

CT-5071T ADSL2+ Ethernet Router User's Manual

Version A3.1, May 15, 2007



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 C - Specifications.

Preface

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

Recycling For The Environment

Never throw your electronic equipment out with household waste. Ask for information from your town council on how to correctly dispose of it, so that it does not damage the environment. Always respect the current legislation regarding waste disposal.

Persons who do not comply are subject to the sanctions and penalties set down in law.

The cardboard box, the plastic contained in the packaging, and the parts that make up the device can be recycled in accordance with regionally established regulations.



The symbol of the container with the cross, which is found on the device means that when the equipment has reached the end of its working life, it must be taken to the recycling centres provided, and that its processing must be separate from that of domestic waste.

Copyright

Copyright© 2007 Comtrend Corporation. All rights reserved. The information and messages contained herein are proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written permission by Comtrend Corporation.

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	6
1.1 FEATURES.....	6
1.2 APPLICATION.....	7
1.3 FRONT PANEL LED INDICATORS.....	8
CHAPTER 2 INSTALLATION	10
2.1 HARDWARE INSTALLATION.....	10
CHAPTER 3 LOGIN VIA THE WEB BROWSER.....	12
3.1 IP ADDRESS.....	12
3.2 LOGIN PROCEDURE	14
3.3 DEFAULT SETTINGS	15
CHAPTER 4 QUICK SETUP.....	16
4.1 WAN.....	17
4.2 STATISTICS	18
4.2.1 LAN Statistics.....	19
4.2.2 WAN Statistics.....	20
4.2.3 ATM statistics	21
4.2.4 ADSL Statistics	23
4.2.5 Route.....	25
4.2.6 ARP.....	25
4.2.7 DHCP.....	26
CHAPTER 5 QUICK SETUP.....	27
5.1 AUTO QUICK SETUP	28
5.2 MANUAL QUICK SETUP	29
5.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....	31
5.2.2 MAC Encapsulation Routing (MER)	36
5.2.3 IP Over ATM.....	40
5.2.4 Bridging.....	44
CHAPTER 6 ADVANCED SETUP	46
6.1 WAN.....	48
6.2 LAN.....	49
6.3 NAT	51
6.3.1 Virtual Servers	51

6.3.2	<i>Port Triggering</i>	53
6.3.3	<i>DMZ Host</i>	55
6.3.4	<i>ALG</i>	56
6.4	SECURITY.....	57
6.4.1	<i>IP Filtering</i>	57
6.4.2	<i>Parental Control</i>	60
6.4.3	<i>MAC Filtering</i>	61
6.5	QUALITY OF SERVICE.....	63
6.6	ROUTING.....	66
6.6.1	<i>Default Gateway</i>	66
6.6.2	<i>Static Route</i>	67
6.7	DNS.....	68
6.7.1	<i>DNS Server</i>	68
6.7.2	<i>Dynamic DNS</i>	69
6.8	DSL.....	71
6.9	PORT MAPPING.....	72
6.10	CERTIFICATE.....	74
6.10.1	<i>Local</i>	74
6.10.2	<i>Trusted CA</i>	76
CHAPTER 7	DIAGNOSTICS	77
CHAPTER 8	MANAGEMENT	79
8.1	SETTINGS.....	79
8.1.1	<i>Configuration Backup</i>	80
8.1.2	<i>Tools – Update Settings</i>	81
8.1.3	<i>Restore Default</i>	82
8.2	SYSTEM LOG.....	84
8.3	TR-069 CLIENT.....	87
8.4	INTERNET TIME.....	89
8.5	ACCESS CONTROL.....	90
8.5.1	<i>Services</i>	91
8.5.2	<i>Access IP Addresses</i>	92
8.5.3	<i>Passwords</i>	93
8.6	UPDATE SOFTWARE.....	94
8.7	SAVE AND REBOOT.....	95
APPENDIX A:	FIREWALL	96
APPENDIX B:	PIN ASSIGNMENTS	102

APPENDIX C: SPECIFICATIONS.....	103
APPENDIX D: SSH CLIENT	105

Chapter 1 Introduction

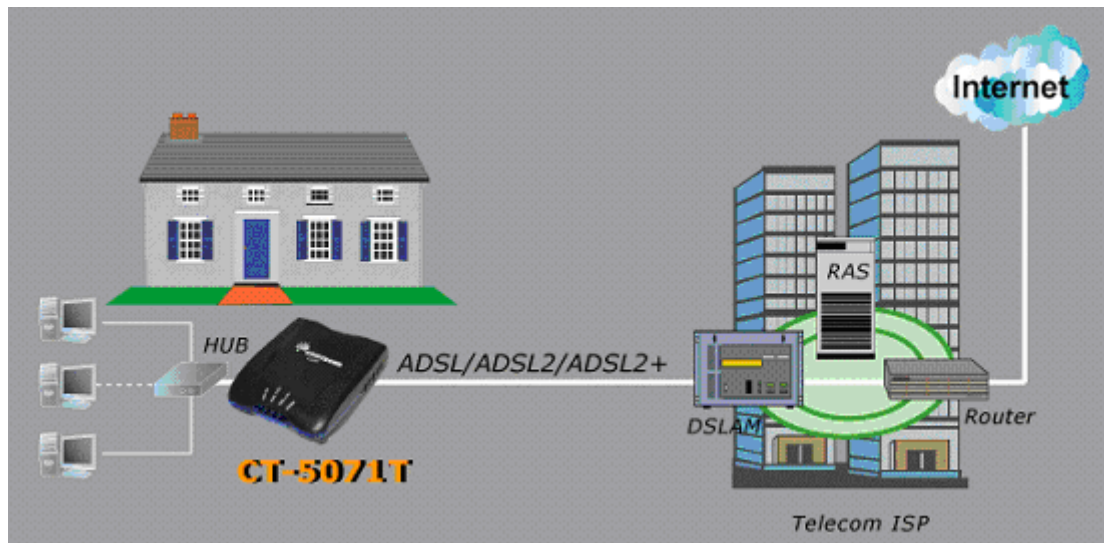
The CT-5071T ADSL2+ compact and high performance Ethernet router provides one 10/100 Ethernet Interface and offers ADSL connectivity at speeds of up to 24 Mbps. It also has full routing capabilities to segment/route IP protocol, and supports advanced security functions.

1.1 Features

- Supports TR-069
- TR-068 compliant
- IP filtering
- SPI (Stateful Packet Inspection)
- DoS protection
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- NAT/PAT
- IGMP proxy
- DHCP server/relay/client
- DNS proxy
- Auto PVC configuration
- Up to 8 VCs
- Web-based management
- Remote configuration and upgrade
- Configuration backup and restoration
- FTP/TFTP server
- Embedded SNMP agent
- IP/MAC address filtering

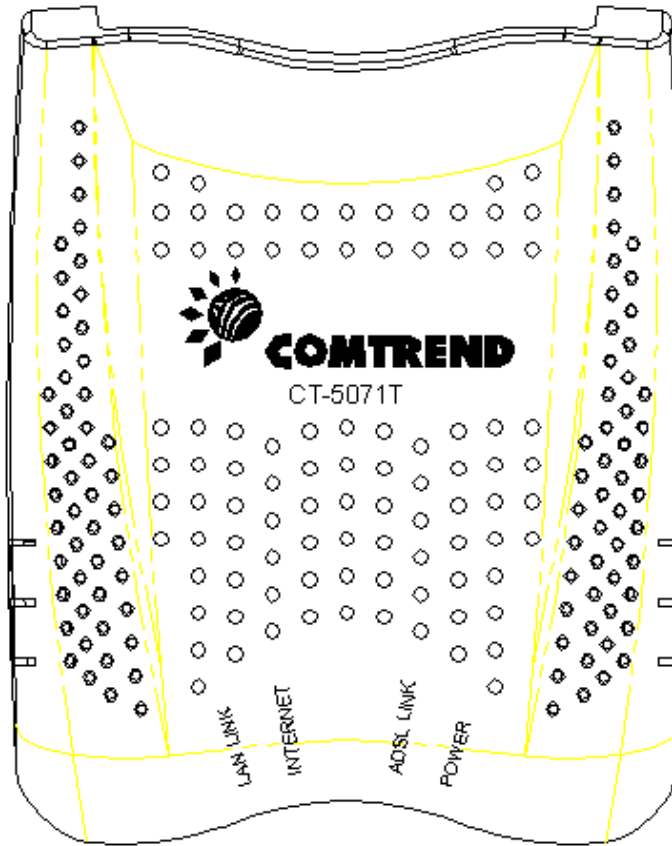
1.2 Application

The following diagram depicts the application of the CT-5071T.



1.3 Front Panel LED Indicators

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



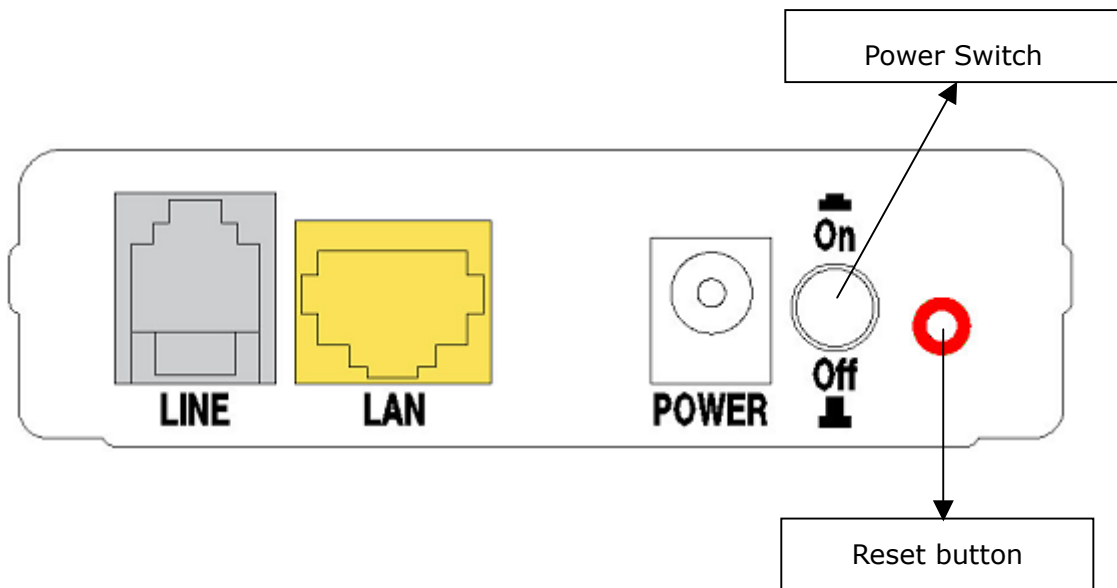
LED	Color	Mode	Function
POWER	Green	On	The router is powered up.
		Off	The router is powered down.
ADSL LINK	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
	Green	Blink	The ADSL link is training.
INTERNET	Green	On	IP connected and no traffic detected.
		Off	Modem power off, modem in bridged mode or ADSL connection not present.
	Green	Blink	IP connected and IP Traffic is passing thru the device (either direction)

	Red	On	<p>Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)</p> <p>For bridged mode, the indicator light is off.</p> <p>If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.</p>
LAN LINK	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.

Chapter 2 Installation

2.1 Hardware Installation

In the rear panel, there is a reset button. It is used to load the factory default settings. Hold down the button until the LED's start blinking simultaneously (about 5 seconds). After the device has booted successfully, the factory default settings are retrieved.



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 one LAN device. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

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, push the power switch in, to the on position. After powering 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 this equipment always disconnect all power cords and telephone lines from the wall outlet.

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 5.0 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.

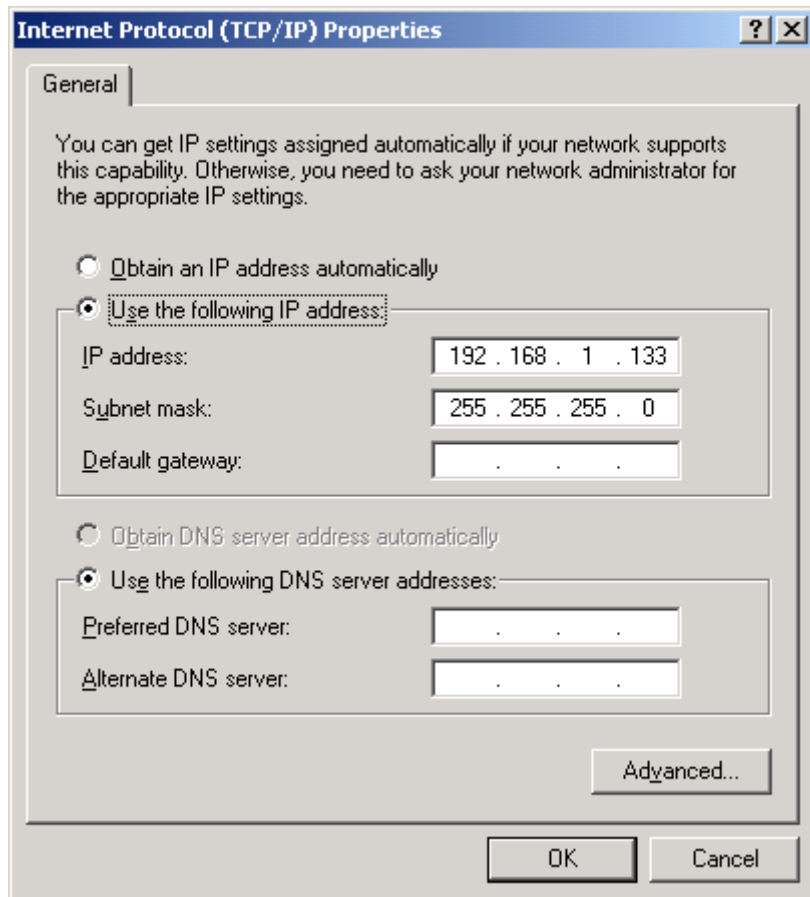
3.1 IP Address

The default IP address of the CT-5071T (LAN port) is 192.168.1.1. To configure the CT-5071T 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.

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.



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

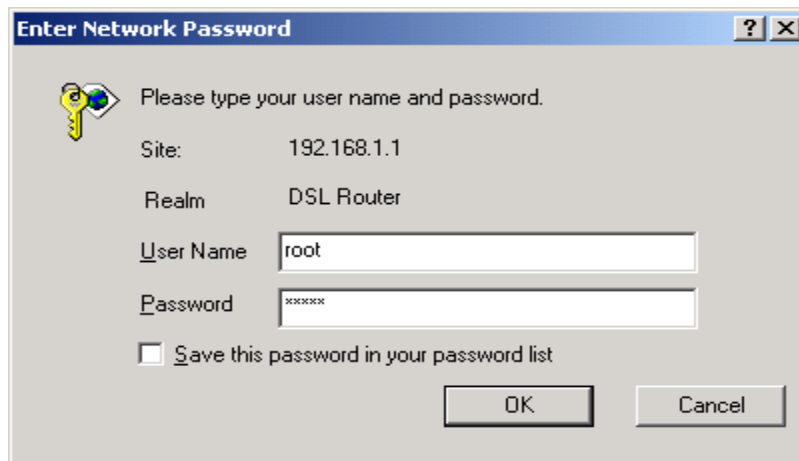
STEP 4: Start your Internet browser and type the IP address for the router (192.168.1.1) in the Web address bar.

3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-5071T. 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

OK Cancel

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



COMTREND
ADSL Router

Quick Setup

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

ATM PVC Configuration

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

DSL Auto-connect

Device Info
Quick Setup
Advanced Setup
Diagnostics
Management

3.3 Default Settings

During power on initialization, the CT-5071T 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. The PC running the browser can be attached to the Ethernet.

- 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: disabled
- Remote WAN access account name: support
- Remote WAN access account password: support
- NAT and firewall: disabled
- DHCP server on LAN interface: enable
- WAN IP address: none

Chapter 4 Quick Setup

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



COMTREND
ADSL Router

Quick Setup

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

ATM PVC Configuration

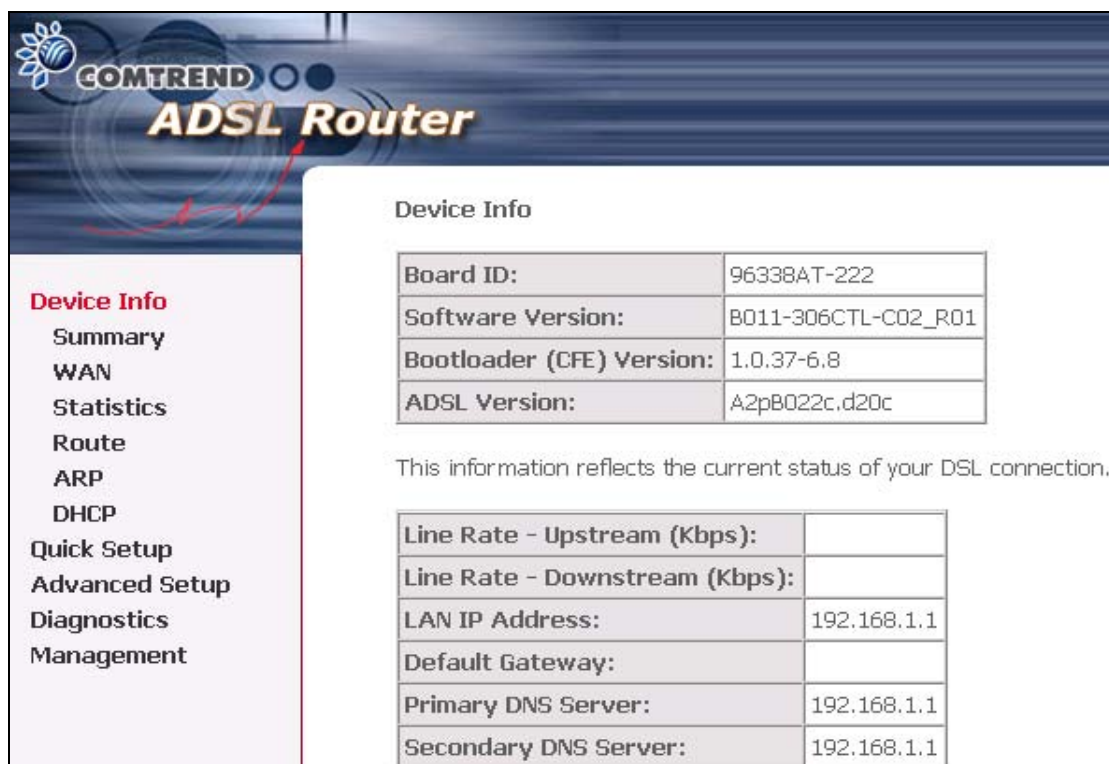
Select the check box below to enable DSL Auto-connect process.

DSL Auto-connect

Next

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

Shown here is the **Device Info** screen for your reference.



COMTREND
ADSL Router

Device Info

Board ID:	96338AT-222
Software Version:	B011-306CTL-C02_R01
Bootloader (CFE) Version:	1.0.37-6.8
ADSL Version:	A2pB022c.d20c

This information reflects the current status of your DSL connection.

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

4.1 WAN

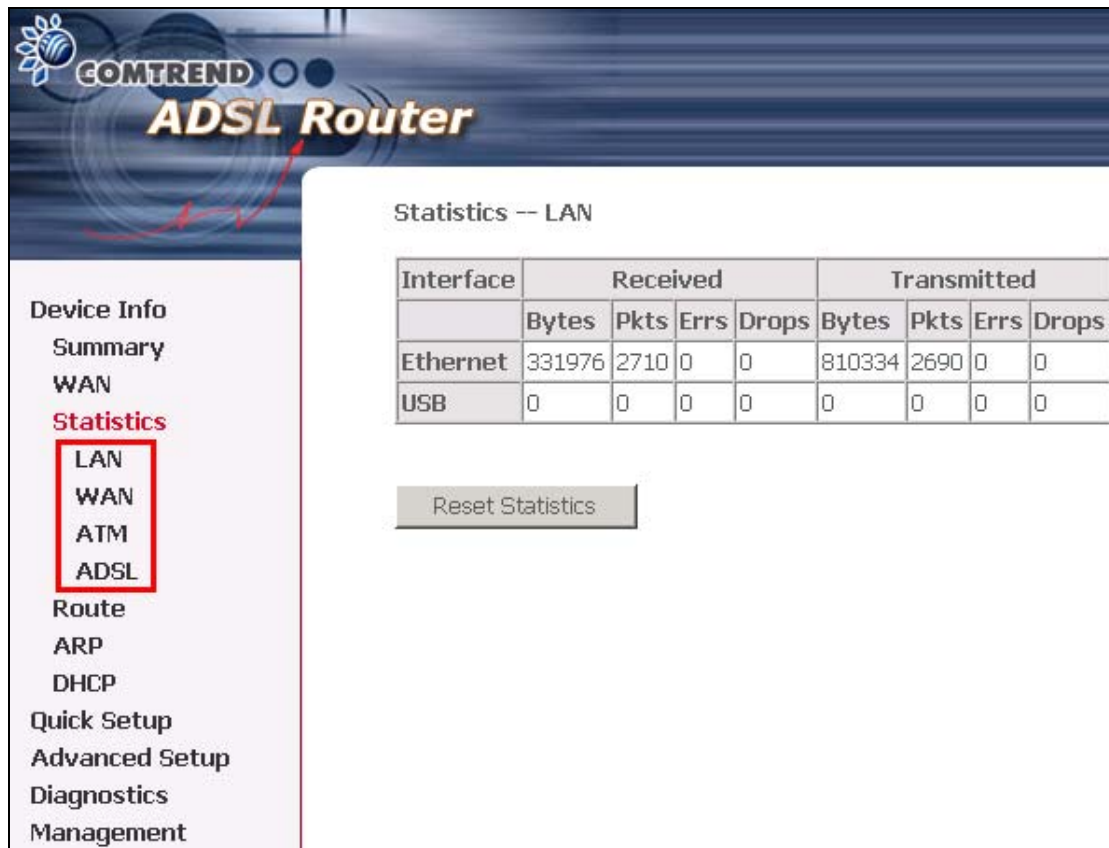
Click **Device Info** on the menu bar to display the WAN option. Then, click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



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 interface
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
QoS	Shows if IP QoS is enabled or disabled
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 and ADSL. All statistics screens are updated every 15 seconds.



The screenshot shows the Comtrend ADSL Router web interface. The main content area displays the "Statistics -- LAN" screen. On the left, there is a navigation menu with the following items: Device Info, Summary, WAN, Statistics (highlighted in red), LAN (highlighted with a red box), WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area contains a table with the following data:

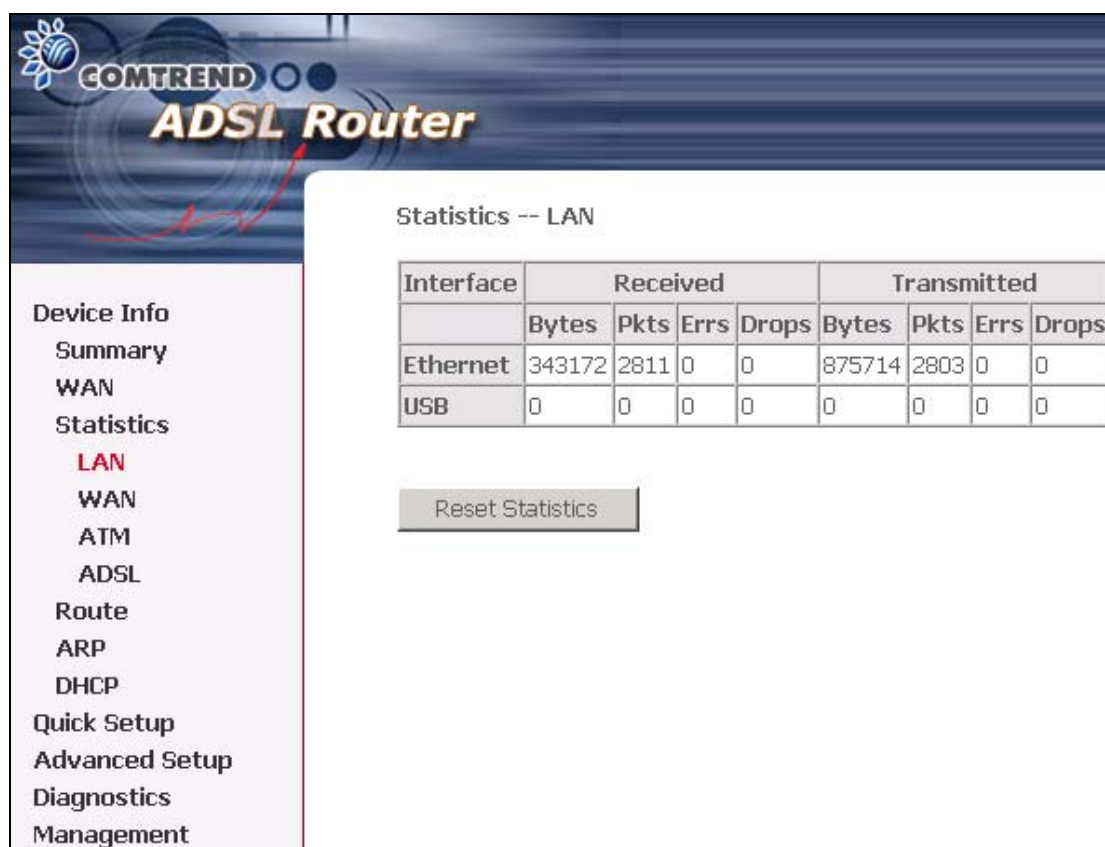
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	331976	2710	0	0	810334	2690	0	0
USB	0	0	0	0	0	0	0	0

Below the table, there is a "Reset Statistics" button.

Note: This device does not support a USB interface.

4.2.1 LAN Statistics

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



The screenshot displays the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and the text "ADSL Router". On the left side, there is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, LAN (highlighted in red), WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area is titled "Statistics -- LAN" and contains a table with the following data:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	343172	2811	0	0	875714	2803	0	0
USB	0	0	0	0	0	0	0	0

Below the table, there is a "Reset Statistics" button.

Note: This device does not support a USB interface.

4.2.2 WAN Statistics

The screenshot shows the Comtrend ADSL Router web interface. The main content area is titled "Statistics -- WAN" and contains a table with the following structure:

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

Below the table is a "Reset Statistics" button.

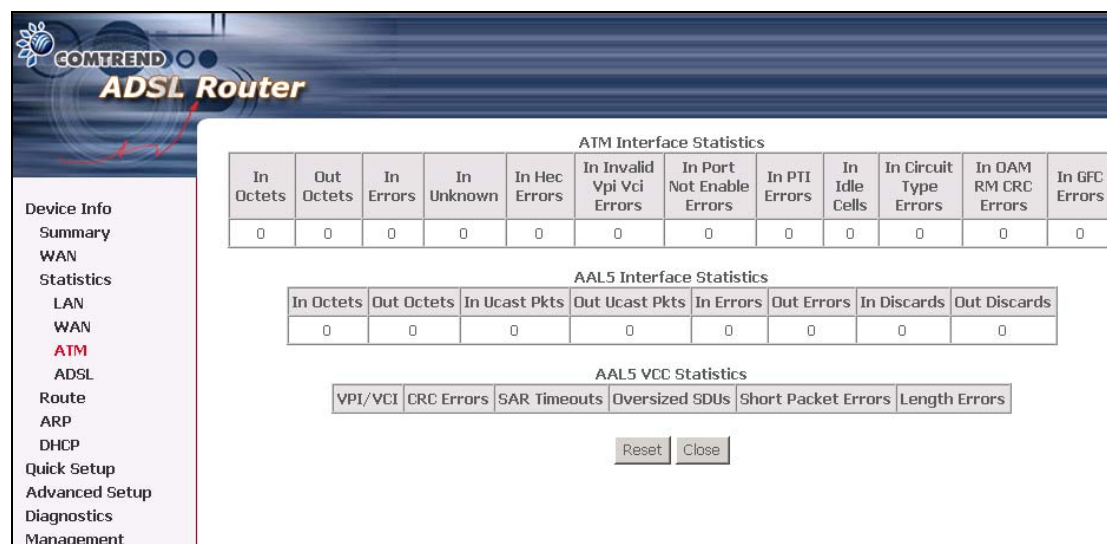
The left navigation menu includes the following items:

- Device Info
 - Summary
 - WAN
 - Statistics
 - LAN
 - WAN**
 - ATM
 - ADSL
- Route
- ARP
- DHCP
- Quick Setup
- Advanced Setup
- Diagnostics
- Management

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 interface
Received/Transmitted	<ul style="list-style-type: none"> - Bytes Rx/TX (receive/transmit) packet in Bytes - Pkts Rx/TX (receive/transmit) packets - Errs Rx/TX (receive/transmit) the errored packets - Drops Rx/TX (receive/transmit) dropped packets

4.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

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

ATM AAL5 LAYER STATISTICS FOR EACH VCC OVER ADSL INTERFACE

Field	Description
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.

COMTREND
ADSL Router

Statistics -- ADSL

Mode:		
Type:		
Line Coding:		
Status:		Link Down
Link Power State:		LO
	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:		N/A
Data Cells:		N/A
Bit Errors:		N/A
Total ES:		
Total SES:		
Total UAS:		

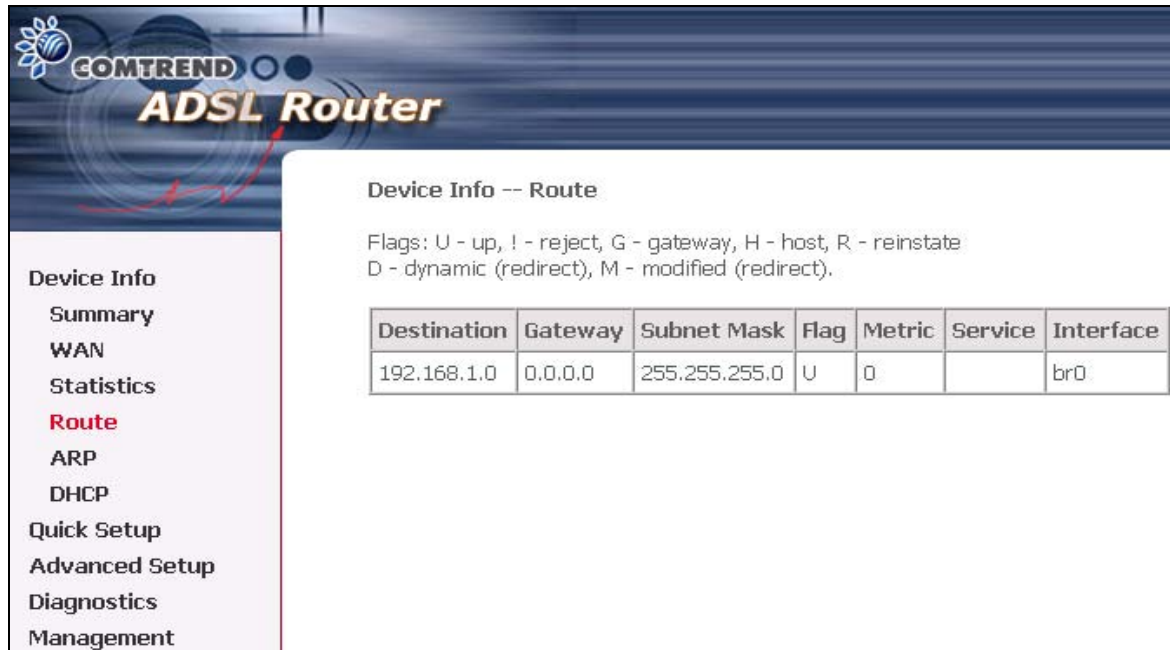
ADSL BER Test Reset Statistics

Device Info
Summary
WAN
Statistics
 LAN
 WAN
 ATM
 ADSL
Route
 ARP
 DHCP
Quick Setup
Advanced Setup
Diagnostics
Management

Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, ADSL2+, AnnexL, AnnexM
Type	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
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

4.2.5 Route

Choose **Route** to display the routes that the router has learned.

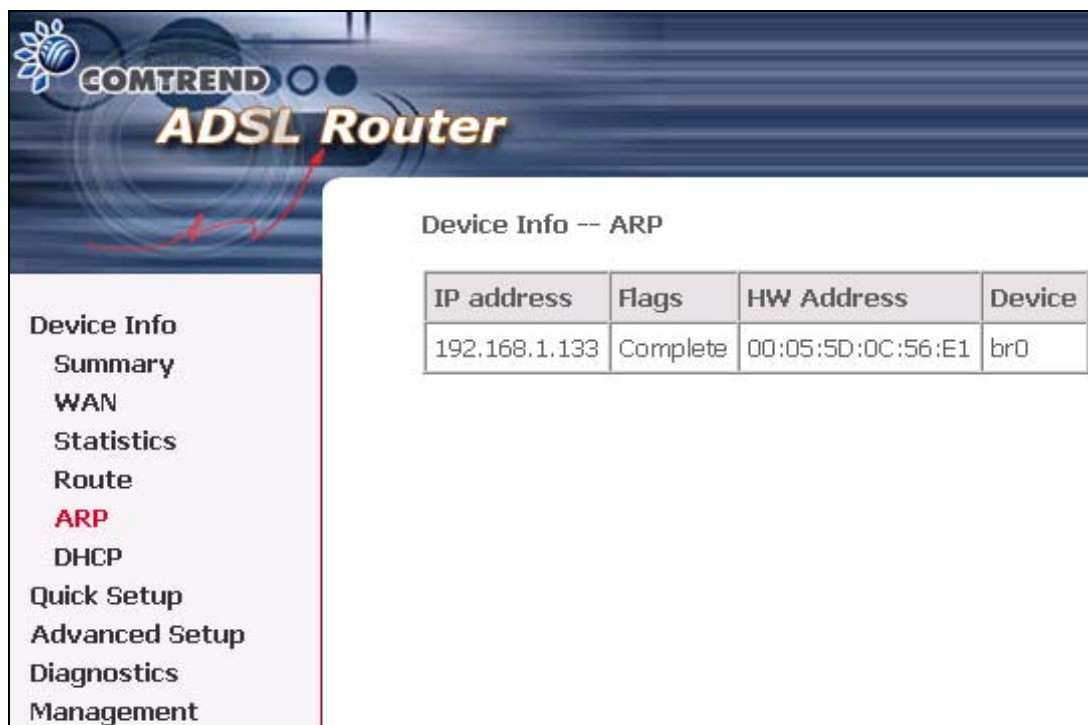


The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, **Route** (highlighted in red), ARP, DHCP, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area is titled "Device Info -- Route" and includes a legend for flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Below the legend is a table with the following data:

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

4.2.6 ARP

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

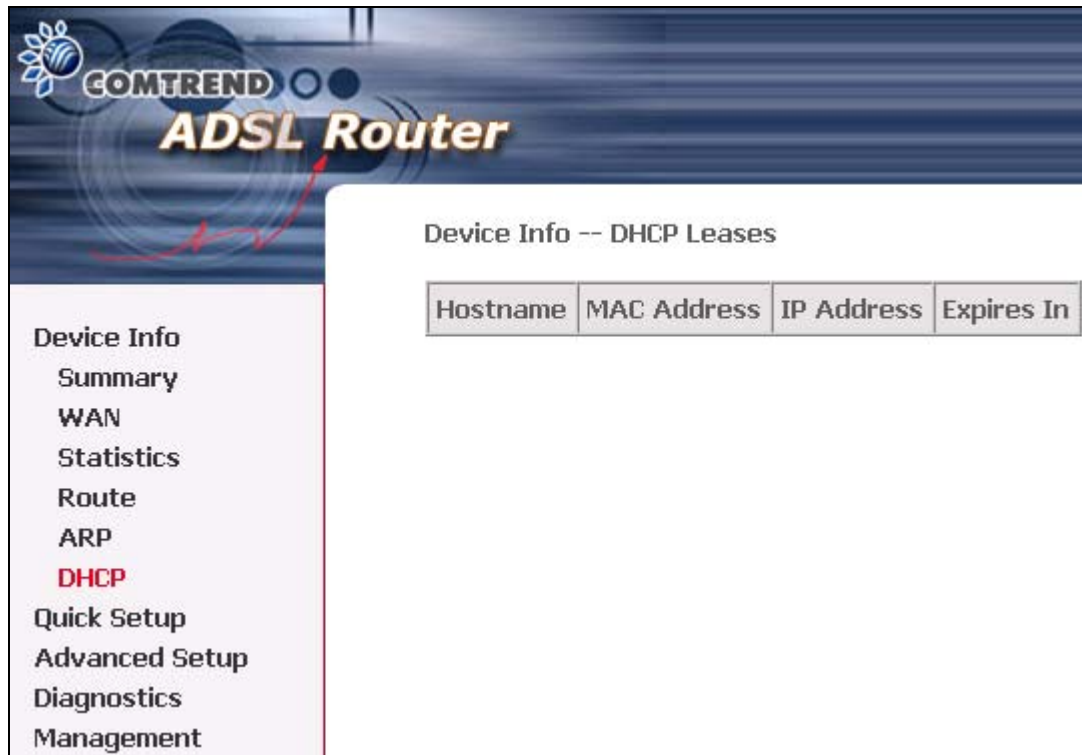


The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a menu with the following items: Device Info, Summary, WAN, Statistics, Route, **ARP** (highlighted in red), DHCP, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area is titled "Device Info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

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

4.2.7 DHCP

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



The screenshot displays the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and the text "ADSL Router". On the left side, there is a vertical navigation menu with the following items: "Device Info", "Summary", "WAN", "Statistics", "Route", "ARP", "DHCP" (highlighted in red), "Quick Setup", "Advanced Setup", "Diagnostics", and "Management". The main content area is titled "Device Info -- DHCP Leases" and contains a table with the following headers: "Hostname", "MAC Address", "IP Address", and "Expires In".

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

Chapter 5 Quick Setup

The Quick Setup allows the user to configure the ADSL router for DSL connectivity and Internet access. It also guides the user through 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-5071T ADSL 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-5071T is to run the PPPoE client. The CT-5071T 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-5071T also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client for non-PPPoE LAN devices. NAT 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, NAT and firewall are always disabled when Bridge mode is selected.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main panel will display or hide the NAT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAT 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 ADSL link to be up. The ADSL router will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

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



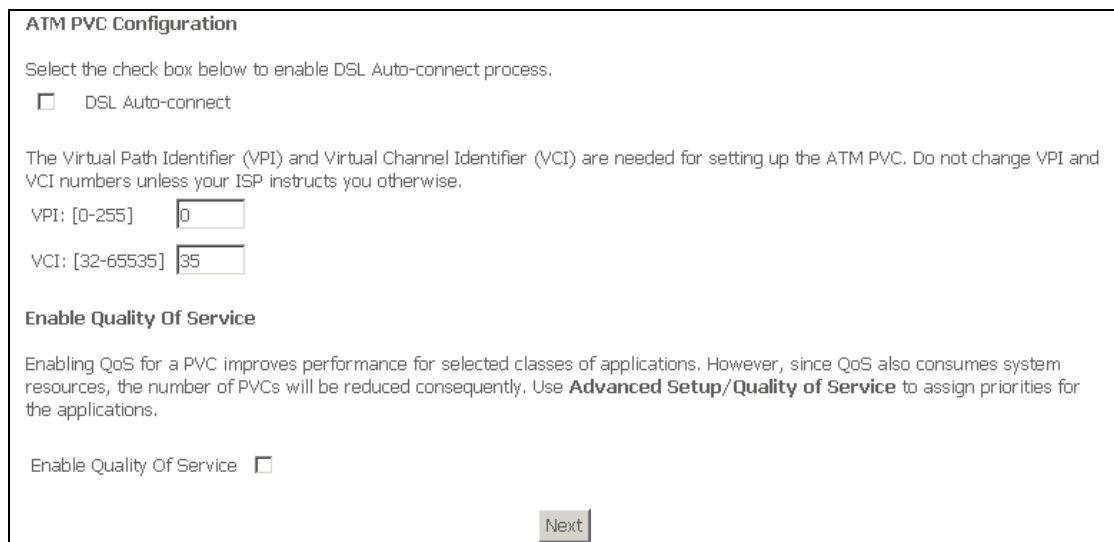
2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.
3. After the settings are complete, you can use the ADSL service.

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.



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



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

STEP 3: 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. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click on "Next" to go to next step.

COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

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

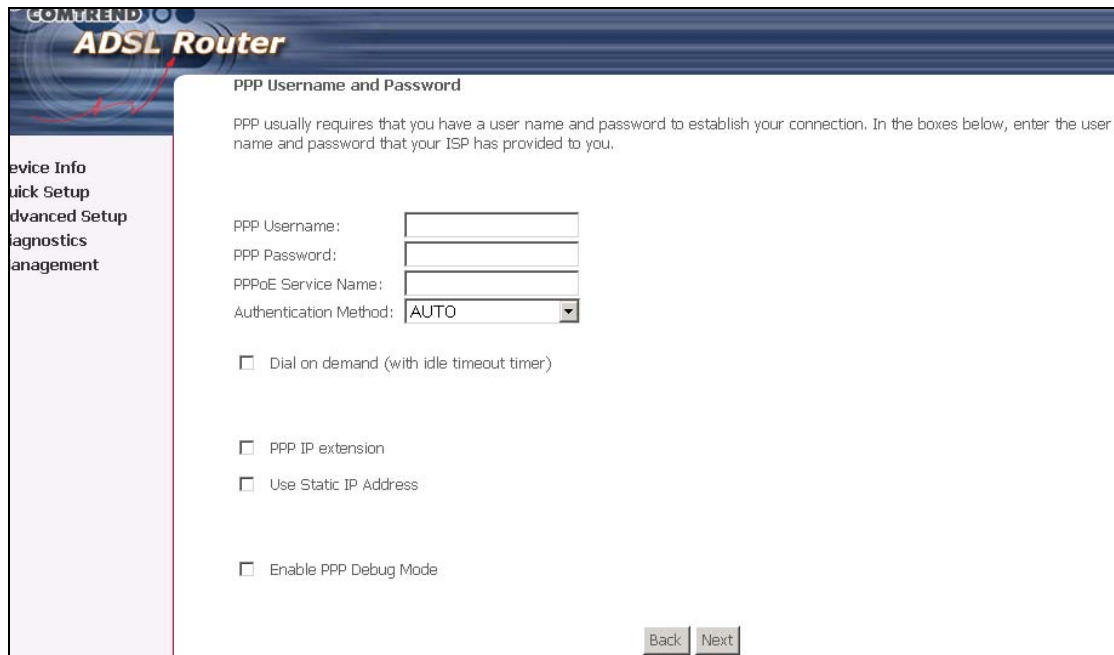
Enable 802.1q

Back Next

Enable 802.1q
VLAN ID[0-4095]:

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:



The screenshot shows the 'COMTREND ADSL Router' configuration interface. The main title is 'PPP Username and Password'. Below the title, there is a paragraph explaining that PPP usually requires a user name and password to establish a connection. The form contains the following fields and options:

- PPP Username: [Text Input Field]
- PPP Password: [Text Input Field]
- PPPoE Service Name: [Text Input Field]
- Authentication Method: [Dropdown Menu with 'AUTO' selected]
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Enable PPP Debug Mode

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

PPP USERNAME/PPP PASSWORD/ PPPOE SERVICE NAME:

The PPP Username, PPP password and the PPPoE Service Name entries 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.

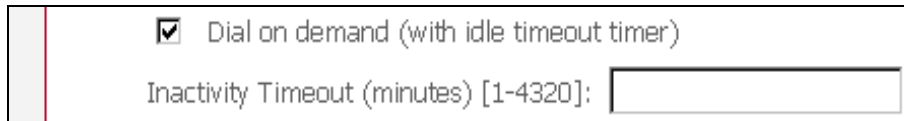
Encapsulation Mode

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

Disconnect if no activity

The CT-5071T can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** 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.



Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:

PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider 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

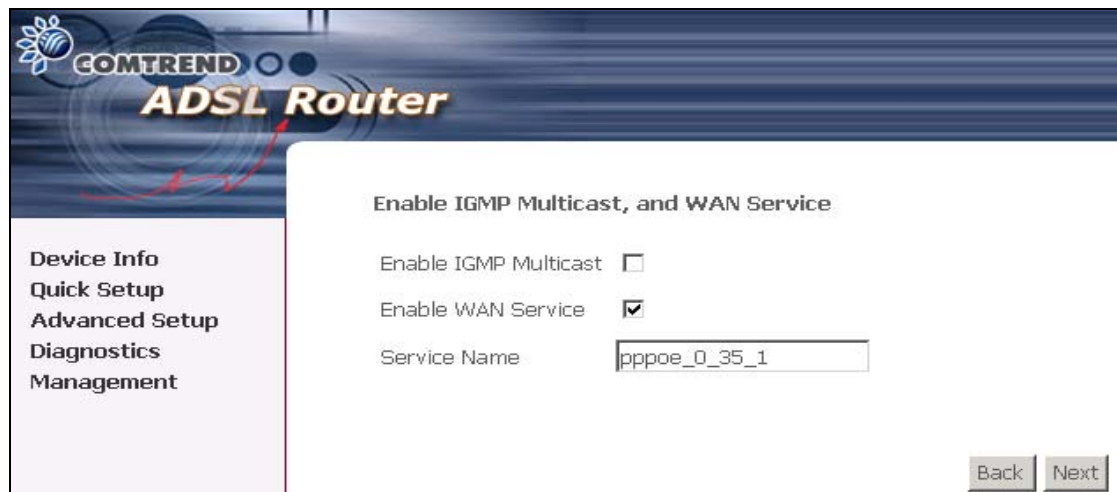
Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

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 ATM service. Untick it to stop the ATM service.

Service Name: This is user-defined.



The screenshot shows the configuration interface for a COMTREND ADSL Router. The title bar reads "COMTREND ADSL Router". On the left, there is a navigation menu with the following items: "Device Info", "Quick Setup", "Advanced Setup", "Diagnostics", and "Management". The main content area is titled "Enable IGMP Multicast, and WAN Service". It contains three settings:

- "Enable IGMP Multicast" with an unchecked checkbox.
- "Enable WAN Service" with a checked checkbox.
- "Service Name" with a text input field containing the value "pppoe_0_35_1".

At the bottom right of the main content area, there are two buttons: "Back" and "Next".

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.

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.

4. 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.

COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
Diagnostics
Management

WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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.

5. 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-5071T 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.

The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with 'Quick Setup' selected. The main content area is titled 'WAN IP Settings' and contains instructions and configuration options. The instructions state that DHCP can be enabled for PVC in MER mode if 'Obtain an IP address automatically' is chosen, and that changing default gateway or DNS affects the whole system. There are three main sections of options: 1) Obtain an IP address automatically (selected) vs. Use the following IP address (with fields for WAN IP Address and WAN Subnet Mask). 2) Obtain default gateway automatically (selected) vs. Use the following default gateway (with checkboxes for 'Use IP Address' and 'Use WAN Interface', and a dropdown menu for the WAN interface). 3) Obtain DNS server addresses automatically (selected) vs. Use the following DNS server addresses (with fields for Primary and Secondary DNS servers). 'Back' and 'Next' buttons are at the bottom right.

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.



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 disabled.

Enable Firewall checkbox: If the firewall checkbox is selected, the Security 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 Security submenu will not be displayed on the left main panel.

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 service. If this item is not selected, you will not be able to use the WAN service.

Service Name: This is User-defined.

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

COMTREND ADSL Router

Device Setup

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

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Enable DHCP Server Relay

DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

Back Next

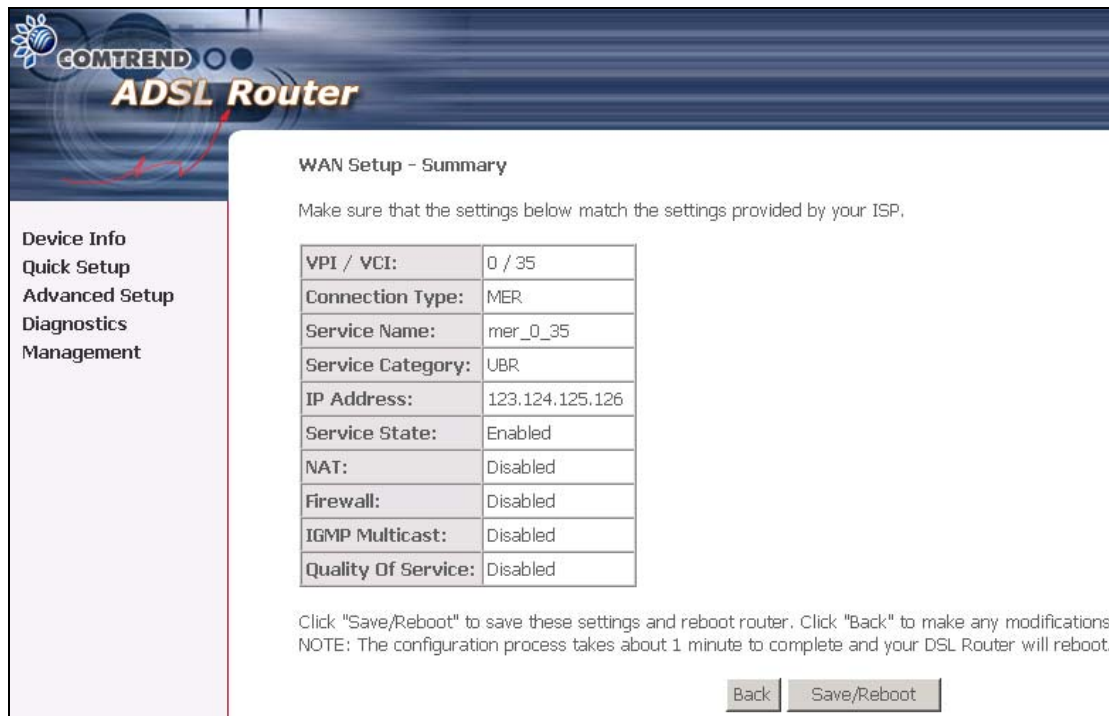
Device Info
Quick Setup
Advanced Setup
Diagnostics
Management

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.

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.



COMTREND
ADSL Router

Device Info
Quick Setup
Advanced Setup
Diagnostics
Management

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:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

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-5071T 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.

The screenshot shows the WAN IP Settings page of the COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with 'Quick Setup' selected. The main content area is titled 'WAN IP Settings' and contains the following elements:

- A note: '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.'
- Input fields for 'WAN IP Address' (123.124.125.126) and 'WAN Subnet Mask' (255.255.255.0).
- A section for 'Use the following default gateway:' with checkboxes for 'Use IP Address' and 'Use WAN Interface' (selected, with a dropdown menu showing 'ipoa_0_35/ipa_0_35').
- A section for 'Use the following DNS server addresses:' with input fields for 'Primary DNS server' and 'Secondary DNS server'.
- 'Back' and 'Next' buttons at the bottom right.

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.

The screenshot shows the Network Address Translation Settings page of the COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with 'Quick Setup' selected. The main content area is titled 'Network Address Translation Settings' and contains the following elements:

- A note: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).'
- Checkboxes for 'Enable NAT' and 'Enable Firewall', both unchecked.
- A section for 'Enable IGMP Multicast, and WAN Service' with checkboxes for 'Enable IGMP Multicast' (unchecked) and 'Enable WAN Service' (checked).
- An input field for 'Service Name' with the value 'ipoa_0_35'.
- 'Back' and 'Next' buttons at the bottom right.

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 (i.e. the LAN side is using a public IP), this checkbox should be de-selected. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Enable Firewall checkbox

If the firewall checkbox is selected, the Security 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 Security submenu will not be displayed on the left main panel.

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.

COMTREND
ADSL Router

Device Setup

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

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

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.

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.

COMTREND ADSL Router

WAN Setup - Summary

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

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

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

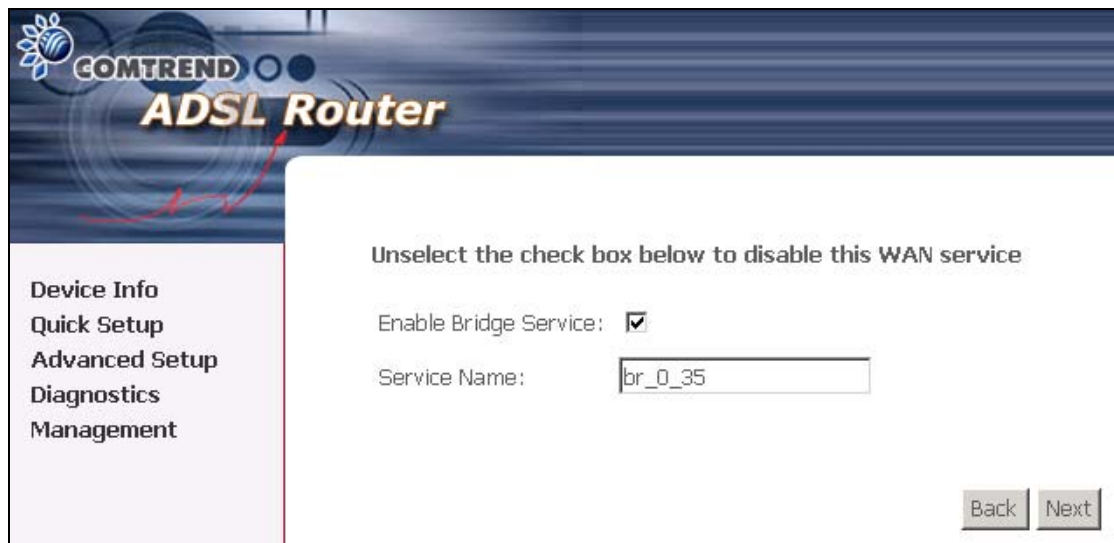
[Back](#) [Save/Reboot](#)

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-5071T 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.



The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main area has a header with the COMTREND logo and 'ADSL Router'. Below the header, it says 'Unselect the check box below to disable this WAN service'. There is a checkbox for 'Enable Bridge Service' which is checked. Below it is a text input field for 'Service Name' containing 'br_0_35'. At the bottom right are 'Back' and 'Next' buttons.

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.



The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main area has a header with the COMTREND logo and 'ADSL Router'. Below the header, it says 'Device Setup'. Underneath, it says 'Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN)'. There are two text input fields: 'IP Address' containing '192.168.1.1' and 'Subnet Mask' containing '255.255.255.0'. At the bottom right are 'Back' and 'Next' buttons.

6. Click **Next** and the following screen will be displayed

The screenshot shows the WAN Setup - Summary screen for a COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area is titled 'WAN Setup - Summary' and includes a note: 'Make sure that the settings below match the settings provided by your ISP.' Below this is a table with the following settings:

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

Below the table, there is a note: '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.' At the bottom right, there are two buttons: 'Back' and 'Save/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, and DNS.....

Note: The options displayed in the menu bar depend on what WAN interface is set up.

The screenshot shows the 'Wide Area Network (WAN) Setup' page. The left sidebar contains a menu with 'Advanced Setup' expanded to show 'WAN' selected. The main content area has instructions: 'Choose Add, Edit, or Remove to configure WAN interfaces. Choose Save/Reboot to apply the changes and reboot the system.' Below this is a table with the following data:

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit
0/35	1	UBR	pppoe_0_35_1	ppp_0_35_1	PPPoE	Disabled	Enabled	N/A	Enabled	<input type="checkbox"/>	Edit

Buttons for 'Add', 'Remove', and 'Save/Reboot' are located below the table.

This screenshot is for PPPoE and PPPoA encapsulations.

The screenshot shows the 'Outgoing IP Filtering Setup' page. The left sidebar menu has 'Security' expanded to show 'IP Filtering' selected. The main content area has instructions: '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.' Below this is a table with the following data:

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

Buttons for 'Add' and 'Remove' are located below the table.

This screenshot is for Mer and IPoA encapsulations.

COMTREND
ADSL Router

Device Info
Advanced Setup
WAN
LAN
Security
MAC Filtering
Parental Control
Quality of Service
Routing
DSL
Port Mapping
Certificate
Diagnostics
Management

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

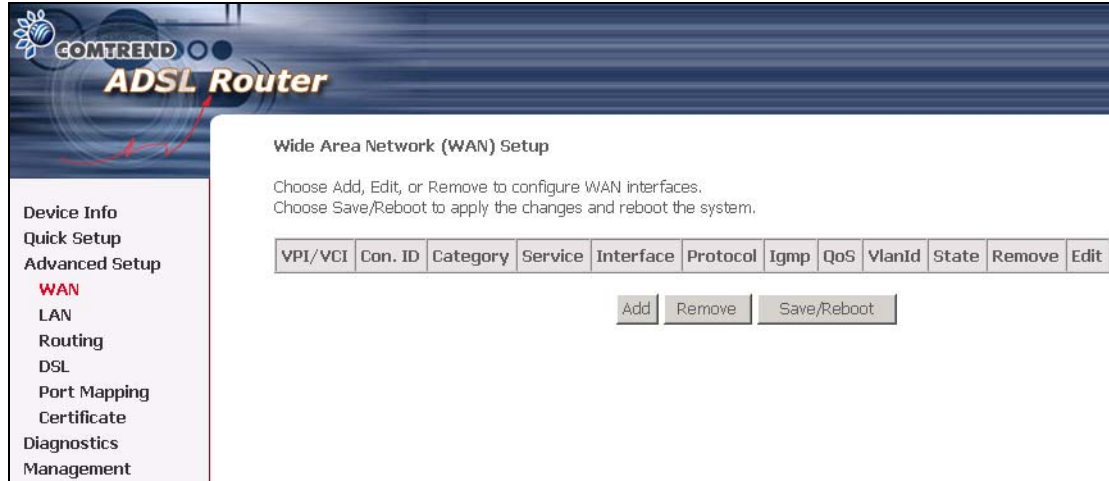
MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching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

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
---------	----------	-----------------	------------	-----------------	--------

This screenshot is for Bridge encapsulation.

6.1 WAN



VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR...
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
IGMP	Shows enable or disable IGMP proxy
QoS	Shows enable or disable QoS
VlanID	* This function means one can add a 802.1Q VLAN tag on PPPoE/MER or Bridge mode.
State	Shows enable or disable WAN connection

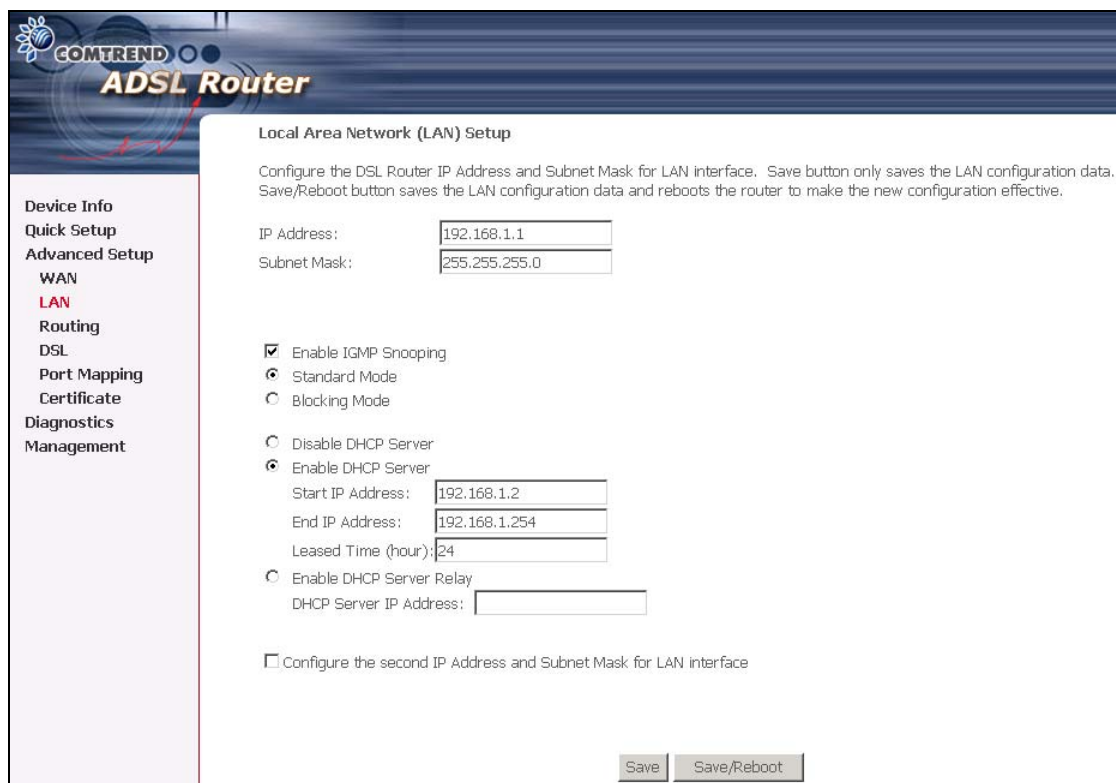
* It means the packet sends to WAN and it will be added specific Vlan Id(802.1Q tag) on Ethernet header. The VlanID shows to which 802.1Q tag will be added.

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.



The screenshot shows the 'Local Area Network (LAN) Setup' page of a COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, WAN, LAN (highlighted in red), Routing, DSL, Port Mapping, Certificate, Diagnostics, and Management. The main content area is titled 'Local Area Network (LAN) Setup' and contains the following configuration options:

- IP Address:
- Subnet Mask:
- Enable IGMP Snooping
 - Standard Mode
 - Blocking Mode
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address:
 - End IP Address:
 - Leased Time (hour):
- Enable DHCP Server Relay
 - DHCP Server IP Address:
- Configure the second IP Address and Subnet Mask for LAN interface

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

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.

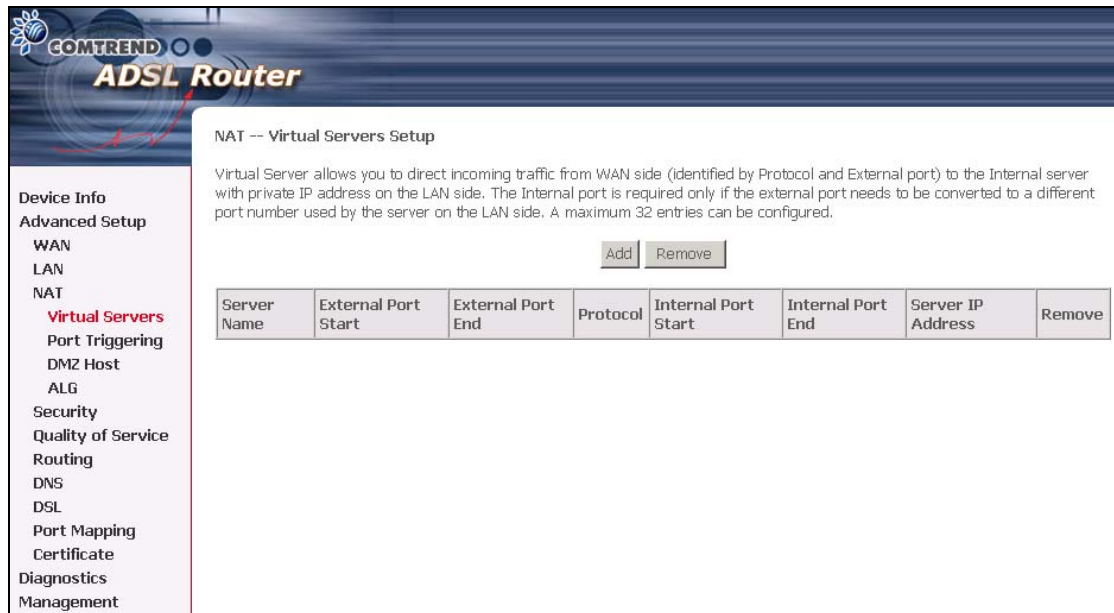
Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.3 NAT

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

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.

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

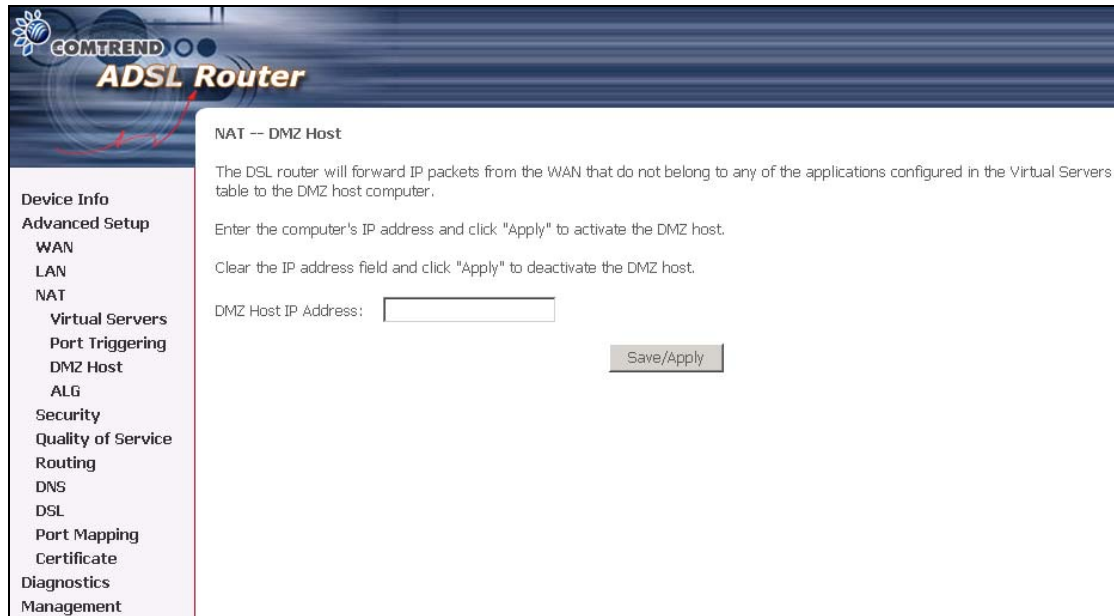
Custom application:

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

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.



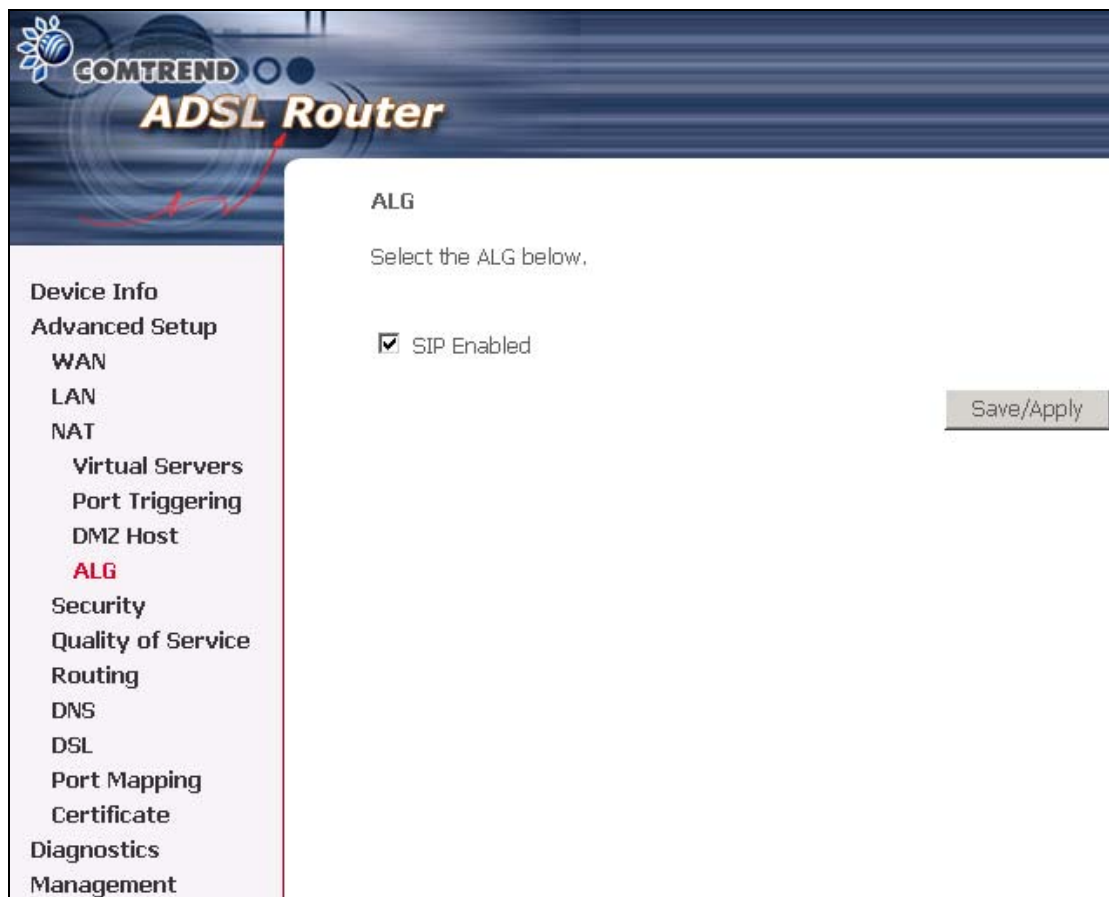
The screenshot shows the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Virtual Servers, Port Triggering, DMZ Host, ALG, Security, Quality of Service, Routing, DNS, DSL, Port Mapping, Certificate, Diagnostics, and Management. The main content area is titled "NAT -- DMZ Host" and contains the following text: "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." Below this, there are two instructions: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." A text input field labeled "DMZ Host IP Address:" is present, followed by a "Save/Apply" button.

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).



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

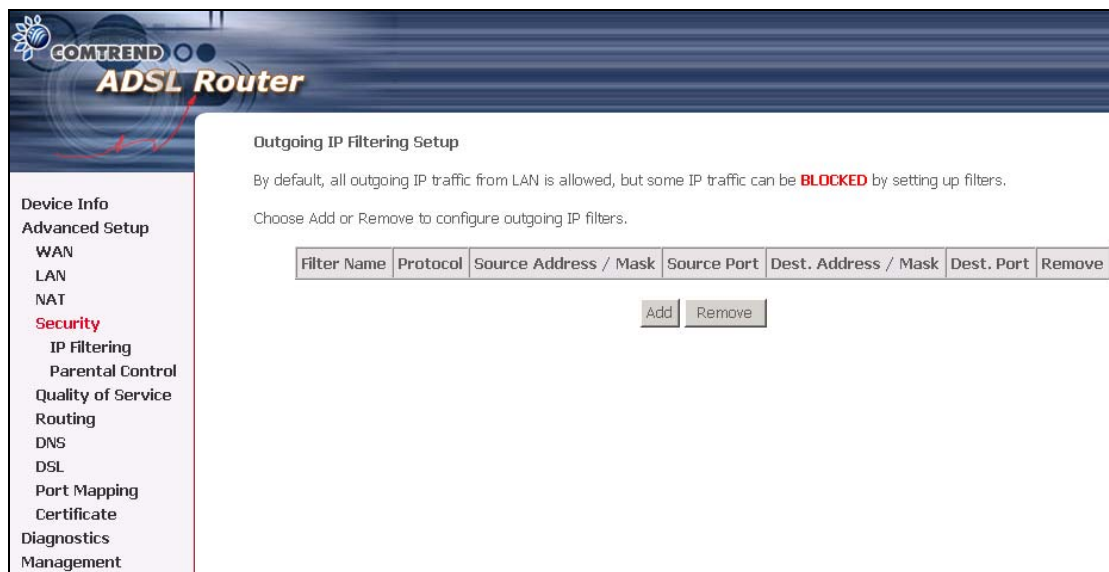
To display the Security function, you need to enable the firewall feature in the WAN Setup.

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

Note: The default setting for all Outgoing traffic is Accepted.



The screenshot shows the COMTREND ADSL Router web interface. The main heading is "Outgoing IP Filtering Setup". Below the heading, there is a paragraph: "By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters." followed by "Choose Add or Remove to configure outgoing IP filters." Below this text is a table with the following columns: Filter Name, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are two buttons: "Add" and "Remove". On the left side of the interface, there is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security (highlighted in red), IP Filtering, Parental Control, Quality of Service, Routing, DNS, DSL, Port Mapping, Certificate, Diagnostics, and Management.

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

COMTREND ADSL Router

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

Note: The default setting for all Incoming traffic is Blocked.

The screenshot shows the 'Incoming IP Filtering Setup' page. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup (WAN, LAN, NAT), Security (IP Filtering, Outgoing, Incoming), Parental Control, Quality of Service, Routing, DNS, DSL, Port Mapping, Certificate, Diagnostics, and Management. The main content area is titled 'Incoming IP Filtering Setup' and contains the following text: '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.' Below this is the instruction: 'Choose Add or Remove to configure incoming IP filters.' A table with the following headers is displayed: Filter Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are two buttons: 'Add' and 'Remove'.

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

The screenshot shows the 'Add IP Filter -- Incoming' page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Add IP Filter -- Incoming' and contains the following text: '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.' Below this is a form with the following fields: Filter Name (text input), Protocol (dropdown menu), Source IP address (text input), Source Subnet Mask (text input), Source Port (port or port:port) (text input), Destination IP address (text input), Destination Subnet Mask (text input), and Destination Port (port or port:port) (text input). Below the form is the section 'WAN Interfaces (Configured in Routing mode and with firewall enabled only)' with the instruction: 'Select at least one or multiple WAN interfaces displayed below to apply this rule.' There are two checkboxes: 'Select All' (checked) and 'pppoe_0_35_1/ppp_0_35_1' (checked). At the bottom right is a 'Save/Apply' button.

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.

COMTREND ADSL Router

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

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

Add Remove

Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management

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

COMTREND ADSL Router

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)

Save/Apply

Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Parental Control
Quality of Service
Routing
DNS
DSL
Port Mapping
Certificate
Diagnostics
Management

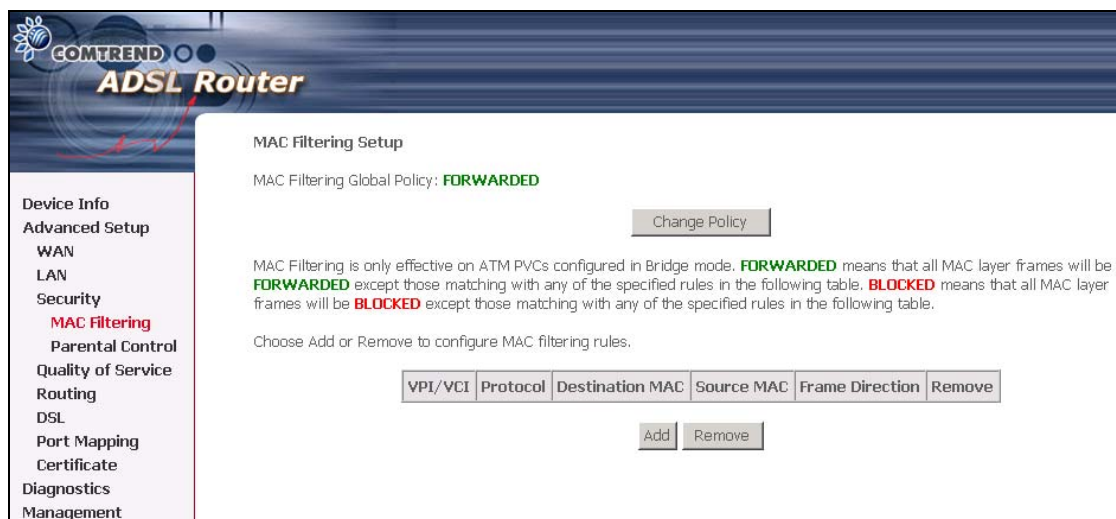
Username:	Input Internet access user name
MAC:	Set the MAC address to access the Internet
Mon, Tue, Wed, Thu, Fri, Sat, Sun:	Set which days that will have block restrictions to Internet access
Start, Stop:	Set Internet block start and stop time

6.4.3 MAC Filtering

Mac Filtering is only available when Bridging PVC is configured.

Each network device has a unique MAC address. You can block or forward the packets based on the MAC addresses. The MAC Filtering Setup screen allows setting up the MAC filtering policy and the MAC filtering rules. MAC Filtering is only effective on ATM PVCs configured in Bridge mode.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table. The default is FORWARD; you change by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen pops up when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Apply** to save and activate the filter.

Option	Description
Protocol type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Define the destination MAC address
Source MAC Address	Define the source MAC address
Frame Direction:	Select a direction of the frame
WAN Interface	Selects the interface that the MAC filter rule(s) will be applied. Only the WAN interface that is configured for bridged can be selected. <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <input checked="" type="checkbox"/> Select All <input checked="" type="checkbox"/> br_0_35/nas_0_35 </div>

6.5 Quality of Service

To display the QoS function, you need to enable the QoS feature in the WAN Setup (under Advanced Menu bar).

Choose **Add** to configure network traffic classes. The following screen will be displayed:

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.
IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Physical LAN Port	User can select the ENET interface.
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:

COMTREND ADSL Router

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 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 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:

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.



The screenshot shows the 'COMTREND ADSL Router' configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup (WAN, LAN, Routing, Default Gateway, Static Route, DSL, Port Mapping, Certificate, Diagnostics, Management). The 'Routing -- Default Gateway' section is active. It contains a title, a descriptive paragraph, a note about rebooting, and a checked checkbox for 'Enable Automatic Assigned Default Gateway'. A 'Save/Apply' button is at the bottom right.

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



This screenshot shows the same configuration page as above, but with the 'Enable Automatic Assigned Default Gateway' checkbox unselected. Below it, there are two unselected checkboxes: 'Use Default Gateway IP Address' with an adjacent text input field, and 'Use Interface' with an adjacent dropdown menu. The 'Save/Apply' button remains at the bottom right.

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.



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.



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.



COMTREND
ADSL Router

Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
Certificate
Diagnostics
Management

DNS Server Configuration

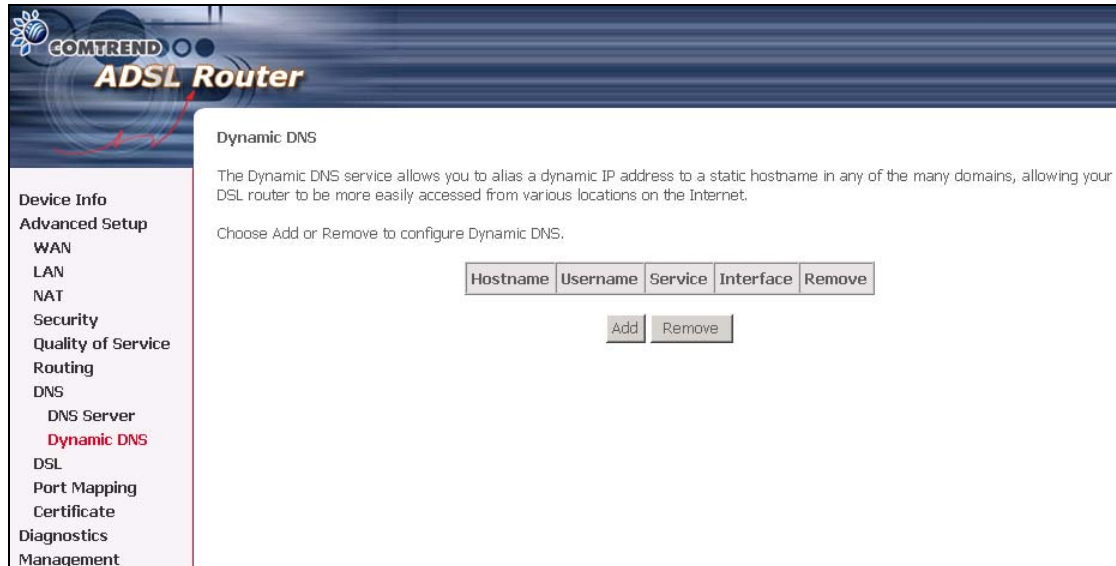
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.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

Enable Automatic Assigned DNS

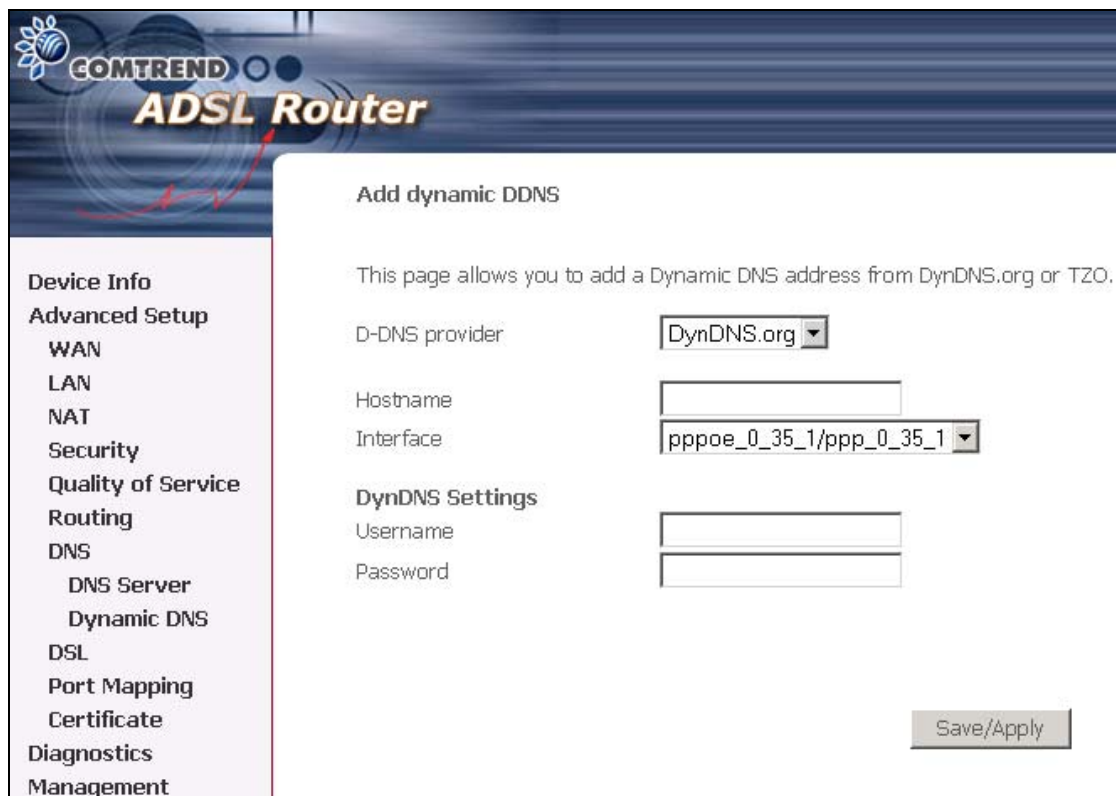
Save

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.



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



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.

Option	Description
G.dmt Enabled	Sets G.Dmt if you want the system to use G.Dmt mode.
G.Lite Enabled	Sets G.Lite if you want the system to use G.Lite mode.
T1.413 Enabled	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 Enabled	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 Port Mapping

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.

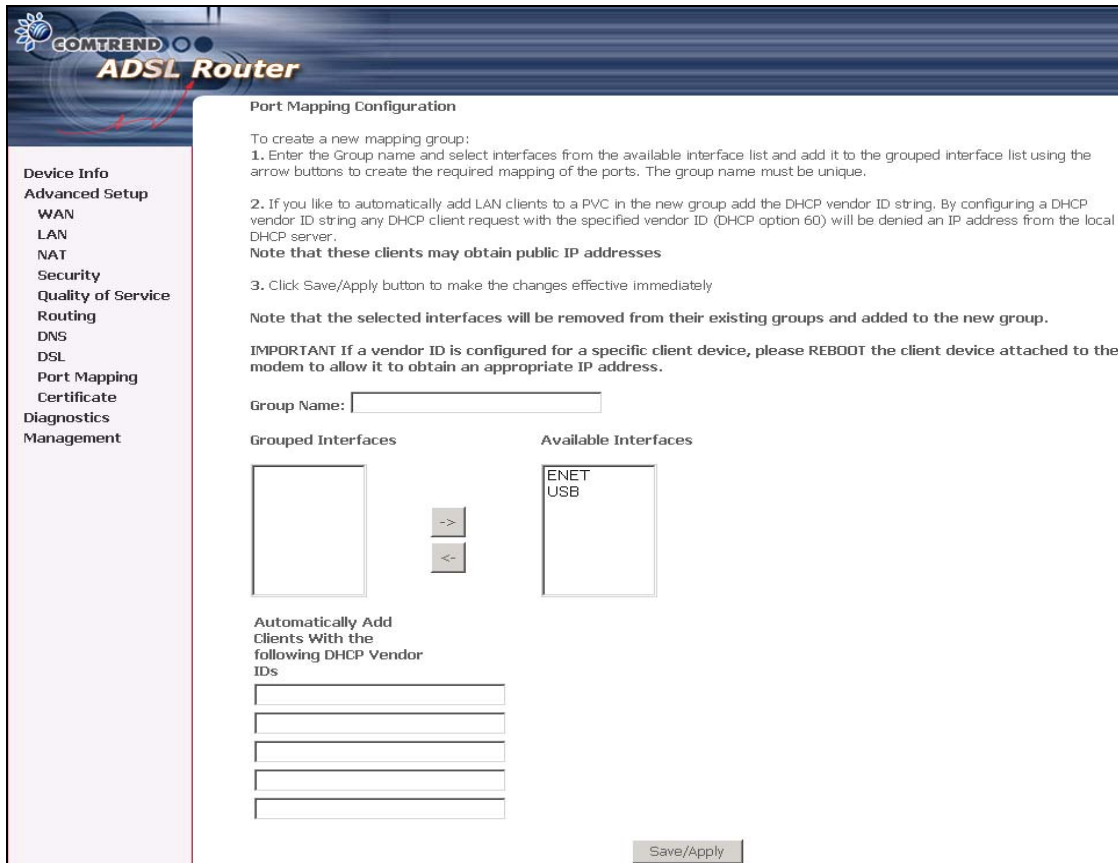
To add a port mapping group, simply click the Add button.

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.

Group Name	Interfaces	Remove	Edit
Default	ENET, USB		

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:

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.

Note: This device does not support a USB interface.

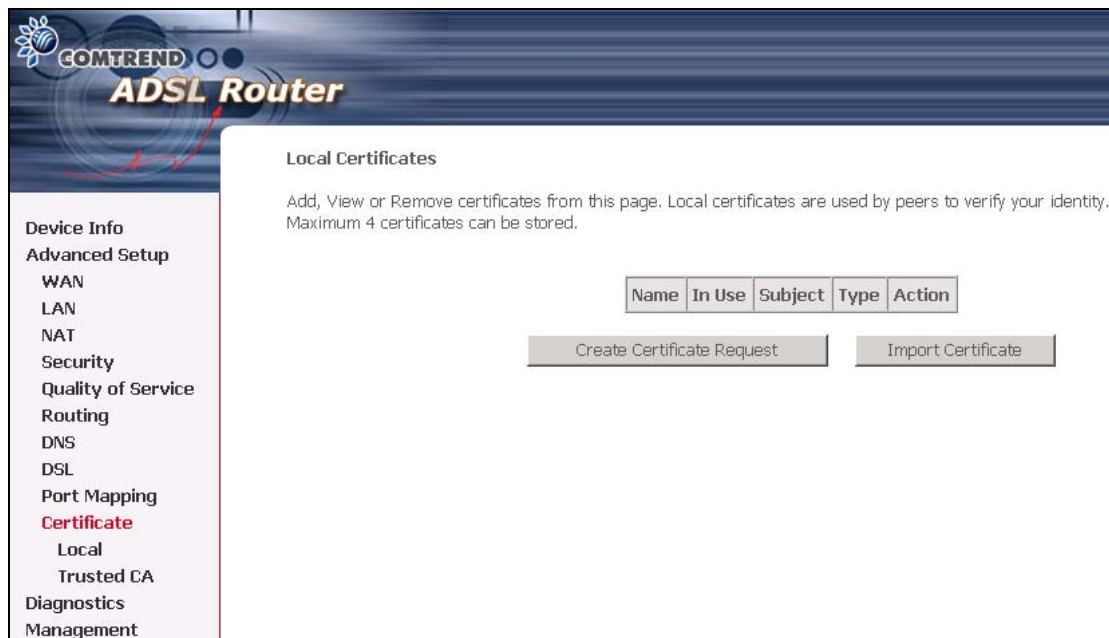
The Lan interface is ENET.

In the LAN side, PC can get IP address from CPE's DHCP server and access Internet via PPPoE (0/33).

6.10 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.

6.10.1 Local



The screenshot shows the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and 'ADSL Router' text. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Quality of Service, Routing (DNS, DSL), Port Mapping, Certificate (Local, Trusted CA), Diagnostics, and Management. The main content area is titled 'Local Certificates' and includes the text: 'Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.' Below this text is a table with columns: Name, In Use, Subject, Type, and Action. At the bottom of the main area are two buttons: 'Create Certificate Request' and 'Import Certificate'.

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.

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.

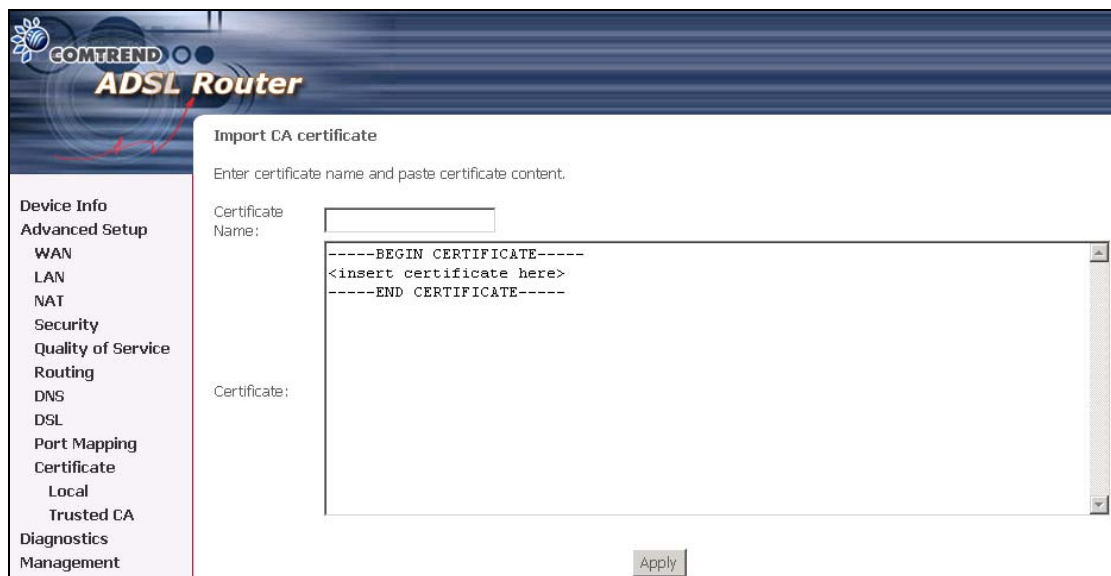
6.10.2 Trusted CA

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.



The screenshot shows the COMTREND ADSL Router web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, DSL, Port Mapping, Certificate, Local, **Trusted CA**, Diagnostics, and Management. The main content area is titled "Trusted CA (Certificate Authority) Certificates" and includes the following text: "Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored." Below this text is a table with four columns: Name, Subject, Type, and Action. An "Import Certificate" button is located below the table.

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.



The screenshot shows the COMTREND ADSL Router web interface with the "Import CA certificate" page. The left sidebar is the same as in the previous screenshot, with "Trusted CA" selected. The main content area is titled "Import CA certificate" and includes the following text: "Enter certificate name and paste certificate content." Below this text is a form with two fields: "Certificate Name:" and "Certificate:". The "Certificate Name:" field is a text input box. The "Certificate:" field is a large text area containing the following text: "-----BEGIN CERTIFICATE-----", "<insert certificate here>", and "-----END CERTIFICATE-----". An "Apply" button is located at the bottom right of the form.

Chapter 7 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-5071T and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Test** 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.

COMTREND
ADSL Router

pppoe_0_35_1 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 Connection:	PASS	Help
Test your USB Connection:	DOWN	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	PASS	Help
Test ATM OAM F5 end-to-end ping:	PASS	Help

Test the connection to your Internet service provider

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

Test Test With OAM F4

Note: The display will vary depending on which PVCs are configured.

Test	Description
Ethernet Connection	<p>Pass: indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful.</p> <p>Fail: Indicates that the DSL Router does not detect the Ethernet interface on your computer.</p>
USB connection (Not available on this device)	<p>Pass: Indicates that the USB interface from your computer is connected to the LAN port of your DSL router.</p> <p>Down: Indicates that the DSL Router does not detect the USB interface on your computer.</p>
ADSL	<p>Pass: Indicates that the DSL modem has detected a DSL</p>

Synchronization	<p>signal from the telephone company. A solid WAN LED on the router also indicates the detection of a DSL signal from the telephone company.</p> <p>Fail: indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The WAN LED will stop blinking and the LED will stop illuminating (i.e. go blank).</p>
ISP Connection	<p>Pass: Indicates we can access the WAN service like the Gateway and DNS.</p> <p>Fail: Indicates we cannot access the WAN side.</p>

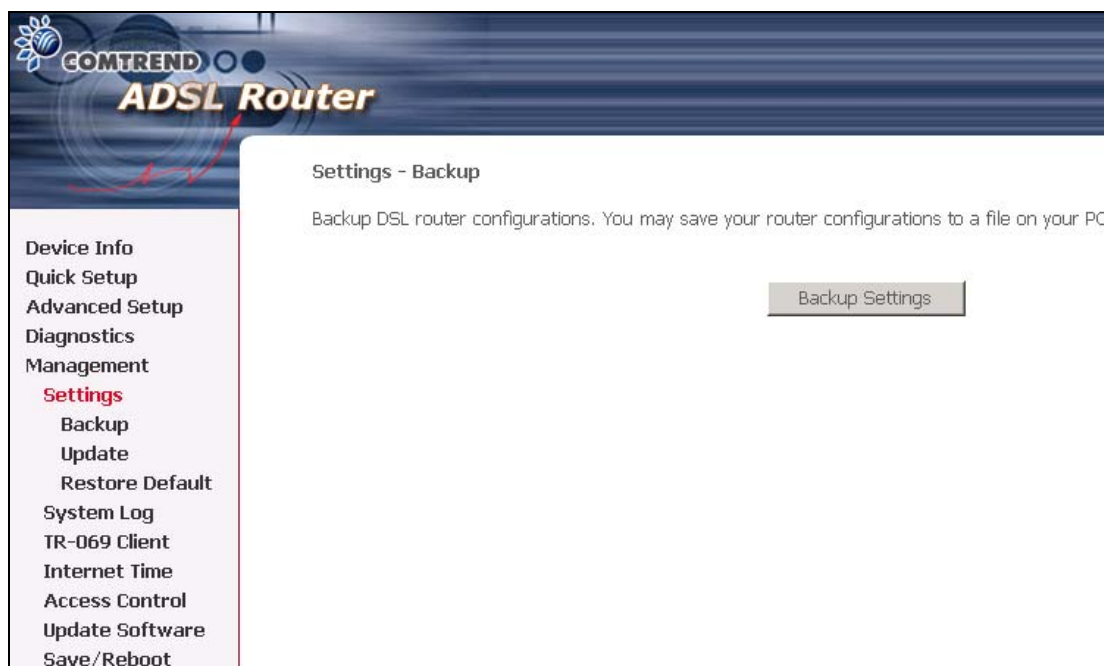
Chapter 8 Management

The Management section of the CT-5071T supports the following maintenance functions and processes:

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

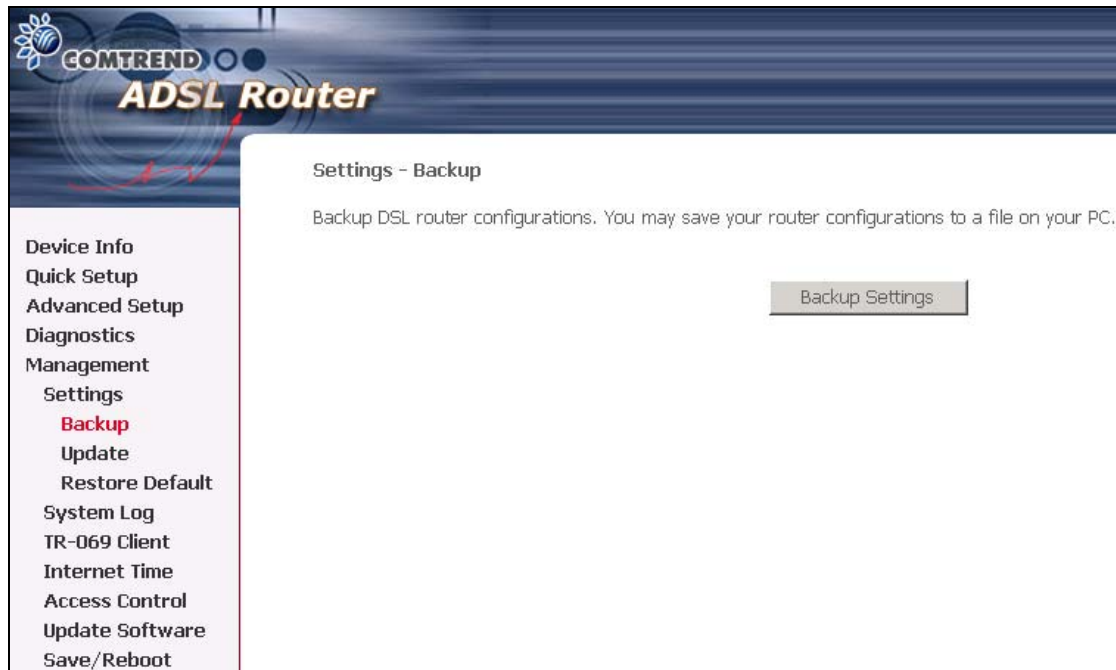
8.1 Settings

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



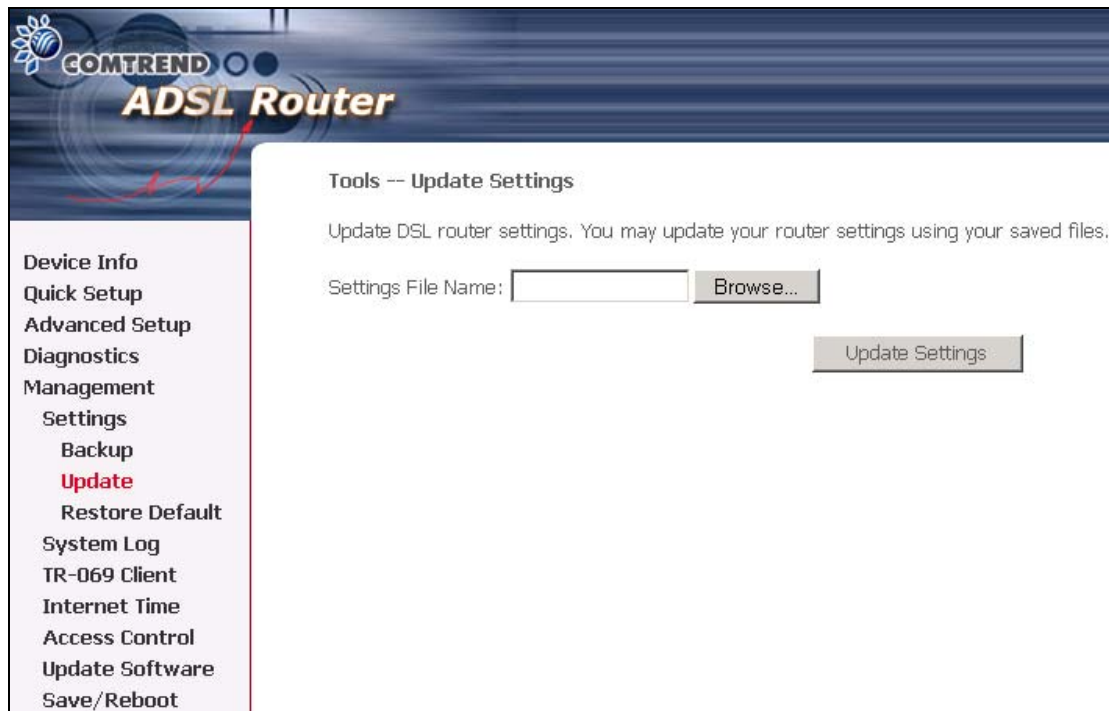
8.1.1 Configuration Backup

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.



8.1.2 Tools – Update Settings

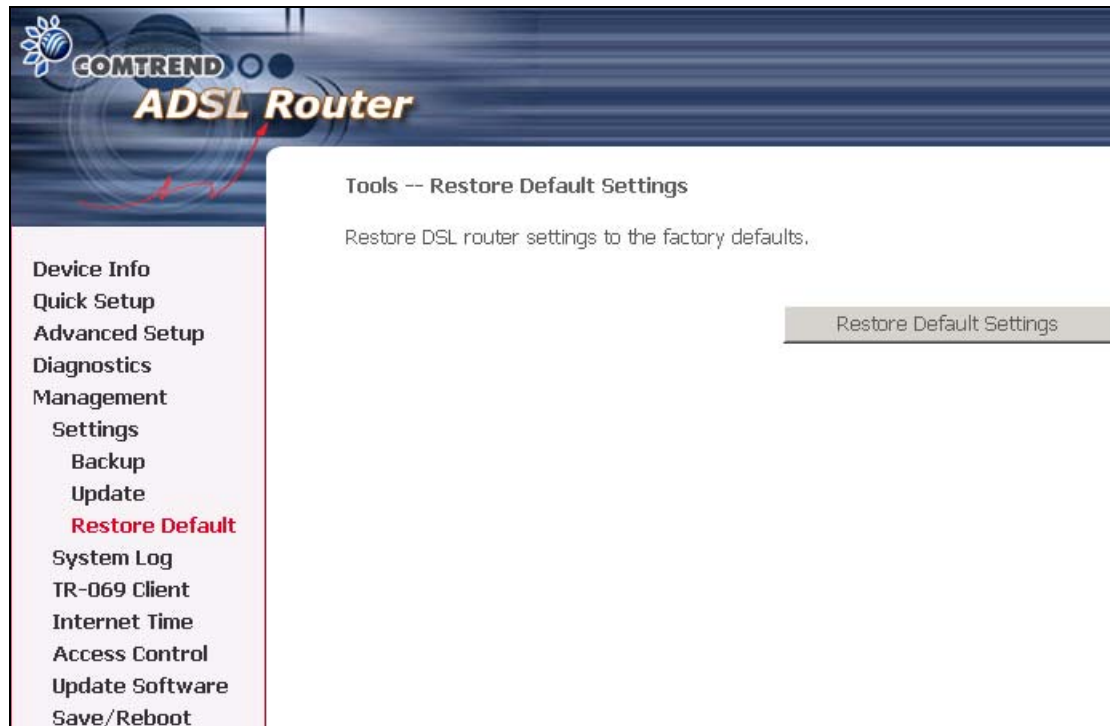
The Update option under Management>Settings update your router settings using your saved files.



The screenshot displays the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and the text "ADSL Router". On the left, a navigation menu lists various options: Device Info, Quick Setup, Advanced Setup, Diagnostics, Management, Settings, Backup, Update (highlighted in red), Restore Default, System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled "Tools -- Update Settings" and contains the following text: "Update DSL router settings. You may update your router settings using your saved files." Below this text is a form with a label "Settings File Name:" followed by an empty text input field and a "Browse..." button. At the bottom right of the form is an "Update Settings" button.

8.1.3 Restore Default

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



NOTE: This entry has the same effect as the hardware reset-to-default button. The CT-5071T 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.

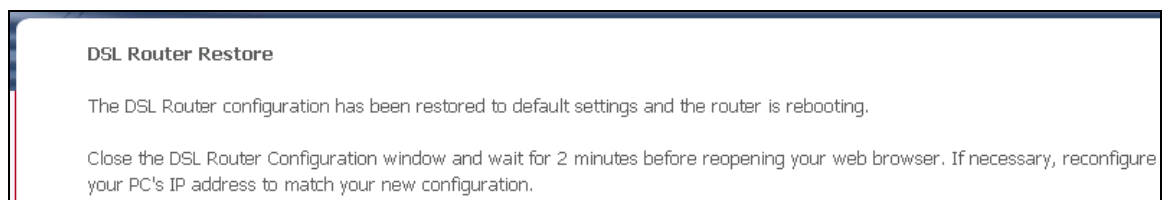
NOTE: Restoring system settings requires a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-5071T.

Default settings

The CT-5071T 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

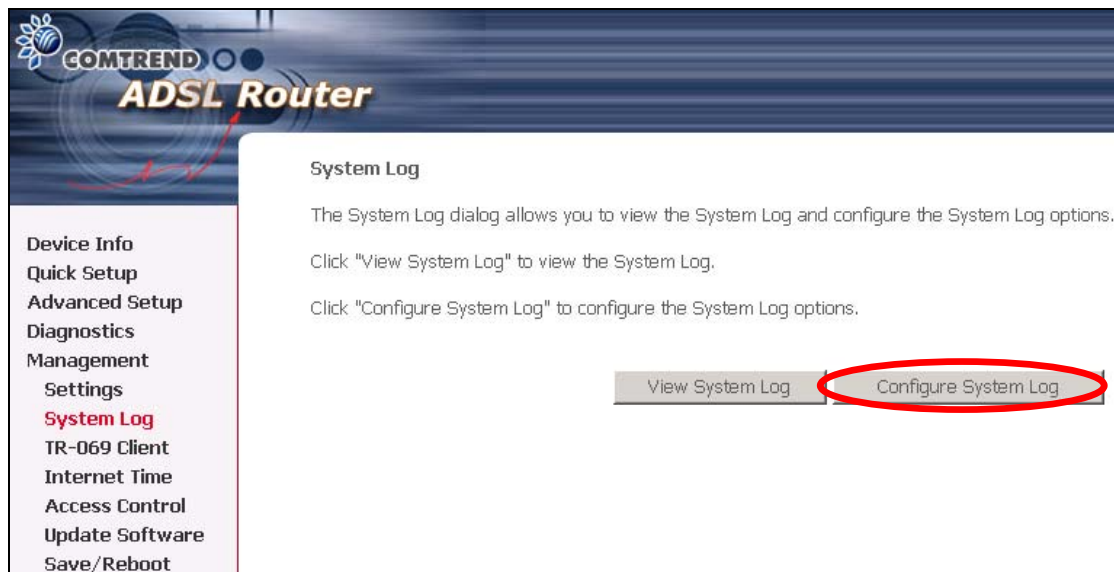
After the Restore Default Configuration button is selected, the following screen appears. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



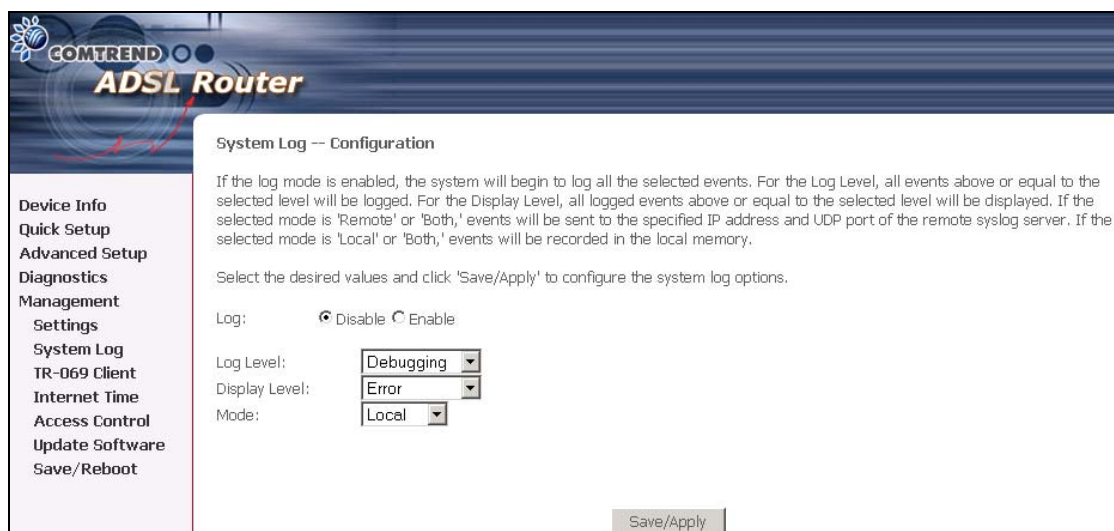
8.2 System Log

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.



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



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	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5071T 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</p> <ul style="list-style-type: none"> • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	Allows the user to select the logged events and displays on the View System Log page for events of this level and above to the highest Emergency level.
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously.</p> <p>If remote mode is selected, view system log will not be able to display events saved in the remote system log server.</p> <p>When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

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

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

8.3 TR-069 Client

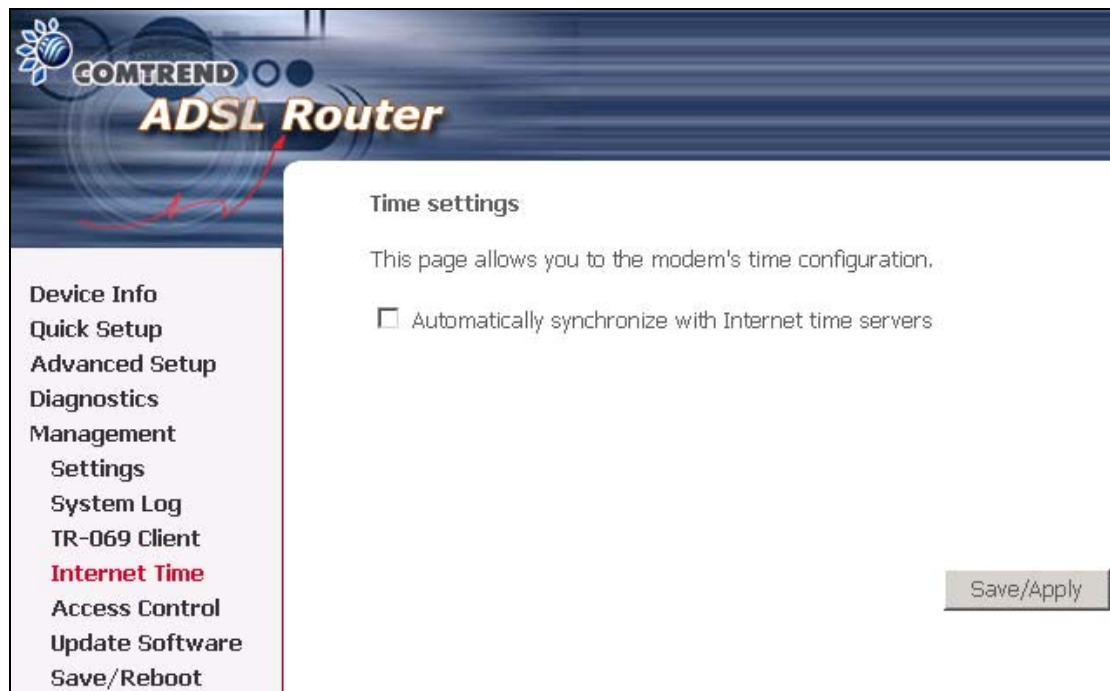
WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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 User Name	Username used to authenticate an ACS making a Connection 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.

8.4 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**.



8.5 Access Control

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



The screenshot displays the web management interface for a Comtrend ADSL Router. The top banner features the Comtrend logo and the text "ADSL Router". A left-hand navigation menu lists various system settings, with "Access Control" highlighted in red. Under "Access Control", the "Services" option is selected. The main content area is titled "Access Control -- Services" and includes a descriptive sentence: "A Service Control List ('SCL') enables or disables services from being used." Below this text is a table with three columns: "Services", "LAN", and "WAN". Each row represents a different service with checkboxes for enabling it on either the LAN or WAN interface. A "Save/Apply" button is located at the bottom right of the configuration area.

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

Save/Apply

8.5.1 Services

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

COMTREND ADSL Router

Access Control -- Services

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

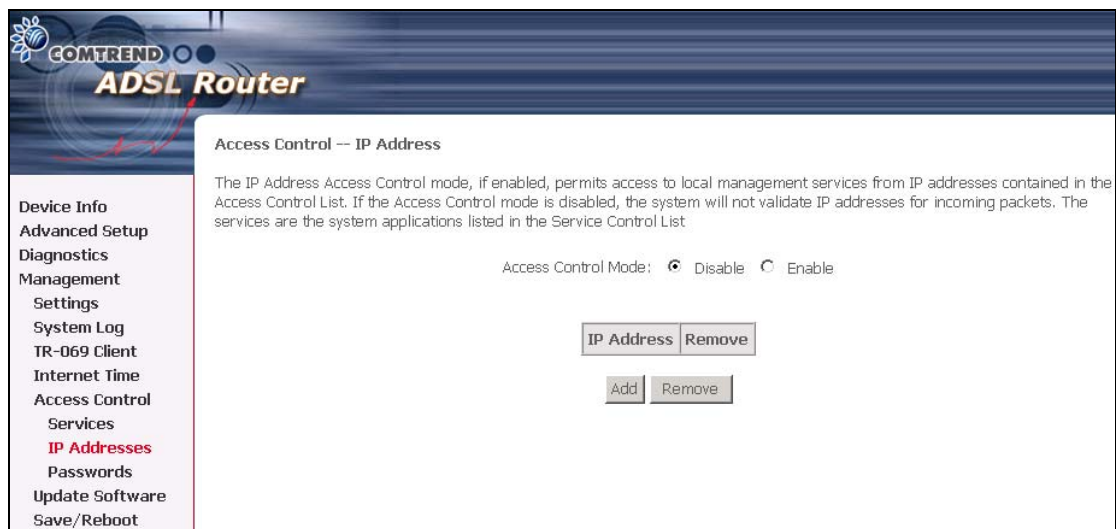
Services	LAN	WAN
FTP	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET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

Save/Apply

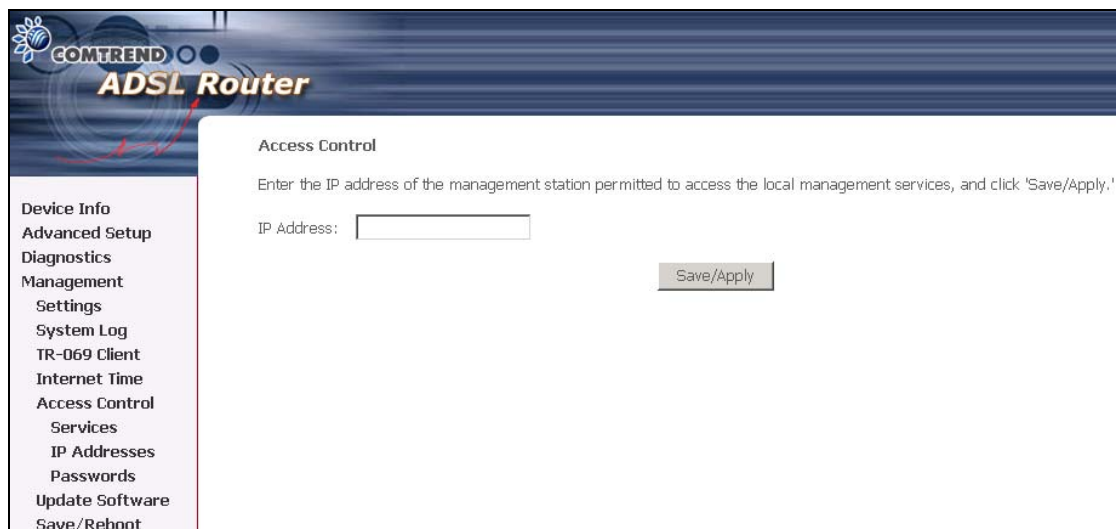
Device Info
Advanced Setup
Diagnostics
Management
Settings
System Log
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot

8.5.2 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 **Save/Apply** to allow the PC with this IP address managing the DSL Router.

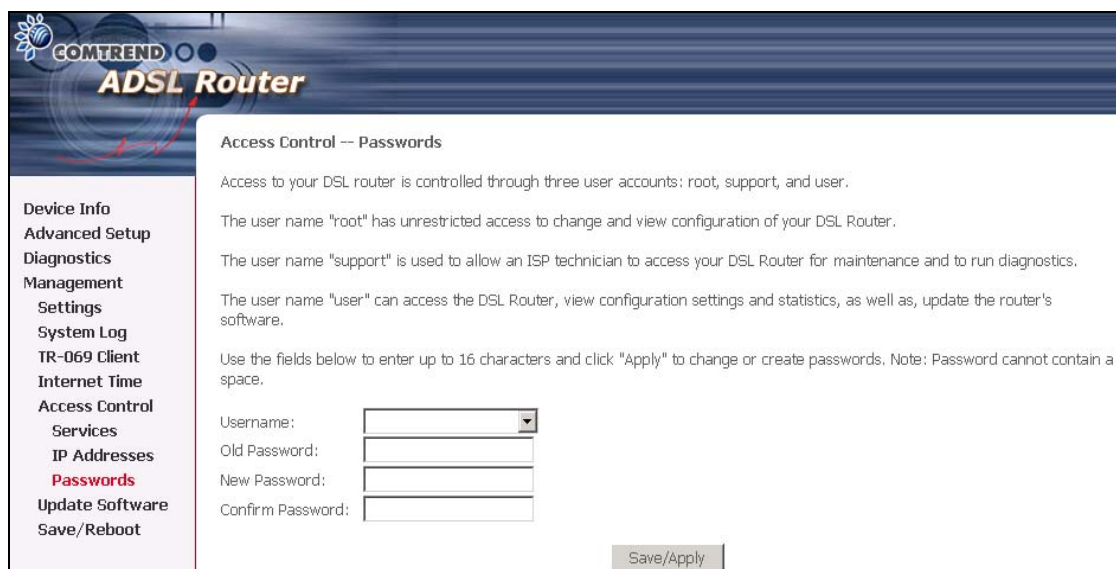


8.5.3 Passwords

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.



The screenshot shows the Comtrend ADSL Router web interface. The page title is "Access Control -- Passwords". The main content area contains the following text:

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:

Save/Apply

The left sidebar contains the following navigation menu:

- Device Info
- Advanced Setup
- Diagnostics
- Management
- Settings
- System Log
- TR-069 Client
- Internet Time
- Access Control
- Services
- IP Addresses
- Passwords
- Update Software
- Save/Reboot

8.6 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.



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.

8.7 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.



Appendix A: Firewall

Stateful Packet Inspection

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

Denial of Service attack

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

TCP/IP/Port/Interface 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 B: 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 C: Specifications

Rear Panel

RJ-11 X1 for ADSL, RJ-45 X1 for LAN, Reset Button X 1, Power Jack X 1, Power switch X 1,

ADSL

ADSL standard	ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2	
G.992.5 (ADSL2+)	Downstream : 24 Mbps	Upstream : 1.3 Mbps
G.992.3 (ADSL2)	Downstream : 12 Mbps	Upstream : 1.3 Mbps
G.DMT	Downstream: 8 Mbps	Upstream: 832 Kbps

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

TR-069, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP, TFTP server, or FTP server

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/DHCP Client, DNS Proxy, ARP

Security Functions

Authentication protocols PAP, CHAP,
TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, Access control

Application Passthrough

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

Power Supply

External power adapter 110/220 Vac to 18 Vac, 0.5A

Environment Condition

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

Dimensions

92mm (W) x 34mm (H) x 114mm (D)

Certifications

FCC Part 15 class B, FCC Part 68, CE

Note: Specifications are subject to change without notice.

Appendix D: 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`