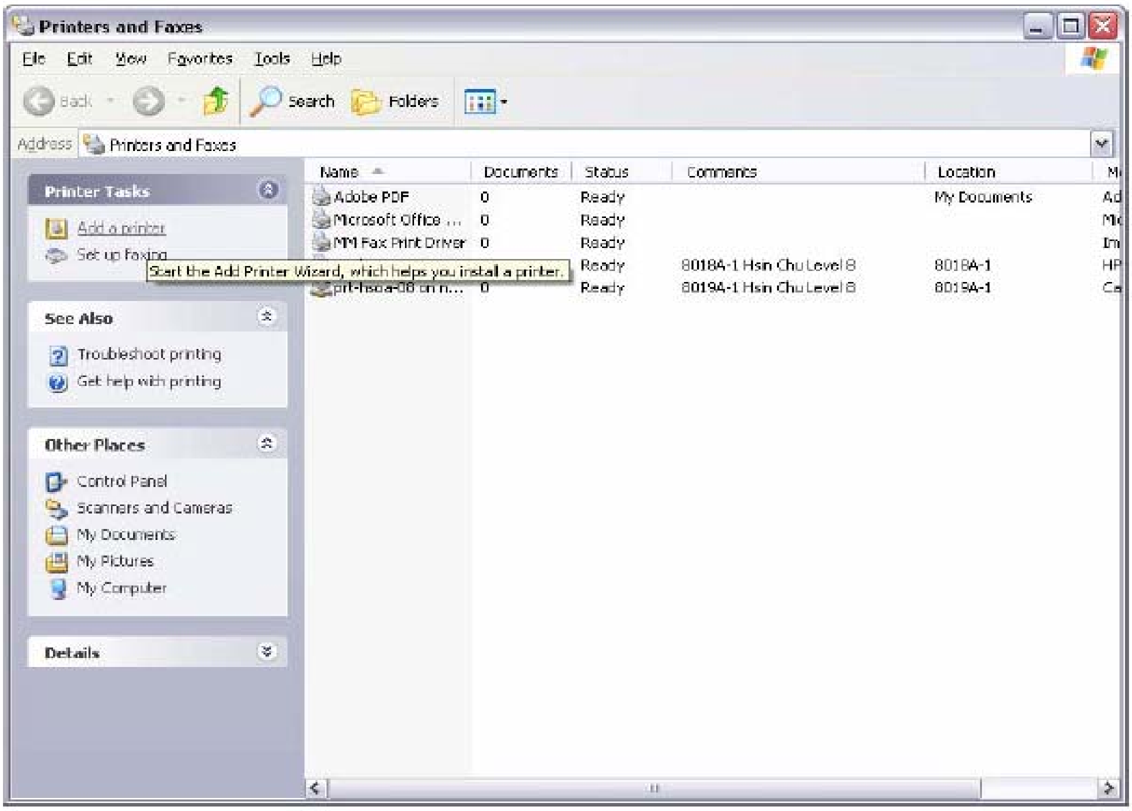
Print Server settings

This page allows you to enable / disable printer support.

☑ Enable on-board print server.

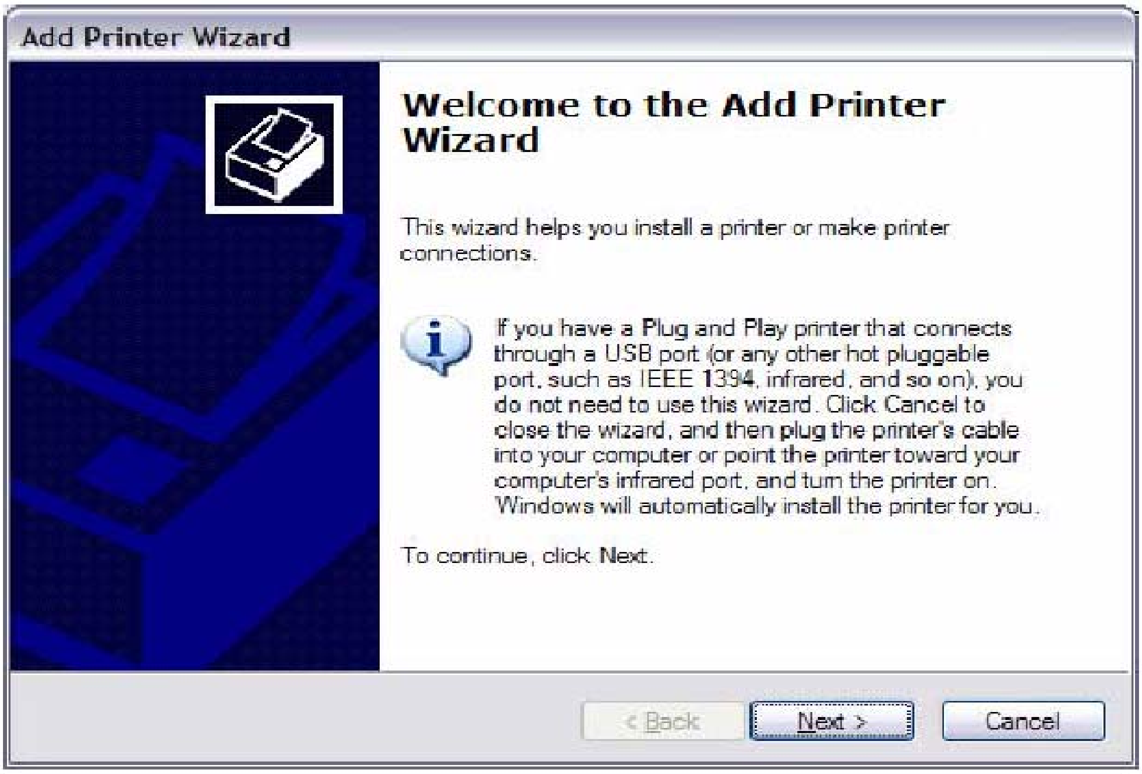
Printer name: hp3845
Make and model: Hp DeskJet 3845

Step2: Click on Add a printer from **Control Panel** of the **Win XP** computer and click "Next".



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

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



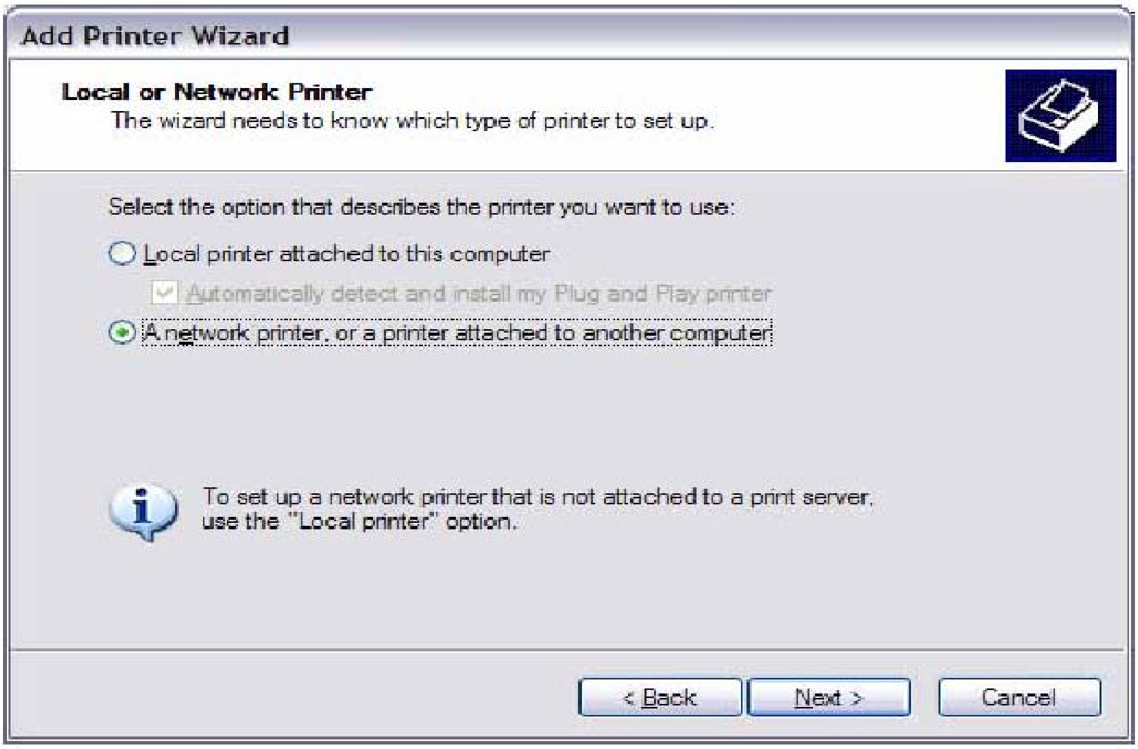
Welcome to the Add Printer Wizard

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

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

To continue, click Next.

Step3: Select Network Printer and click "Next".



Add Printer Wizard

Local or Network Printer

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

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

○ Local printer attached to this computer

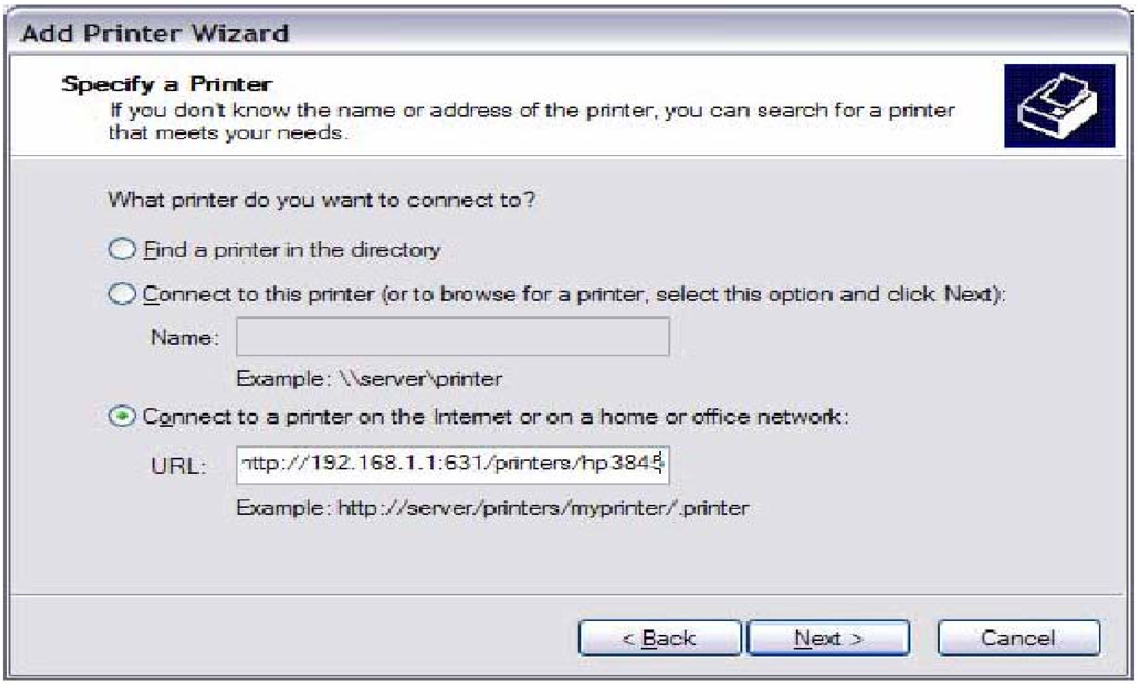
☑ Automatically detect and install my Plug and Play printer

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

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

Step4: Select Connect to a printer on the Internet, type "http://192.168.1.1:631/printers/hp3845" and click "Next".

The printer name "hp3845" must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.



Add Printer Wizard

Specify a Printer

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

What printer do you want to connect to?

○ Find a printer in the directory

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

Name:

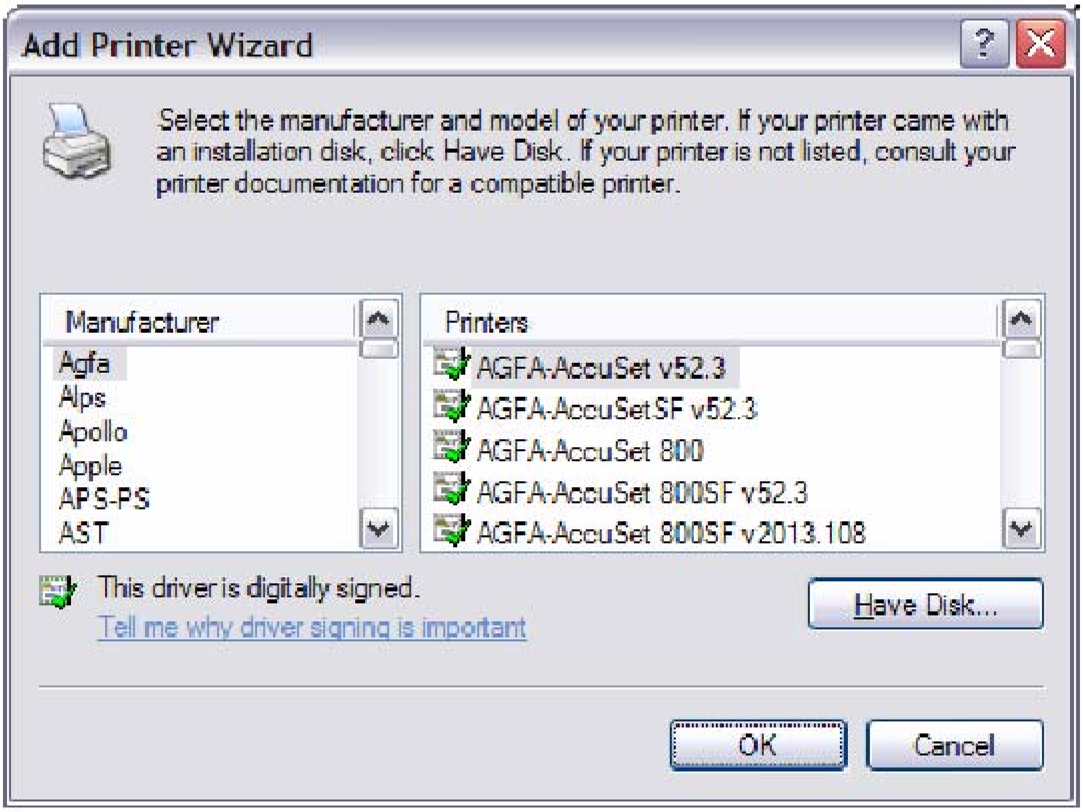
Example: \\server\printer

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

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

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

Step 5: Click "Have Disk", insert printer driver CD.



Add Printer Wizard

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

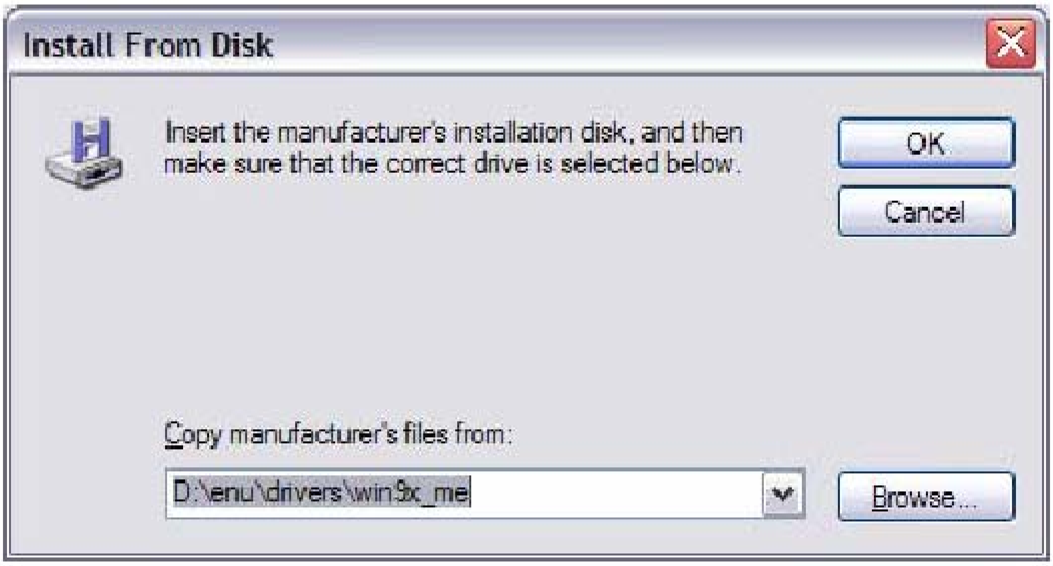
Manufacturer
Agfa
Alps
Apollo
Apple
APS-PS
AST

Printers
AGFA-AccuSet v52.3
AGFA-AccuSet SF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
AGFA-AccuSet 800SF v2013.108

This driver is digitally signed.

Tell me why driver signing is important

Step 6: Select driver file directory on CD-ROM and click “OK”.



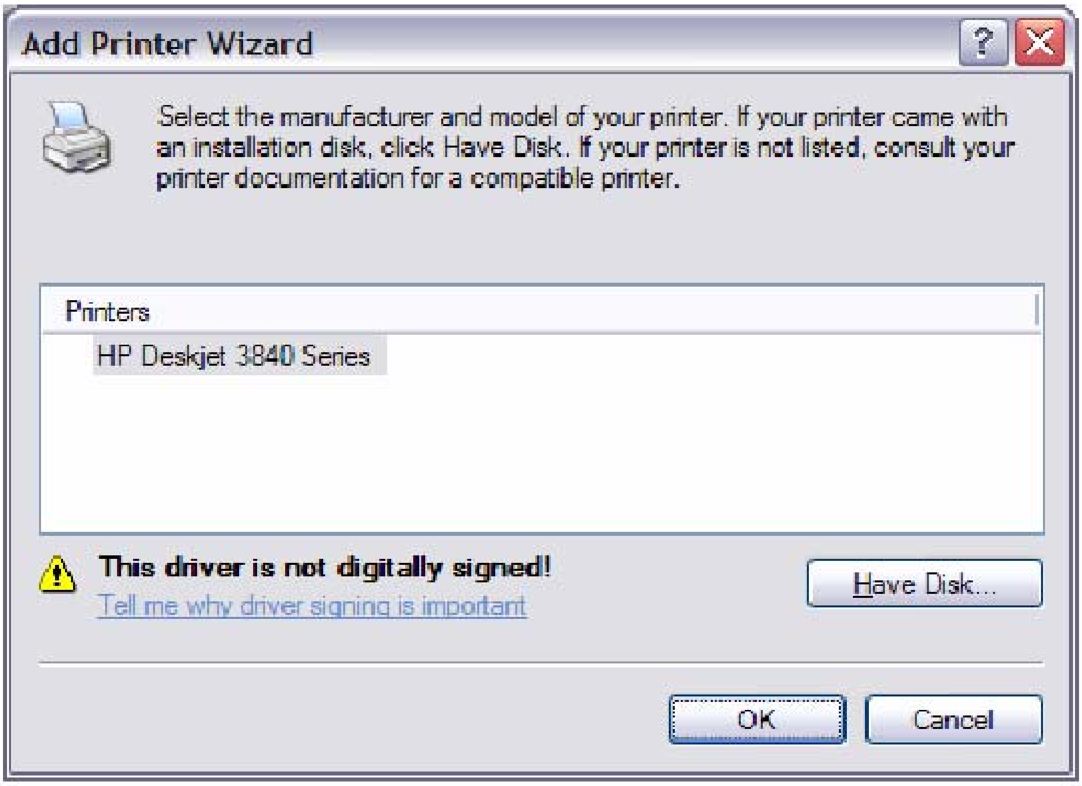
Install From Disk

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

Copy manufacturer's files from:

D:\enu\drivers\win9x_me

Step 7: Once the printer name appears, click “OK”.



Add Printer Wizard

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

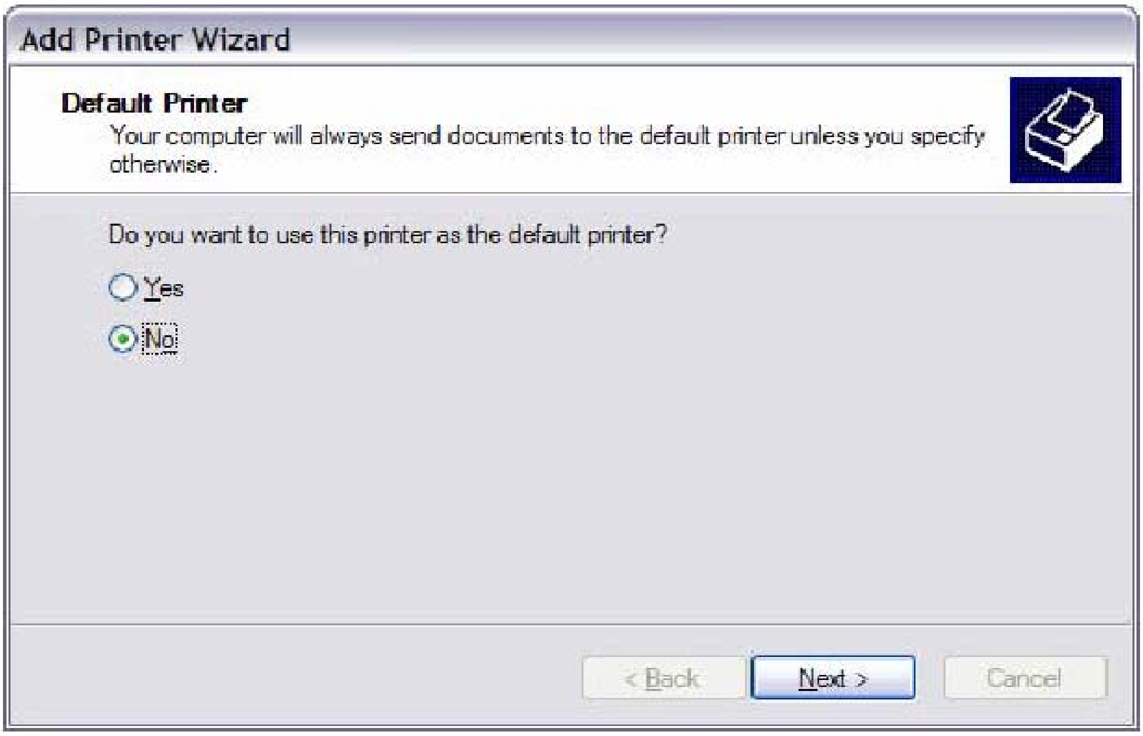
Printers

HP Deskjet 3840 Series

This driver is not digitally signed!

Tell me why driver signing is important

Step 8: Choose "Yes" or "No" for default printer setting and click "Next".



Add Printer Wizard

Default Printer

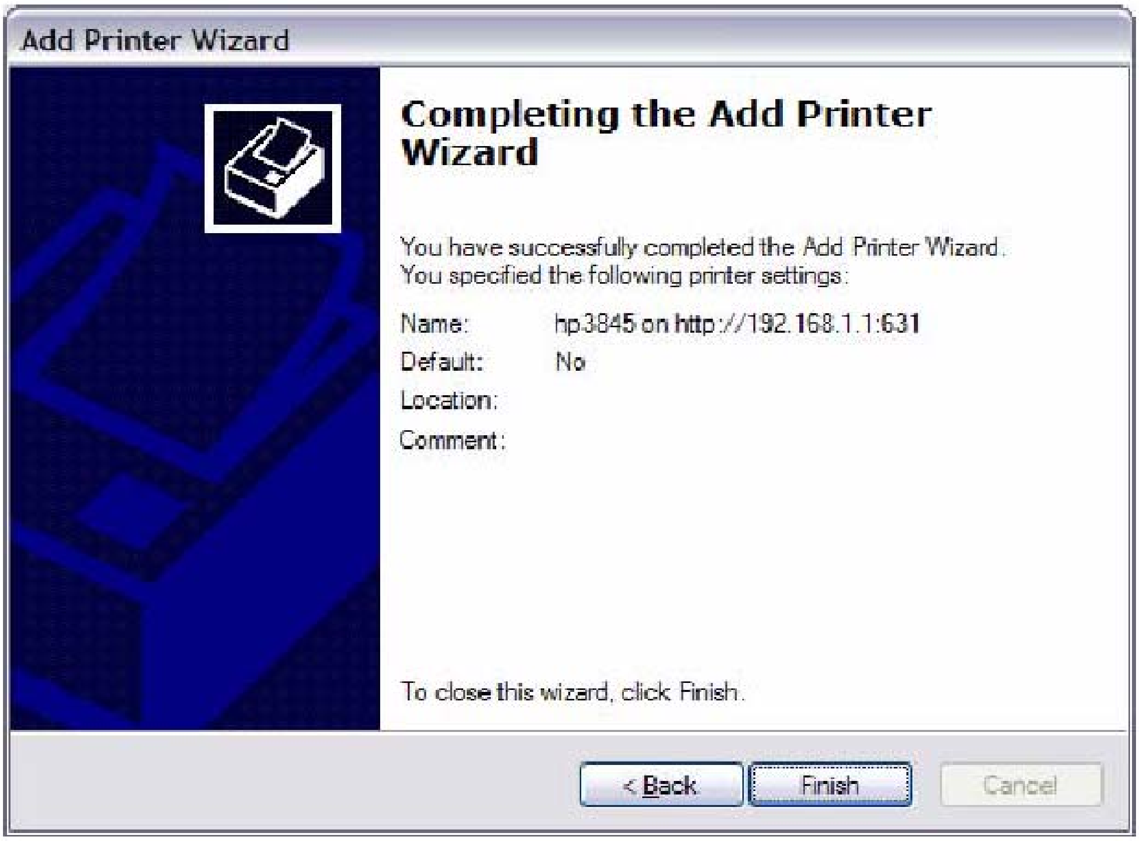
Your computer will always send documents to the default printer unless you specify otherwise.

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

○ Yes

● No

Step 9: Click "Finish".



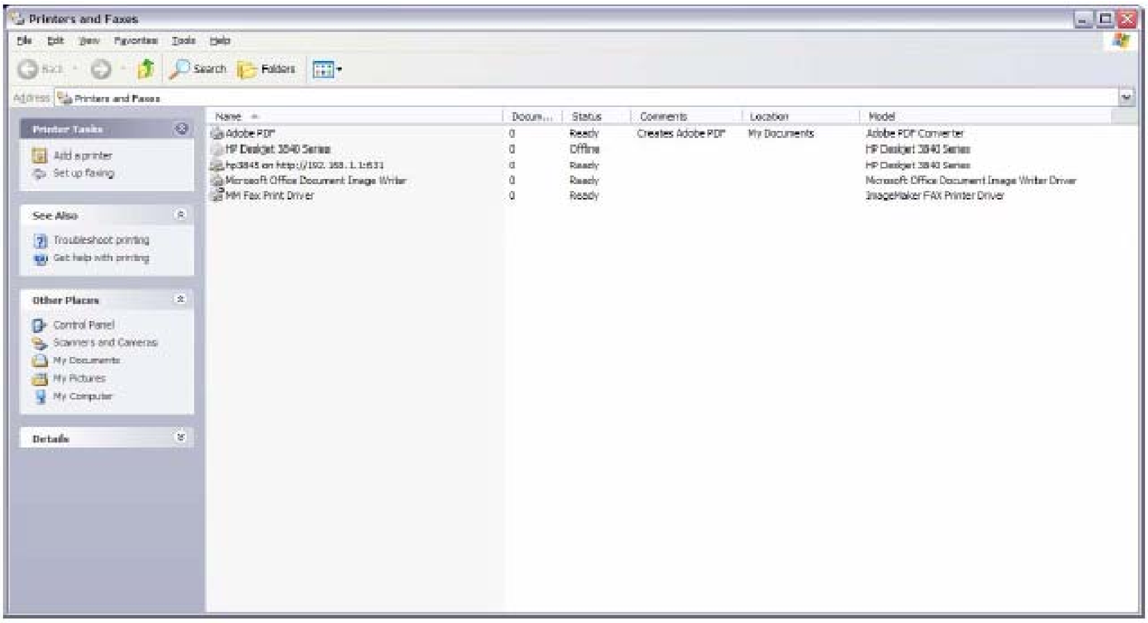
Completing the Add Printer Wizard

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

Name: hp3845 on http://192.168.1.1:631
Default: No
Location:
Comment:

To close this wizard, click Finish.

Step 10: Check the status of printer from Windows Control Panel, printer window. Status should be shown ready.



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

Appendix B: 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 filtering rules

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, web page.

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

Filter Name: User defined Filter Name.

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

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.
Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular

"Destination IP Address/Destination Subnet Mask" combination will be dropped.

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

Examples:

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

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

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

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

Incoming IP Filtering:

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

Filter Name: User defined Filter Name.

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

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

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

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

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

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

Examples:

1.	Filter Name	: In_Filter1
	Protocol	: TCP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 80
	Dest. Address	:NA
	Dest. Sub. Mask	: NA
	Dest. Port	: NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2.	Filter Name	: In_Filter2
	Protocol	: UDP
	Source Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 5060:6060
	Dest. Address	:192.168.1.45
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub.Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC Layer Filtering:

These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

Global Policy:

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

To setup a rule:

Protocol Type: Can be either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

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

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

Frame Direction:

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

User needs to select the interface on which this rule is applied.

Examples:

1.
Global Policy: Forwarded
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78
Source MAC Addr: NA
Frame Direction: LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

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

2.
Global Policy: Blocked
Protocol Type: PPPoE
Dest. MAC Addr: 00:12:34:56:78:90
Source MAC Addr: 00:34:12:78:90:56
Frame Direction: WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br_0_34 WAN interface. All other frames on this interface are dropped.

Daytime Parental Control

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

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

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

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:

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

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

Appendix C: Pin Assignments

Line port (RJ11)

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

Pin Assignments of the RJ11 Port

LAN Port (RJ45)

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

Pin assignments of the LAN Port

Appendix D: Specifications

Rear Panel

RJ-11 X1 for ADSL2+/VDSL2, RJ-45 X 4 for LAN, Reset Button X 1, Power switch X 1, USB X 1, USB host X 1

DSL

ADSL	ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2
ADSL2+	Downstream：24 Mbps Upstream：1.3 Mbps
VDSL2 Standard	ITU-T G.993.2
VDSL2	Downstream：100 Mbps Upstream：65 Mbps

Ethernet

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

ATM Attributes

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

Support PVCs	8
AAL type	AAL5
ATM service class	UBR/CBR/VBR
ATM UNI support	UNI3.1/4.0
OAM F4/F5	Yes

Management

SNMP, Telnet, Web-based management, Configuration backup and restoration

Software upgrade via HTTP, TFTP server, or FTP server

Supports TR-069

Bridge Functions

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

Routing Functions

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay, DNS Proxy, ARP

Security Functions

Authentication protocols PAP, CHAP,

TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, access control, SSH

Application Passthrough

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

Power Supply

External power adapter 110 Vac or 220 Vac

Environment Condition

Operating temperature	0 ~ 50 degrees Celsius
Relative humidity	5 ~ 90% (non-condensing)

Dimensions

200 mm (W) x 44 mm (H) x 136.5 mm (D)

Certifications

FCC Part 15 class B, FCC Part 68, CE

Note: Specifications are subject to change without notice

Appendix E: SSH Client

Linux OS comes with ssh client. MicroSoft Windows does not have ssh client but there is a public domain one “putty” that you can download.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the router using Linux ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN.
(default is enabled)
type: ssh -l admin 192.168.1.1

From WAN: In the router, use WEB UI to enable SSH access from WAN.
type: ssh -l support router-WAN-ip-address

To access the router using Windows putty ssh client:
From LAN: Use the router WEB UI to enable SSH access from LAN
(default is enabled)
type: putty -ssh -l admin 192.168.1.1

From WAN: In the router, use WEB UI to enable SSH access from WAN.
type: putty -ssh -l support router-WAN-ip-address