

# CT-5071T

## ADSL2+ Ethernet Router

# User Manual

Version A3.3, December 22, 2008

---



## Preface

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

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

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

## Important Safety Instructions

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

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

### CAUTION:

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



### WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in [Appendix C](#).

## Copyright

Copyright©2008 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

|   |
|---|
| <b>NOTE:</b> This document is subject to change without notice. |
|---|

# Table of Contents

|   |           |
|---|-----------|
| <b>CHAPTER 1 INTRODUCTION.....</b>                            | <b>4</b>  |
| 1.1 FEATURES .....  | 4         |
| 1.2 APPLICATION .....   | 4         |
| <b>CHAPTER 2 INSTALLATION.....</b>                            | <b>5</b>  |
| 2.1 HARDWARE SETUP.....                                       | 5         |
| 2.2 ROUTER STAND SETUP .....                                  | 6         |
| 2.3 LED INDICATORS .....                                      | 7         |
| <b>CHAPTER 3 WEB USER INTERFACE.....</b>                      | <b>8</b>  |
| 3.1 DEFAULT SETTINGS .....                                    | 8         |
| 3.2 IP CONFIGURATION.....                                     | 9         |
| 3.3 LOGIN PROCEDURE.....                                      | 10        |
| <b>CHAPTER 4 QUICK SETUP .....</b>                            | <b>12</b> |
| 4.1 AUTO QUICK SETUP.....                                     | 13        |
| 4.2 MANUAL QUICK SETUP .....                                  | 14        |
| 4.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)..... | 16        |
| 4.2.2 MAC Encapsulation Routing (MER) .....                   | 20        |
| 4.2.3 IP Over ATM.....  | 23        |
| 4.2.4 Bridging.....   | 26        |
| <b>CHAPTER 5 DEVICE INFORMATION.....</b>                      | <b>28</b> |
| 5.1 WAN .....   | 29        |
| 5.2 STATISTICS.....   | 29        |
| 5.2.1 LAN Statistics.....                                     | 30        |
| 5.2.2 WAN Statistics.....                                     | 30        |
| 5.2.3 ATM statistics .....                                    | 31        |
| 5.2.4 ADSL Statistics .....                                   | 33        |
| 5.3 ROUTE .....   | 36        |
| 5.4 ARP.....  | 37        |
| 5.5 DHCP .....  | 37        |
| <b>CHAPTER 6 ADVANCED SETUP.....</b>                          | <b>38</b> |
| 6.1 WAN .....   | 38        |
| 6.2 LAN .....   | 39        |
| 6.3 NAT .....   | 40        |
| 6.3.1 Virtual Servers .....                                   | 40        |
| 6.3.2 Port Triggering.....                                    | 42        |
| 6.3.3 DMZ Host .....  | 43        |
| 6.3.4 ALG .....   | 43        |
| 6.4 SECURITY .....  | 44        |
| 6.4.1 IP Filtering .....                                      | 44        |
| 6.4.2 MAC Filtering.....                                      | 46        |
| 6.4.3 Parental Control.....                                   | 48        |
| 6.5 QUALITY OF SERVICE .....                                  | 49        |
| 6.6 ROUTING .....   | 51        |
| 6.6.1 Default Gateway.....                                    | 51        |
| 6.6.2 Static Route.....                                       | 52        |
| 6.6.3 RIP.....  | 52        |
| 6.7 DNS SERVER .....  | 53        |
| 6.7.1 DNS Server .....  | 53        |
| 6.7.2 Dynamic DNS .....                                       | 53        |
| 6.8 DSL.....  | 55        |
| 6.9 CERTIFICATE.....  | 56        |
| 6.9.1 Local.....  | 56        |
| 6.9.2 Trusted CA.....   | 58        |
| <b>CHAPTER 7 DIAGNOSTICS.....</b>                             | <b>59</b> |

|   |           |
|---|-----------|
| <b>CHAPTER 8 MANAGEMENT .....</b>         | <b>61</b> |
| 8.1 SETTINGS.....                         | 61        |
| 8.1.1 <i>Backup Settings</i> .....        | 61        |
| 8.1.2 <i>Update Settings</i> .....        | 61        |
| 8.1.3 <i>Restore Default</i> .....        | 62        |
| 8.2 SYSTEM LOG .....                      | 63        |
| 8.3 SNMP AGENT .....                      | 65        |
| 8.4 TR-069 CLIENT .....                   | 65        |
| 8.5 INTERNET TIME .....                   | 66        |
| 8.6 ACCESS CONTROL .....                  | 67        |
| 8.6.1 <i>Services</i> .....               | 67        |
| 8.6.2 <i>IP Addresses</i> .....           | 67        |
| 8.6.3 <i>Passwords</i> .....              | 68        |
| 8.7 UPDATE SOFTWARE .....                 | 69        |
| 8.8 SAVE AND REBOOT .....                 | 70        |
| <b>APPENDIX A – FIREWALL.....</b>         | <b>71</b> |
| <b>APPENDIX B – PIN ASSIGNMENTS .....</b> | <b>75</b> |
| <b>APPENDIX C – SPECIFICATIONS .....</b>  | <b>76</b> |
| <b>APPENDIX D – SSH CLIENT.....</b>       | <b>78</b> |

# Chapter 1 Introduction

The CT-5071T ADSL2+ Ethernet Router is a high-performance device that features TR-069 compliance for remote network management. It has one 10/100 Base-T Ethernet port and one ADSL2+ port for broadband Internet access.

The CT-5071T also has a TR-068 compliant rear panel and LED indicators for easy installation and use. It supports LAN or Video on Demand at speeds of up to 24 Mbps over a regular telephone line.

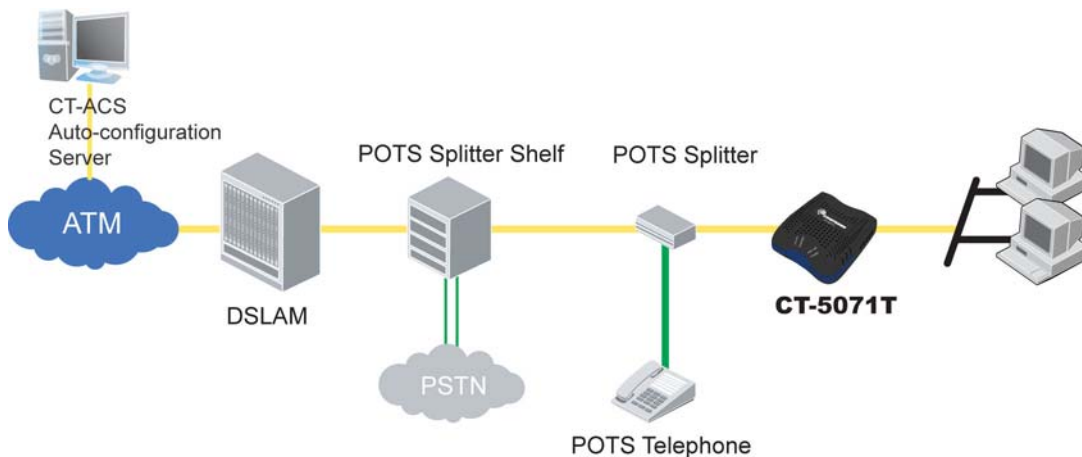
The CT-5071T has full routing capabilities to segment and route IP packets. It provides protection for the local area network with advanced security technologies, such as VPNs (Virtual Private Networks) with PPTP pass-through, L2TP pass-through, IPSec pass-through and Firewall.

## 1.1 Features

- CT-5071T (Annex A)
- SPI (Stateful Packet Inspection)
- Static route and RIP v1/v2
- NAT/PAT
- DHCP server/relay/client
- Auto PVC configuration
- FTP/TFTP server
- IP/MAC address filtering
- Web-based management
- TR-069/TR-098/TR-111 compliant
- Configuration backup and restoration
- IP filtering
- DoS protection
- Dynamic IP assignment
- IGMP proxy
- DNS proxy
- Up to 8 VCs
- Embedded SNMP agent
- TR-068 compliant
- Supports remote administration
- Automatic firmware upgrade and configuration

## 1.2 Application

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

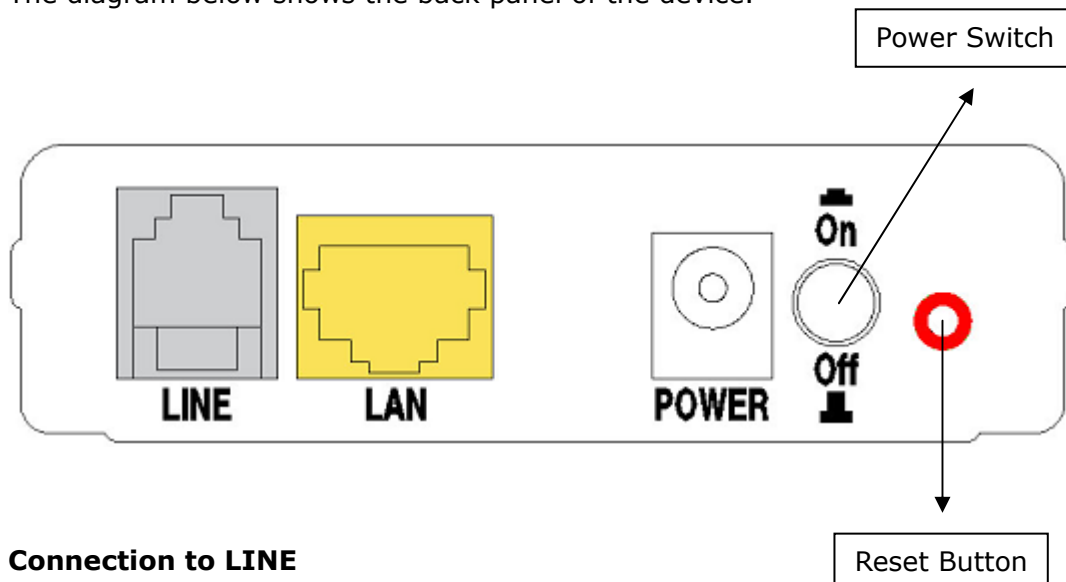


# Chapter 2 Installation

## 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

The diagram below shows the back panel of the device.



### Connection to LINE

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

### Connection to LAN

Use RJ45 cable to connect up to four network devices. These ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

### Power ON

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section [2.3 LED Indicators](#)).

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

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

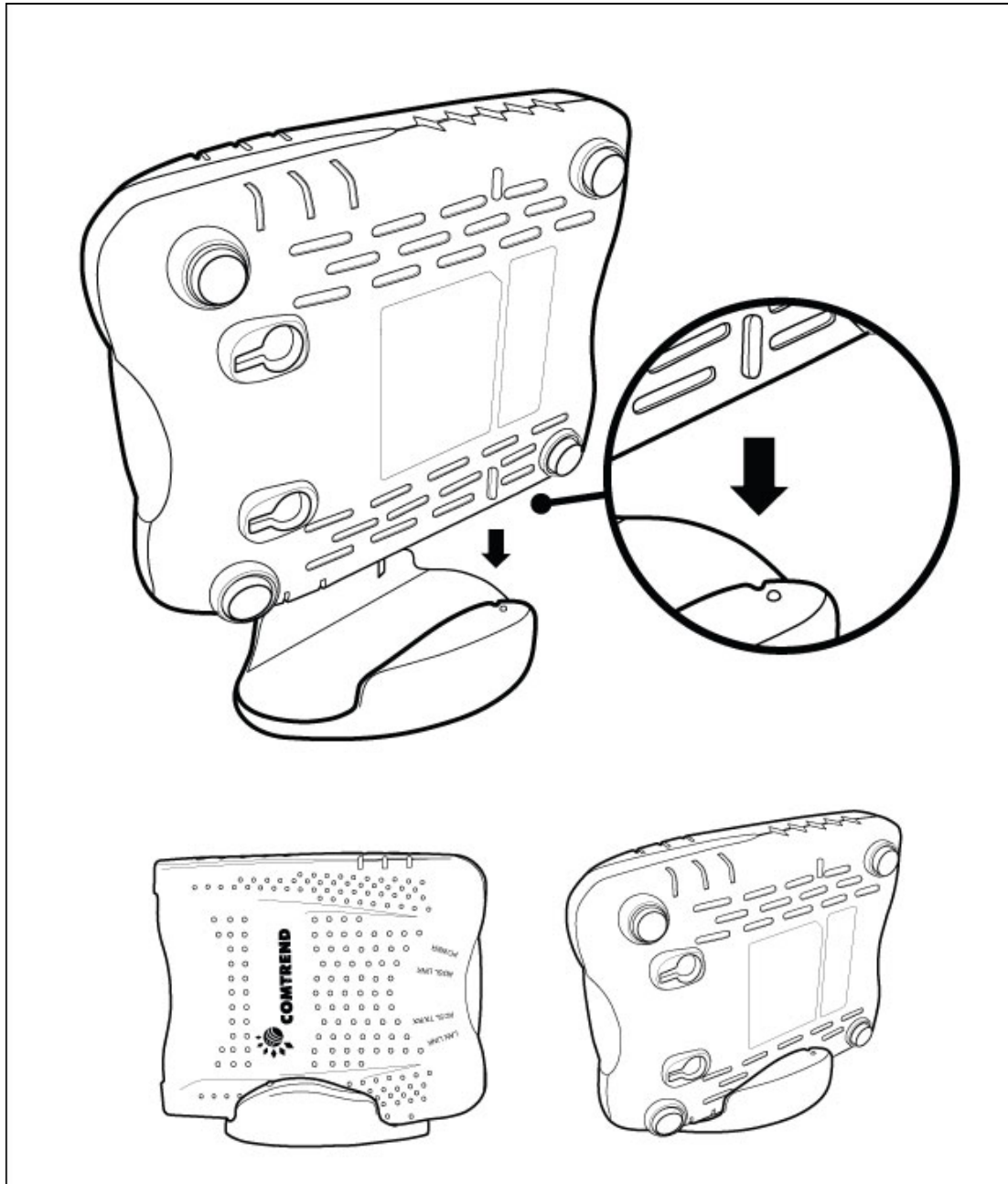
### Reset Button

Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section [2.3 LED Indicators](#) for details).

**NOTE:** If pressed down for more than 20 seconds, the CT-5071T will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

## 2.2 Router Stand Setup

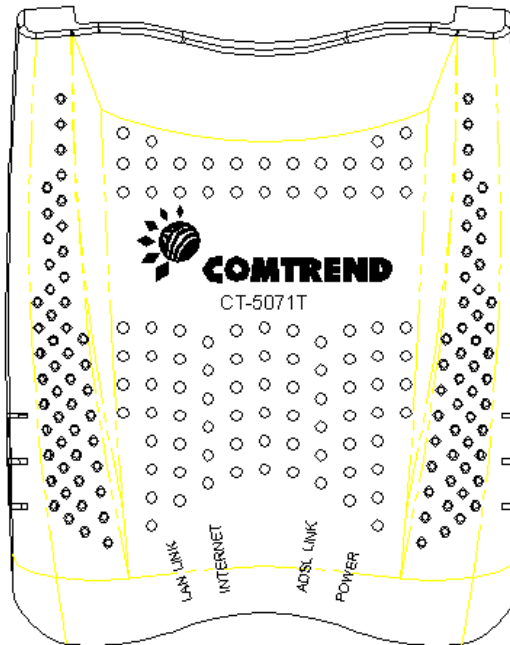
The router stand can be used to save workspace. As shown in the figure below, simply slide the router into the notches on the stand and position vertically.



**NOTE:** Be careful to place the router (and stand) on a flat stable surface. Avoid locations where it is likely to be knocked over or fall down.

## 2.3 LED Indicators

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



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



# Chapter 3 Web User Interface

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

## 3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
  - LAN subnet mask: 255.255.255.0
  - Administrative access (username: **root** , password: **12345**)
  - User access (username: **user**, password: **user**)
  - WAN IP address: none
  - Remote WAN access: TR-069 and ICMP **enabled**
  - Remote (WAN) access (username: **support**, password: **support**)
- 

This device supports the following connection types.

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

- DHCP server: **enabled** in routing modes (PPPoA/E, MER & IPoA)  
**not available** for Bridge mode
- Firewall and NAT: **disabled** in routing modes (PPPoA/E, MER & IPoA)  
**not available** in Bridge mode

### Technical Note:

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

## 3.2 IP Configuration

### STATIC IP MODE

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

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

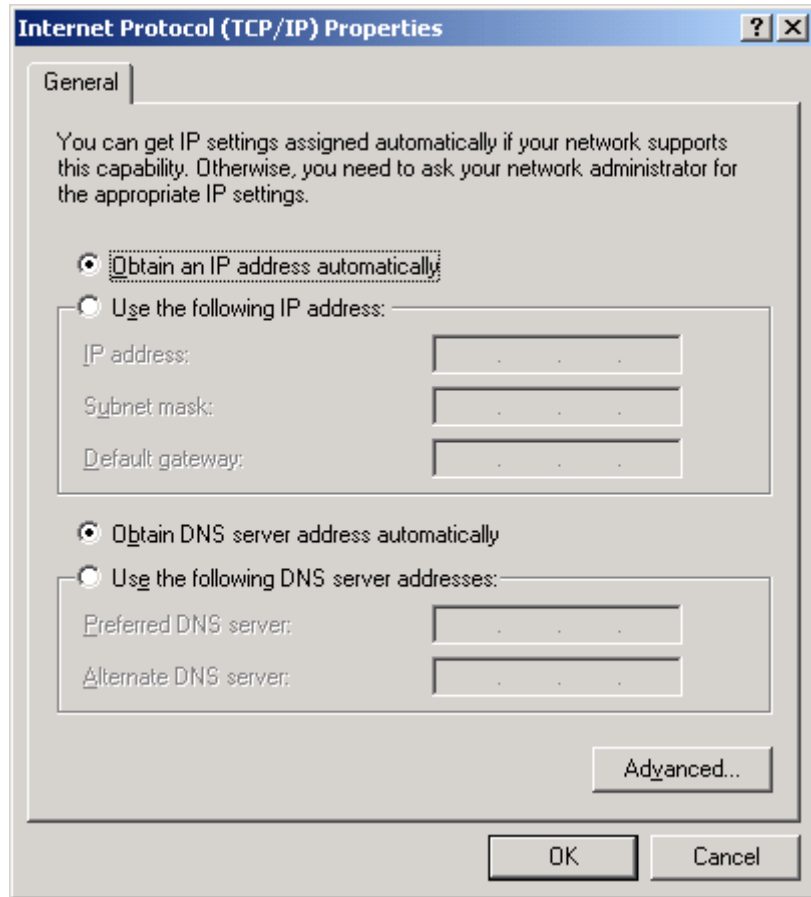
**STEP 2:** Select **Internet Protocol (TCP/IP)** and click the **Properties** button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x ( $1 < x < 255$ ) with subnet mask of 255.255.255.0.

The screenshot shows the 'Internet Protocol (TCP/IP) Properties' dialog box. The 'General' tab is active. It contains instructions about automatic IP assignment. Two radio buttons are present: 'Obtain an IP address automatically' (unselected) and 'Use the following IP address:' (selected). Below the selected option are three text boxes: 'IP address:' containing '192 . 168 . 1 . 133', 'Subnet mask:' containing '255 . 255 . 255 . 0', and 'Default gateway:' which is empty. A second set of radio buttons is below: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server addresses:' (selected). Below this are two text boxes: 'Preferred DNS server:' and 'Alternate DNS server:', both empty. An 'Advanced...' button is located at the bottom right of the main content area. At the very bottom are 'OK' and 'Cancel' buttons.

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

## DHCP MODE

Set your PC to DHCP mode by selecting **Obtain an IP address automatically** in the Internet Protocol Properties dialog box, as shown below.



## 3.3 Login Procedure


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

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

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

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

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

A Windows-style dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, it shows "Site: 192.168.1.1" and "Realm: DSL Router". There are two input fields: "User Name" with the text "root" and "Password" with masked characters "xxxxxx". At the bottom, there is a checkbox labeled "Save this password in your password list" which is currently unchecked. Two buttons, "OK" and "Cancel", are at the bottom right.

Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm: DSL Router

User Name: root

Password: xxxxxx

☐ Save this password in your password list

OK Cancel

Click **OK** to continue.

**NOTE:** The login password can be changed later (section [8.6.3 Passwords](#))

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

A screenshot of the COMTREND ADSL Router web interface. The top banner features the COMTREND logo and "ADSL Router" in large, stylized text. On the left is a vertical menu with options: "Device Info", "Quick Setup" (highlighted), "Advanced Setup", "Diagnostics", and "Management". The main content area is titled "Quick Setup" and contains the text: "This Quick Setup will guide you through the steps necessary to configure your DSL Router." Below this is a section titled "ATM PVC Configuration" with the instruction: "Select the check box below to enable DSL Auto-connect process." There is a checked checkbox followed by the text "DSL Auto-connect".

COMTREND ADSL Router

Device Info  
Quick Setup  
Advanced Setup  
Diagnostics  
Management

**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

**NOTE1:** If a PVC connection already exists then this Quick Setup screen will be bypassed and the [Device Info – Summary](#) screen will display instead.

**NOTE2:** The selections available on the main menu (onscreen at left) are based upon the configured connection and user account privileges.

## Chapter 4 Quick Setup

The function allows the user to configure the ADSL router for DSL connectivity and Internet access. It guides the user through the WAN network setup first and then the LAN interface setup. The user can either manually customize the router or follow the auto quick setup procedure.

The following configuration considerations apply:

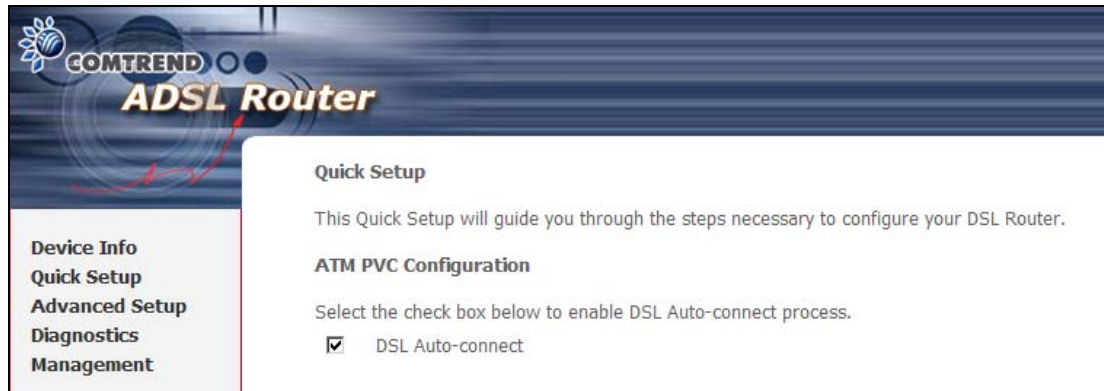
- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running 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 are not running a PPPoE client, then select PPPoE. If all LAN-side devices are running PPPoE clients, then select Bridge In PPPoE mode, CT-5071T also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from 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 NAT and firewall status, the main menu will display or hide the NAT/Firewall menu. For instance, if the default network-operating mode is Bridge, the main menu will not show the NAT and Firewall menu.

|  |
|--|
| <p><b>NOTE:</b> Up to 8 PVC profiles can be configured and saved in the flash memory. To activate a particular PVC profile, you must navigate through all the setup screens until the last summary screen, and click <b>Save/Reboot</b>.</p> |
|--|

## 4.1 Auto Quick Setup

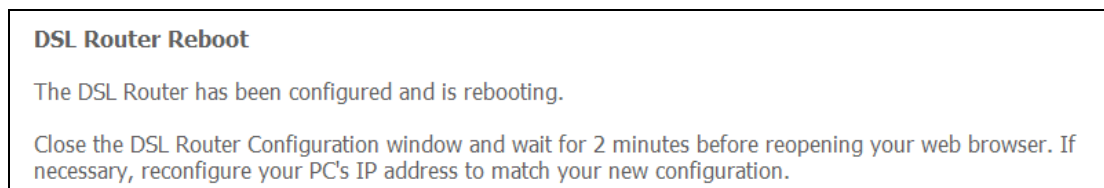
The auto quick setup procedures require the ADSL link to be up to automatically detect PVCs. You simply need to follow the online instructions as prompted.

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



**Step 2:** Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some advanced setup procedures (such as PVC index and encapsulation selection).

**Step 3:** After the setup is complete the CT-5071T will reboot.



**NOTE:** After the device reboots, the [Device Info – Summary](#) screen should appear. If the browser does not refresh automatically, close it and restart. You will need to login again.

## 4.2 Manual Quick Setup

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

### Quick Setup

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

### ATM PVC Configuration

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

☒ DSL Auto-connect

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

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

VPI: [0-255]

VCI: [32-65535]

### Enable Quality Of Service

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

Enable Quality Of Service ☐

Next

**STEP 2:** Adjust the VPI/VCI settings for the connection you wish to establish. You may also **Enable Quality of Service** (QoS) with its checkbox ☒.

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

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

You may also choose to **Enable 802.1q** (available in PPPoE, MER and Bridging modes) and enter the VLAN ID, as shown below.

**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]:

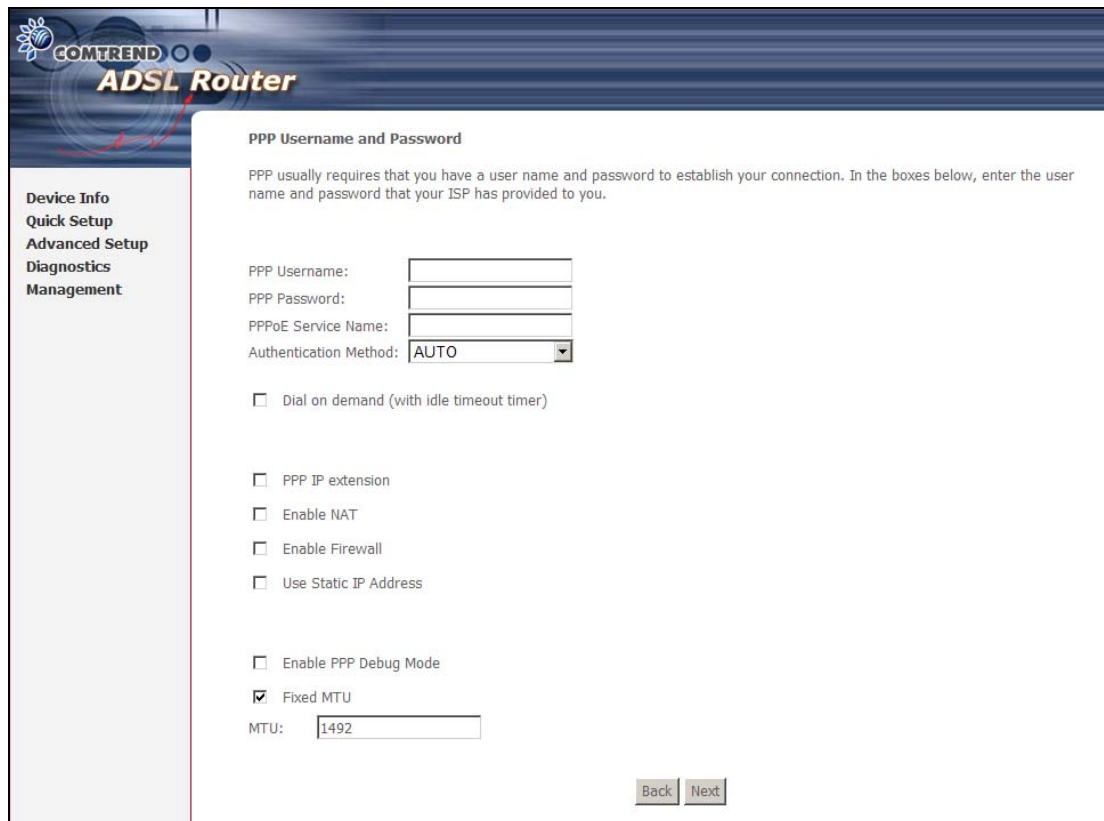
Click **Next** to continue...

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



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

**STEP 4:** Enter the PPP settings as provided by your ISP.



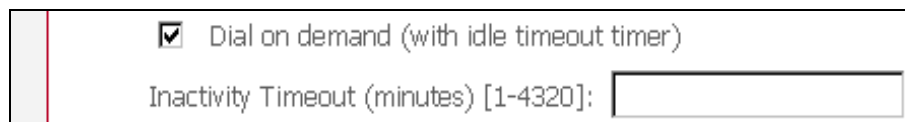
The screenshot shows the 'COMTREND ADSL Router' configuration interface. On the left is a sidebar with links: 'Device Info', 'Quick Setup', 'Advanced Setup', 'Diagnostics', and 'Management'. The main area is titled 'PPP Username and Password'. It contains a text box for 'PPP Username', a text box for 'PPP Password', a text box for 'PPPoE Service Name', and a dropdown menu for 'Authentication Method' set to 'AUTO'. Below these are several checkboxes: 'Dial on demand (with idle timeout timer)', 'PPP IP extension', 'Enable NAT', 'Enable Firewall', 'Use Static IP Address', 'Enable PPP Debug Mode', and 'Fixed MTU' (which is checked). The 'Fixed MTU' checkbox is followed by a text box containing '1492'. At the bottom right are 'Back' and 'Next' buttons.

### PPP Settings

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

### Dial on Demand

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 must enter an inactivity timeout period of 1 to 4320 minutes.



This is a close-up of the 'Dial on demand (with idle timeout timer)' checkbox, which is checked. Below it is the 'Inactivity Timeout (minutes) [1-4320]:' label followed by an empty text input box.

### PPP IP Extension

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

PPP IP Extension does the following:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the

- device has only a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.

#### **Enable NAT**

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

#### **Enable Firewall**

If this checkbox ☒ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☒ should be de-selected to free up system resources for better performance.

#### **Use Static IP Address**

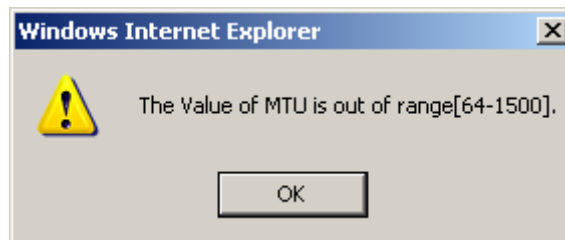
Unless your service provider specially requires this setup, do not select it. If selected, enter your static IP address in the IP Address field.

#### **Enable PPP Debug Mode**


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

#### **Fixed MTU**

This option allows for changes to the MTU size of PPPoE and PPPoA WAN interfaces. The default values for MTU size are 1492 for PPPoE and 1500 for PPPoA. The allowable range of values for MTU size is from 64 to 1500. If a value is entered outside this range the following dialog box will be displayed.



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



Device Info  
Quick Setup  
Advanced Setup  
Diagnostics  
Management

### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☒

Service Name

Back Next

### 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.

**Service Name:** This is the WAN Service label.

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



Device Info  
Quick Setup  
Advanced Setup  
Diagnostics  
Management

### Device Setup

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

IP Address:

Subnet Mask:

☐ Disable DHCP Server  
☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay  
 DHCP Server IP Address:

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

Back Next

This screen allows for the configuration of the CT-5071T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to other LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

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

**NOTE:** **Enable DHCP Server Relay** will not display if NAT is enabled.


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

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

IP Address:

Subnet Mask:

**STEP 7:** Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



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:                | 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 screen automatically. The CT-5071T is ready for operation when the front panel LED indicators display as described in section [2.3 LED Indicators](#).

## 4.2.2 MAC Encapsulation Routing (MER)

**STEP 4:** Enter the WAN IP settings as provided by your ISP.

The screenshot shows the 'WAN IP Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with 'Device Info', 'Quick Setup', 'Advanced Setup', 'Diagnostics', and 'Management'. The main content area has a title 'WAN IP Settings' and a paragraph of instructions. Below the instructions are several configuration options with radio buttons and checkboxes. The 'Obtain an IP address automatically' option is selected. The 'Obtain default gateway automatically' option is also selected. The 'Obtain DNS server addresses automatically' option is selected. At the bottom right, there are 'Back' and 'Next' buttons.

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.  
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.  
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

☐ Obtain an IP address automatically  
☒ Use the following IP address:  
WAN IP Address:   
WAN Subnet Mask:

☒ Obtain default gateway automatically  
☐ Use the following default gateway:  
☐ Use IP Address:   
☐ Use WAN Interface: mer\_0\_35/nas\_0\_35

☒ Obtain DNS server addresses automatically  
☐ Use the following DNS server addresses:  
Primary DNS server:   
Secondary DNS server:

Back Next

DHCP can be enabled if the **Obtain an IP address automatically** checkbox ☒ is checked. Configuring the default gateway or the DNS with static values will disable the automatic assignment from DHCP or other WAN connection.

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

The screenshot shows the 'Network Address Translation Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with 'Device Info', 'Quick Setup', 'Advanced Setup', 'Diagnostics', and 'Management'. The main content area has a title 'Network Address Translation Settings' and a paragraph of instructions. Below the instructions are several configuration options with checkboxes. The 'Enable NAT' checkbox is unchecked. The 'Enable Firewall' checkbox is unchecked. The 'Enable IGMP Multicast, and WAN Service' section has 'Enable IGMP Multicast' unchecked and 'Enable WAN Service' checked. The 'Service Name' field contains 'mer\_0\_35'. At the bottom right, there are 'Back' and 'Next' buttons.

**Network Address Translation Settings**

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

Enable NAT ☐  
Enable Firewall ☐

**Enable IGMP Multicast, and WAN Service**

Enable IGMP Multicast ☐  
Enable WAN Service ☒  
Service Name: mer\_0\_35

Back Next

### Enable NAT

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

### Enable Firewall

If this checkbox ☒ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☒ should be de-selected to free up system resources for better performance.

### 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.

**Service Name** is user-defined.

**STEP 6:** 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

This screen allows for the configuration of the CT-5071T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

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

**NOTE:** The **Enable DHCP Server Relay** option will not display if NAT is enabled.




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

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

IP Address:

Subnet Mask:

**STEP 7:** Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



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:         | Automatically Assigned |
| Service State:      | Enabled                |
| NAT:                | Disabled               |
| Firewall:           | Disabled               |
| IGMP Multicast:     | Disabled               |
| Quality Of Service: | Disabled               |

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

BackSave/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 screen automatically. The CT-5071T is ready for operation when the front panel LED indicators display as described in section [2.3 LED Indicators](#).

### 4.2.3 IP Over ATM

**STEP 4:** Enter the WAN IP settings as provided by your ISP.

The screenshot shows the 'WAN IP Settings' page of a COMTREND ADSL Router. The page has a dark blue header with the 'COMTREND ADSL Router' logo. On the left, there is a sidebar menu with options: 'Device Info', 'Quick Setup', 'Advanced Setup', 'Diagnostics', and 'Management'. The main content area is titled 'WAN IP Settings' and contains the following text: 'Enter information provided to you by your ISP to configure the WAN IP settings.' and a notice: '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.' Below this, there are input fields for 'WAN IP Address:' and 'WAN Subnet Mask:'. There are two main sections with checkboxes. The first section is 'Use the following default gateway:' with sub-options 'Use IP Address:' (checkbox) and 'Use WAN Interface:' (checkbox) which is selected and shows a dropdown menu with 'ipoa\_0\_35/ipa\_0\_35'. The second section is 'Use the following DNS server addresses:' with sub-options 'Primary DNS server:' and 'Secondary DNS server:'. At the bottom right, there are 'Back' and 'Next' buttons.

Since DHCP is not supported over IPoA, the default gateway settings and DNS server addresses must be entered here. These should be provided by your ISP.

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

The screenshot shows the 'Network Address Translation Settings' page of a COMTREND ADSL Router. The page has a dark blue header with the 'COMTREND ADSL Router' logo. On the left, there is a sidebar menu with options: 'Device Info', 'Quick Setup', 'Advanced Setup', 'Diagnostics', and 'Management'. The main content area is titled 'Network Address Translation Settings' and contains the following text: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).' Below this, there are two checkboxes: 'Enable NAT' (checkbox) and 'Enable Firewall' (checkbox). There is a section titled 'Enable IGMP Multicast, and WAN Service' with sub-options 'Enable IGMP Multicast' (checkbox) and 'Enable WAN Service' (checkbox) which is checked. Below this, there is a 'Service Name:' field with the value 'ipoa\_0\_35'. At the bottom right, there are 'Back' and 'Next' buttons.

#### Enable NAT

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

#### Enable Firewall

If this checkbox ☒ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☒ should be de-selected to free up system resources for better performance.

#### 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.

**Service Name** is user-defined.

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

**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

This screen allows for the configuration of the CT-5071T LAN interface IP address, subnet mask and DHCP server. To auto-assign IP addresses, DNS server and default gateway to LAN devices, select the **Enable DHCP server** radio box. You must also enter the start and end IP address and DHCP leased time.

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

**NOTE:** The **Enable DHCP Server Relay** option will not display if NAT is enabled.

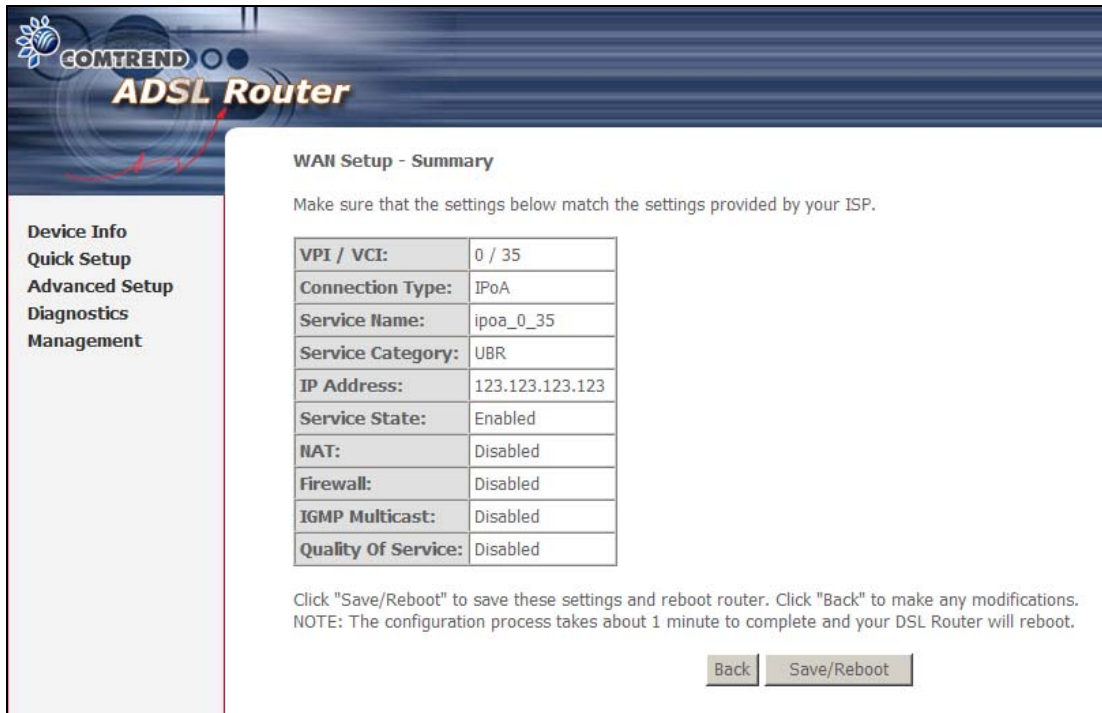
To configure a secondary IP address for the LAN port, click the checkbox ☒ shown.

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

IP Address:

Subnet Mask:

**STEP 7:** Click **Next** to display the 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.

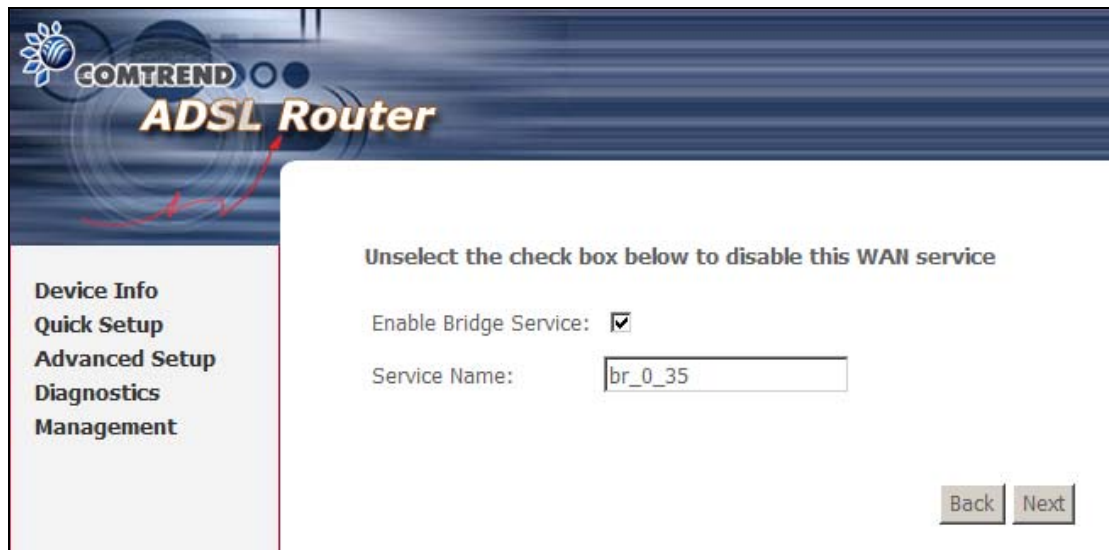
|                     |                 |
|---------------------|-----------------|
| VPI / VCI:          | 0 / 35          |
| Connection Type:    | IPoA            |
| Service Name:       | ipoa_0_35       |
| Service Category:   | UBR             |
| IP Address:         | 123.123.123.123 |
| Service 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 screen automatically. The CT-5071T is ready for operation when the front panel LED indicators display as described in section [2.3 LED Indicators](#).

## 4.2.4 Bridging

**STEP 4:** To enable bridge service, tick the checkbox ☒ and enter a service name.



The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a sidebar with navigation links: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area has a header that says "Unselect the check box below to disable this WAN service". Below this, there is a checkbox labeled "Enable Bridge Service:" which is checked. Next to it is a text field labeled "Service Name:" containing the text "br\_0\_35". At the bottom right of the main area are two buttons: "Back" and "Next".


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



The screenshot shows the "Device Setup" screen in the COMTREND ADSL Router configuration interface. The sidebar on the left is the same as in the previous screenshot. The main content area has a title "Device Setup" and a subtitle "Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN)". Below this, there are two text fields: "IP Address:" with the value "192.168.1.1" and "Subnet Mask:" with the value "255.255.255.0". At the bottom right are "Back" and "Next" buttons.

Enter the IP address and subnet mask for the LAN interface. These settings are used to manage the CT-5071T. In bridge mode, there is no WAN IP address and therefore no remote access to the router for technical support or other purposes.

**STEP 6:** Click **Next** to display the configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.



**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:    | Bridge         |
| Service Name:       | br_0_35        |
| Service Category:   | UBR            |
| IP Address:         | Not Applicable |
| Service State:      | Enabled        |
| NAT:                | Disabled       |
| Firewall:           | Disabled       |
| IGMP Multicast:     | Not Applicable |
| Quality Of Service: | Disabled       |

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

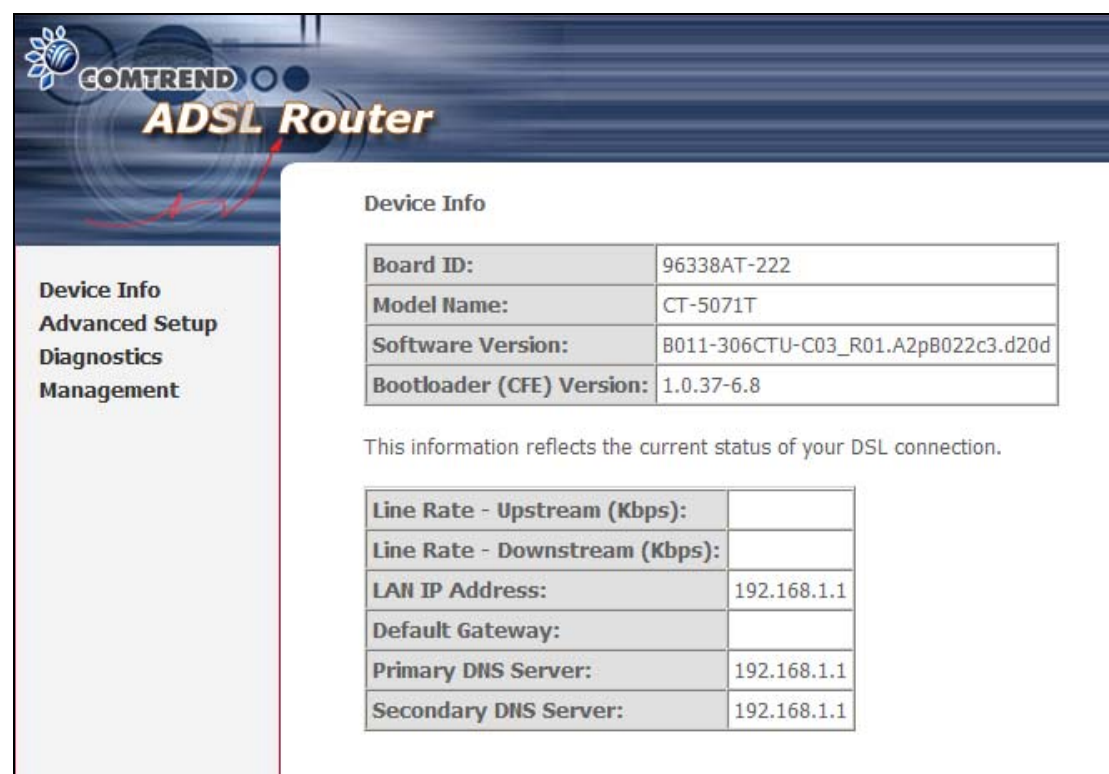
After clicking **Save/Reboot**, the router will save the configuration to the flash memory and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info screen automatically. The CT-5071T is ready for operation when the front panel LED indicators display as described in section [2.3 LED Indicators](#).

# Chapter 5 Device Information

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

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

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



The screenshot shows the web interface of a COMTREND ADSL Router. The header features the COMTREND logo and the text "ADSL Router". On the left is a sidebar menu with the following options: "Device Info", "Advanced Setup", "Diagnostics", and "Management". The "Device Info" option is selected. The main content area is titled "Device Info" and contains two tables. The first table lists hardware and software details, and the second table lists DSL connection status information.

| Device Info               |                                    |
|---------------------------|------------------------------------|
| Board ID:                 | 96338AT-222                        |
| Model Name:               | CT-5071T                           |
| Software Version:         | B011-306CTU-C03_R01.A2pB022c3.d20d |
| Bootloader (CFE) Version: | 1.0.37-6.8                         |

This information reflects the current status of your DSL connection.

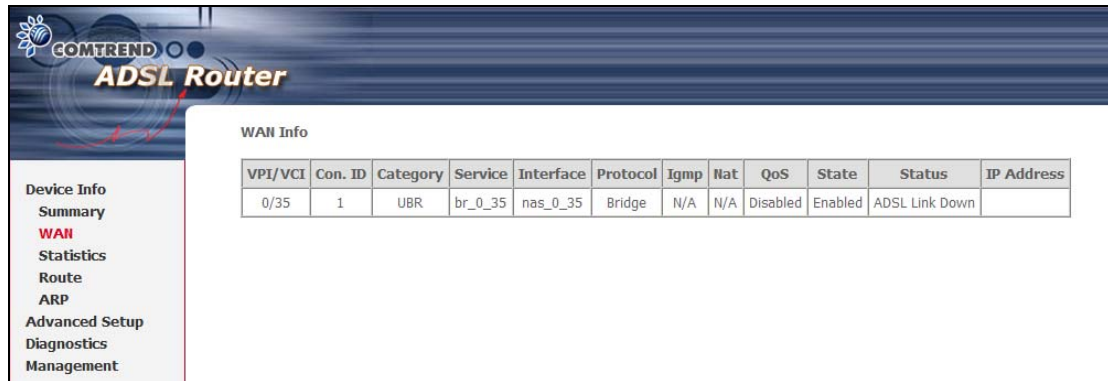
|                                |             |
|--------------------------------|-------------|
| Line Rate - Upstream (Kbps):   |             |
| Line Rate - Downstream (Kbps): |             |
| LAN IP Address:                | 192.168.1.1 |
| Default Gateway:               |             |
| Primary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

The Device Info Summary screen (shown above) is the default startup screen.

It provides summary information regarding hardware, software, data transmission (i.e. Line Rate), and the IP configuration of the device.

## 5.1 WAN

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



| VPI/VCI | Con. ID | Category | Service | Interface | Protocol | Igmp | Nat | QoS      | State   | Status         | IP Address |
|---------|---------|----------|---------|-----------|----------|------|-----|----------|---------|----------------|------------|
| 0/35    | 1       | UBR      | br_0_35 | nas_0_35  | Bridge   | N/A  | N/A | Disabled | Enabled | ADSL Link Down |            |

| Heading    | Description  |
|------------|--|
| VPI/VCI    | ATM VPI (0-255) / VCI (32-65535)                       |
| Con. ID    | WAN connection ID number                               |
| Category   | ATM service category                                   |
| Service    | Name of the WAN connection                             |
| Interface  | Name of the interface for WAN                          |
| Protocol   | Shows the connection type                              |
| IGMP       | Shows Internet Group Management Protocol (IGMP) status |
| Nat        | Shows Network Address Translation (NAT) status         |
| QoS        | Shows Quality of Service (QoS) status                  |
| State      | Shows the connection state of the WAN connection       |
| Status     | Lists the status of DSL link                           |
| IP Address | Shows WAN IP address                                   |

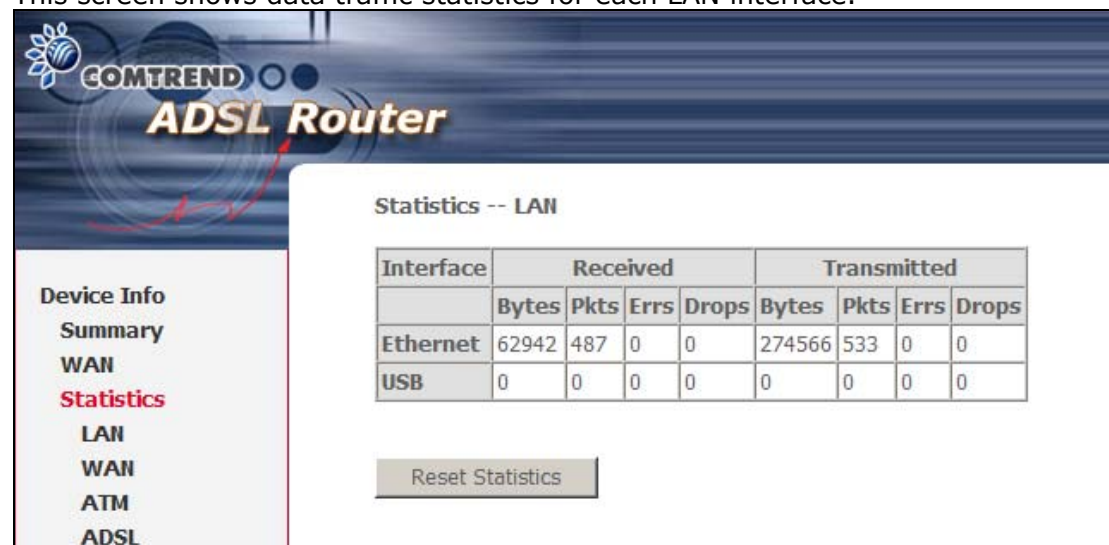
## 5.2 Statistics

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

**NOTE:** These screens are updated every 15 seconds.

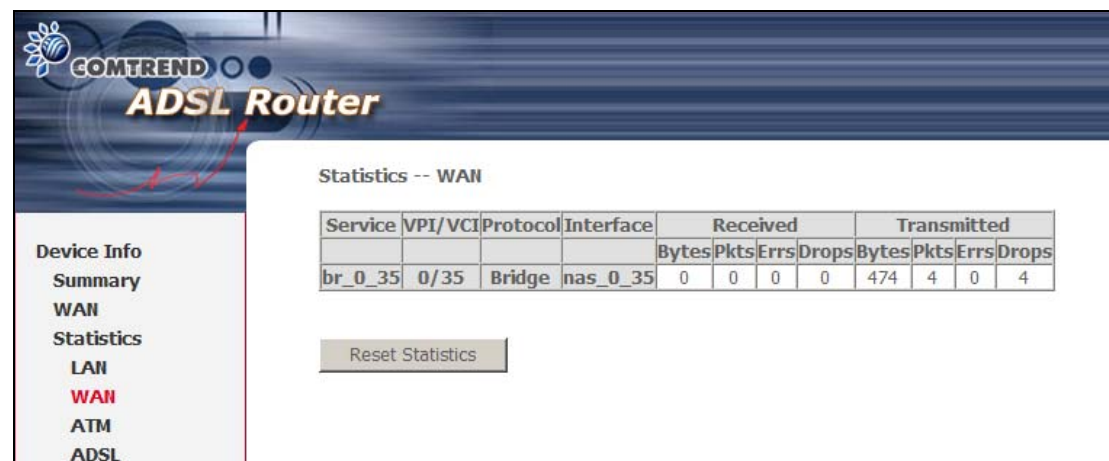
### 5.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



| Heading               | Description  |
|-----------------------|--|
| Interface             | LAN interface(s)   |
| Received/Transmitted: | <ul style="list-style-type: none"> <li>- Bytes: Number of Bytes</li> <li>- Pkts: Number of Packets</li> <li>- Errs: Number of packets with errors</li> <li>- Drops: Number of dropped packets</li> </ul> |

### 5.2.2 WAN Statistics

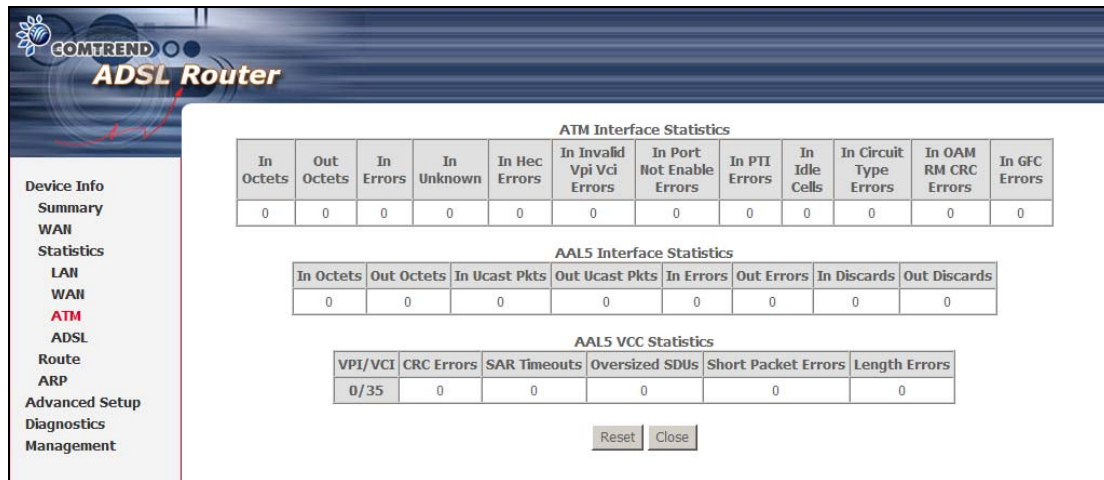


| Heading               | Description  |
|-----------------------|--|
| Service               | WAN service label  |
| VPI/VCI               | ATM Virtual Path/Channel Identifiers   |
| Protocol              | Connection type (e.g. PPPoE, IPoA, Bridge)   |
| Interface             | Shows connection interfaces  |
| Received/Transmitted: | <ul style="list-style-type: none"> <li>- Bytes: Number of Bytes</li> <li>- Pkts: Number of Packets</li> <li>- Errs: Number of packets with errors</li> <li>- Drops: Number of dropped packets</li> </ul> |



### 5.2.3 ATM statistics

The following figure shows the ATM statistics screen.



#### ATM Interface Statistics

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

#### AAL5 Interface Statistics

| Heading        | Description  |
|----------------|--|
| In Octets      | Number of received AAL5/AAL0 CPCS PDU octets   |
| Out Octets     | Number of received AAL5/AAL0 CPCS PDU octets transmitted   |
| In Ucast Pkts  | Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission                           |
| Out Ucast Pkts | Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmission                       |
| In Errors      | Number of received AAL5/AAL0 CPCS PDUs received that contain an error. These errors include CRC-32 errors. |



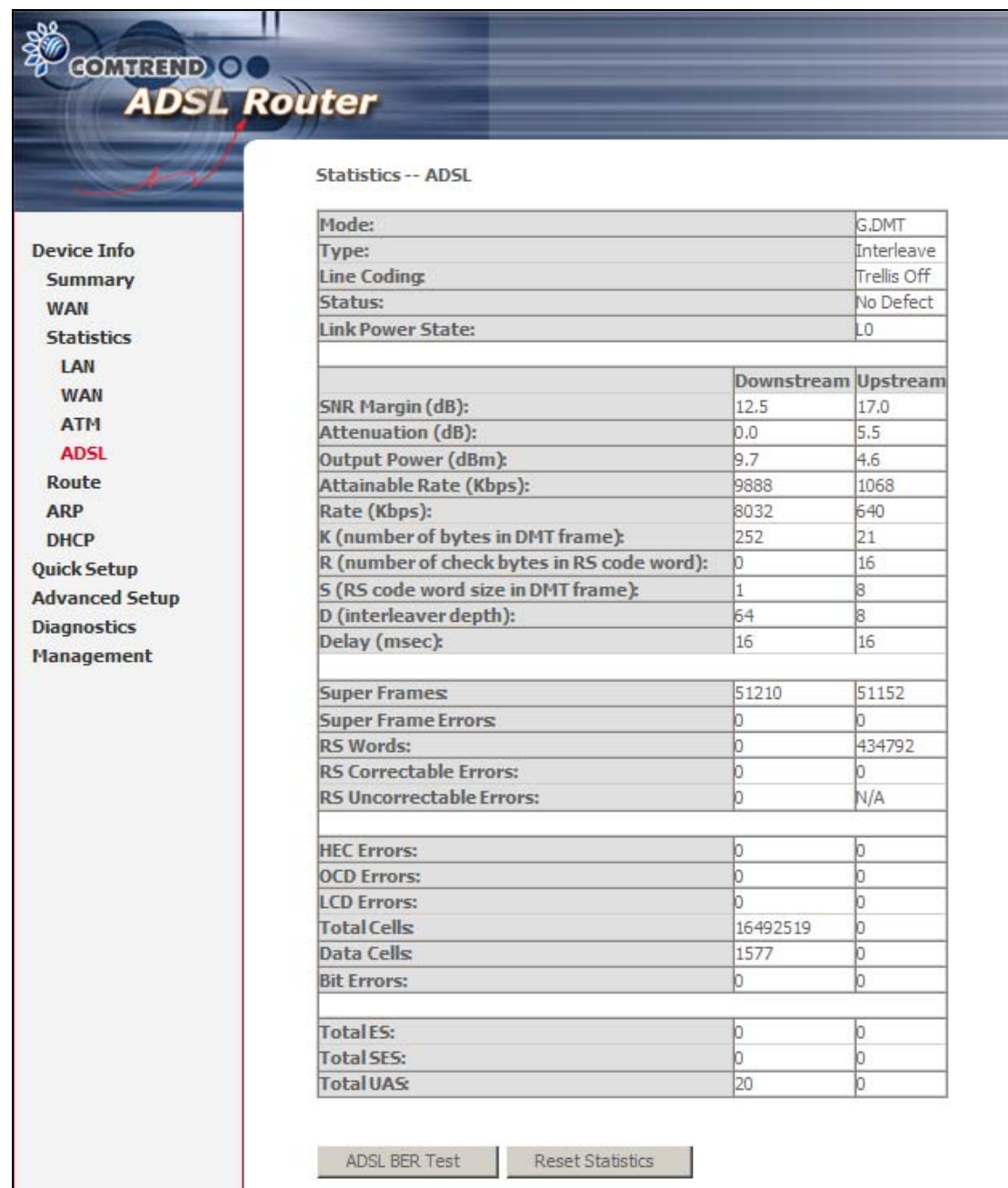
|              |   |
|--------------|---|
| Out Errors   | Number of received AAL5/AAL0 CPCS PDUs that could not be transmitted due to errors.         |
| In Discards  | Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition. |
| Out Discards | This field is not currently used  |

### **AAL5 VCC Statistics**

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

## 5.2.4 ADSL Statistics

The following figure shows the ADSL Statistics screen in G.Dmt mode.



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

| Field            | Description                          |
|------------------|--------------------------------------|
| Mode             | G.Dmt, G.lite, T1.413, ADSL2, ADSL2+ |
| Type             | Channel type Interleave or Fast      |
| Line Coding      | Trellis On/Off                       |
| Status           | Lists the status of the DSL link     |
| Link Power State | Link output power state.             |

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

**In G.DMT mode, the following section is inserted.**

|       |                                       |
|-------|---------------------------------------|
| K     | Number of bytes in DMT frame          |
| R     | Number of check bytes in RS code word |
| S     | RS code word size in DMT frame        |
| D     | The interleaver depth                 |
| Delay | The delay in milliseconds (msec)      |

**In ADSL2+ mode, the following section is inserted.**

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

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

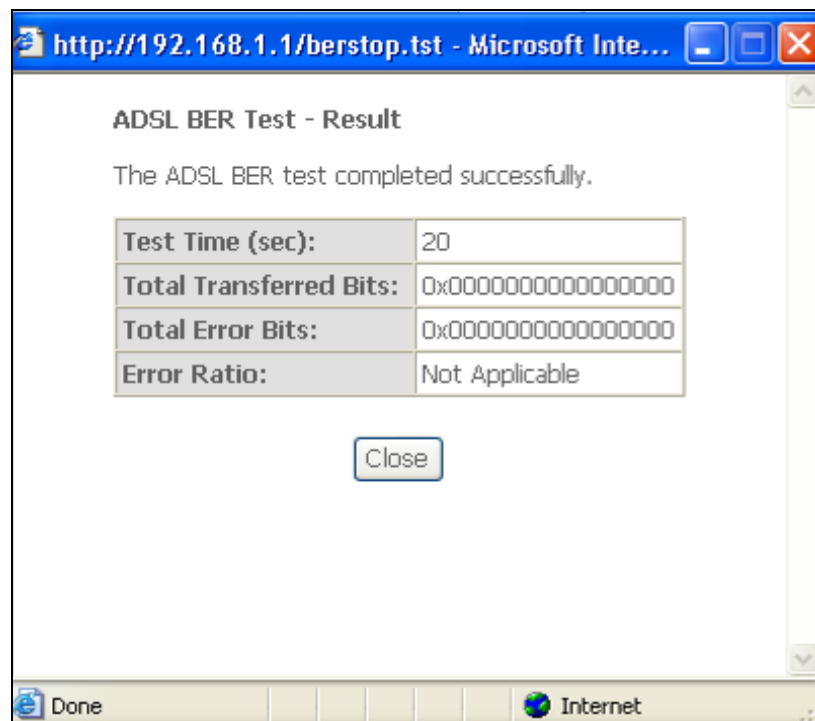
|             |   |
|-------------|---|
| HEC Errors  | Total Number of Header Error Checksum errors            |
| OCD Errors  | Total Number of out-of-cell Delineation errors          |
| LCD Errors  | Total number of Loss of Cell Delineation                |
| Total Cells | Total number of ATM cells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

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

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

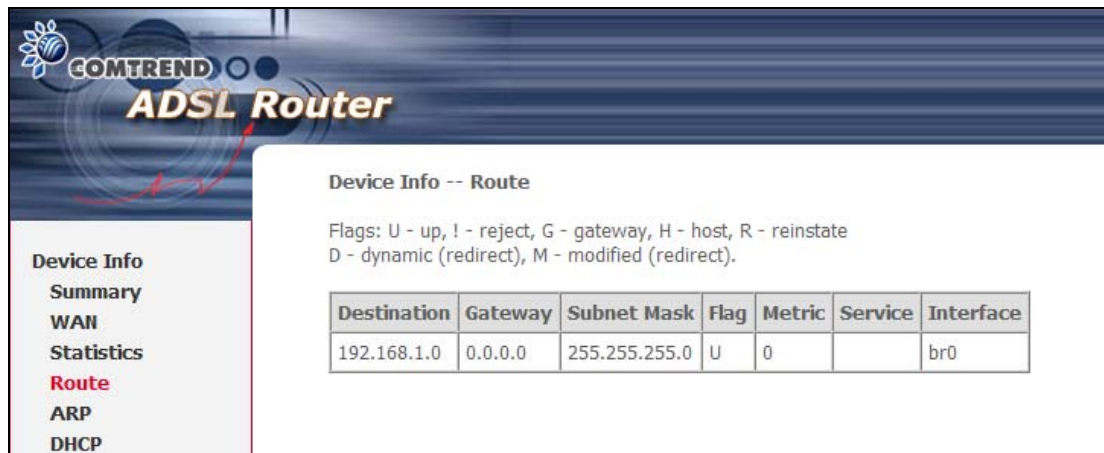


If the test is successful, the pop-up window will display as follows.



## 5.3 Route

Choose **Route** to display the routes that the CT-5071T has found.



The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with options: Device Info, Summary, WAN, Statistics, **Route** (highlighted in red), ARP, and DHCP. The main content area is titled 'Device Info -- Route'. It 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 showing the current route.

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

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

## 5.4 ARP

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



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

| IP address    | Flags    | HW Address        | Device |
|---------------|----------|-------------------|--------|
| 192.168.1.100 | Complete | 00:05:5D:A0:CD:E9 | br0    |

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

## 5.5 DHCP

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



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

| Hostname    | MAC Address       | IP Address  | Expires In |
|-------------|-------------------|-------------|------------|
| TECHWRITER2 | 00:05:5D:A0:CD:E9 | 192.168.1.2 | 51 seconds |

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

# Chapter 6 Advanced Setup

This chapter explains the following screens:

|                        |                 |
|------------------------|-----------------|
| 6.1 WAN                | 6.6 Routing     |
| 6.2 LAN                | 6.7 DNS         |
| 6.3 NAT                | 6.8 DSL         |
| 6.4 Security           | 6.9 Certificate |
| 6.5 Quality of Service |                 |

## 6.1 WAN

This screen allows for the configuration of WAN interfaces. To **Add** a new WAN connection, click **Add**. To edit an existing connection, click the **Edit** button next to the connection. To complete the **Add** or **Edit** go to **STEP 2** in section [4.2 Manual Quick Setup](#). To remove a connection select its radio button under the **Remove** column of the table and click the **Remove** button under the table.

COMTREND ADSL Router

Wide Area Network (WAN) Setup

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

| VPI/VCI | Con. ID | Category | Service      | Interface  | Protocol | Igmp     | Nat     | QoS      | VlanId | State   | Remove                   | Edit |
|---------|---------|----------|--------------|------------|----------|----------|---------|----------|--------|---------|--------------------------|------|
| 0/35    | 1       | UBR      | br_0_35      | nas_0_35   | Bridge   | N/A      | N/A     | Disabled | N/A    | Enabled | <input type="checkbox"/> | Edit |
| 1/35    | 1       | UBR      | pppoe_1_35_1 | ppp_1_35_1 | PPPoE    | Disabled | Enabled | Enabled  | N/A    | Enabled | <input type="checkbox"/> | Edit |

Add Remove Save/Reboot

| Heading   | Description  |
|-----------|--|
| VPI/VCI   | ATM VPI (0-255) / VCI (32-65535)                       |
| Con. ID   | WAN connection ID number                               |
| Category  | ATM service category                                   |
| Service   | Name of the WAN connection                             |
| Interface | Name of the interface for WAN                          |
| Protocol  | Shows the connection type                              |
| Igmp      | Shows Internet Group Management Protocol (IGMP) status |
| Nat       | Shows Network Address Translation (NAT) status         |
| QoS       | Shows Quality of Service (QoS) status                  |
| VlanId    | VLAN ID is used for VLAN Tagging (IEEE 802.1Q)         |
| State     | Shows the connection state of the WAN connection       |
| Remove    | Used to select connections for removal                 |
| Edit      | Used to edit connections                               |

## 6.2 LAN

From this screen, LAN interface settings can be configured.

**COMTREND ADSL Router**

**Local Area Network (LAN) Setup**

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

IP Address:

Subnet Mask:

☐ Enable UPnP

☒ Enable IGMP Snooping

☒ Standard Mode

☐ Blocking Mode

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

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

**NOTE:** NAT is enabled so **UPnP** is shown above (see underlined notes below).

Consult the field descriptions below for more details.

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

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

**Enable UPnP:** Tick the box to enable Universal Plug and Play.  
*This option is hidden when NAT disabled or if no PVC exists*

**Enable IGMP Snooping:** This function does not apply to this model.

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

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

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

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

IP Address:

Subnet Mask:



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

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

**NOTE:** The **Save** button simply saves changes, while the **Save/Reboot** button both saves and reboots the device to make any changes effective.

## 6.3 NAT

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

### 6.3.1 Virtual Servers

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



**COMTREND ADSL Router**

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

**COMTREND ADSL Router**

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE:** The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified. Remaining number of entries that can be configured:32

Server Name:

☒ Select a Service: Select One

☐ Custom Server:

Server IP Address: 192.168.1.

Save/Apply

| External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End |
|---------------------|-------------------|----------|---------------------|-------------------|
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |
|                     |                   | TCP      |                     |                   |

Save/Apply

Consult the table below for field and header descriptions.


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

### 6.3.2 Port Triggering

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

[illegible]

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



Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

ALG

Security

Quality of Service

Routing

DNS Server

DSL

Certificate

Diagnostics

Management

## NAT -- Port Triggering

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

**Remaining number of entries that can be configured:32**

Application Name:

☒ Select an application: Select One
☐ Custom application:

Save/Apply

| Trigger Port Start | Trigger Port End | Trigger Protocol | Open Port Start | Open Port End | Open Protocol |
|--------------------|------------------|------------------|-----------------|---------------|---------------|
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |
|                    |                  | TCP              |                 |               | TCP           |

Save/Apply

Consult the table below for field and header descriptions.

| Field/Header   | Description  |
|--|--|
| Select an Application<br><b>Or</b><br>Custom Application | User should select the application from the list.<br><b>Or</b><br>User can enter the name of their choice. |

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

### 6.3.3 DMZ Host

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

**COMTREND ADSL Router**

**NAT -- DMZ Host**

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

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

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

DMZ Host IP Address:

**Save/Apply**

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

### 6.3.4 ALG

Session Initiation Protocol (SIP - RFC3261) Application Layer Gateway (ALG) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. If the user has an IP phone (SIP) or VoIP gateway (SIP) situated behind the router, the SIP ALG can help VoIP packets pass through when NAT is enabled.

Tick the **SIP Enabled** checkbox ☒ to enable SIP ALG. The text box defines the UDP port to be used (see NOTE below). Adjust settings and then click **Save/Apply**.

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

## 6.4 Security

To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions, with examples, please consult [Appendix A – Firewall](#).

### 6.4.1 IP Filtering

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

**NOTE:** This function is not available when in bridge mode. Instead of IP Filtering, [MAC Filtering](#) (pg. 46) performs a similar function.

#### OUTGOING IP FILTER

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

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

The screenshot shows the 'Add IP Filter -- Outgoing' configuration page. On the left is a navigation menu with 'Device Info' and 'Advanced Setup' expanded, showing options like WAN, LAN, NAT, Security, IP Filtering (Outgoing, Incoming), MAC Filtering, Parental Control, Quality of Service, Routing, DNS Server, DSL, and Certificate. The main area has a title 'Add IP Filter -- Outgoing' and a description: '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.' Below this are input fields for Filter Name, Protocol (a dropdown menu), Source IP address, Source Subnet Mask, Source Port (port or port:port), Destination IP address, Destination Subnet Mask, and Destination Port (port or port:port). A 'Save/Apply' button is at the bottom right.

Consult the table below for field descriptions.

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

## INCOMING IP FILTER

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

The screenshot shows the 'Incoming IP Filtering Setup' configuration page. The left navigation menu is similar to the previous screen, but 'Incoming' is highlighted under IP Filtering. The main area has a title 'Incoming IP Filtering Setup' and a description: '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.' and a table with columns: Filter Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are 'Add' and 'Remove' buttons.

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



**COMTREND ADSL Router**

**Add IP Filter -- Incoming**

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

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

☒ Select All  
☒ pppoe\_1\_35\_1/ppp\_1\_35\_1

For detailed field descriptions, please reference the previous table.

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

## 6.4.2 MAC Filtering

**NOTE:** This option is only available in bridge mode. Other modes (i.e. PPPoE/A, IPoA, MER) use [IP Filtering](#) (pg. 44) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5071T can be set according to the following procedure.

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

**COMTREND ADSL Router**

**MAC Filtering Setup**

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

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 |
|--|----------|-----------------|------------|-----------------|--------|
| <a href="#">Add</a> <a href="#">Remove</a> |          |                 |            |                 |        |

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

**COMTREND ADSL Router**

**Add MAC Filter**

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

☒ Select All

☒ br\_0\_35/nas\_0\_35

[Save/Apply](#)

Consult the table below for detailed field descriptions.

| Field                   | Description  |
|-------------------------|--|
| Protocol Type           | PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP   |
| Destination MAC Address | Defines the destination MAC address  |
| Source MAC Address      | Defines the source MAC address   |
| Frame Direction         | Select the incoming/outgoing packet interface  |
| WAN Interfaces          | Applies the filter to selected bridge PVCs. These rules are arranged according to bridge PVC, as shown under the VPI/VCI heading on the previous screen. |



### 6.4.3 Parental Control

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

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

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

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:A0:CD:E9  
☐ Other MAC Address

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

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

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

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

**Other MAC Address:** MAC address of another LAN device.

**Days of the Week:** The days the restrictions apply.

**Start Blocking Time:** The time the restrictions start.

**End Blocking Time:** The time the restrictions end.

## 6.5 Quality of Service

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

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

Differentiated Service Configuration

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

[Add](#) [Remove](#)

Choose **Add** to configure network traffic classes. The following screen will display.

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:

Mark IP Precedence:

Mark IP Type Of Service:

Mark 802.1p if 802.1q is enabled on WAN:

Specify Traffic Classification Rules

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

SET-1

Protocol:

Source IP Address:

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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

SET-2

802.1p Priority:

[Save/Apply](#)

| Field                        | Description  |
|------------------------------|--|
| Traffic Class Name           | Enter name for traffic class.  |
| Assign ATM Transmit Priority | Select Low, Medium or High.  |
| Mark IP Precedence           | Select between 0-7. The lower the digit shows the higher the priority.                   |
| Mark IP Type Of Service      | Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay |

|  |   |
|--|---|
| Mark 802.1p if 802.1q is enabled on WAN      | Select between 0-7. The higher the digit shows the higher the priority. |
| <b>SET-1</b>                                 |   |
| Protocol                                     | 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.                        |
| UDP/TCP Source Port (port or port:port)      | Enter source port number or port range.                                 |
| Destination IP address                       | Enter destination IP address.   |
| Destination Subnet Mask                      | Enter destination subnet mask.  |
| UDP/TCP Destination port (port or port:port) | Enter destination port number or port range.                            |
| <b>SET-2</b>                                 |   |
| 802.1p Priority                              | Select between 0-7. The lower the digit shows the higher the priority   |

If the **Enable Differentiated Service Configuration** checkbox ☒ is selected, some **additional fields** will display, as shown below.

**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**

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:

Save/Apply

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

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

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

### 6.6.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox ☒ is selected, the 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**.

**COMTREND ADSL Router**

**Routing -- Default Gateway**

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

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

☒ Enable Automatic Assigned Default Gateway

☐ Use Default Gateway IP Address

☐ Use Interface

Save/Apply

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

## 6.6.2 Static Route

This option allows for the configuration of static routes. Click **Add** to create a new static route. Click **Remove** to delete the selected static route.

The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a sidebar menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, Default Gateway, Static Route (highlighted in red), and RIP. The main content area is titled "Routing -- Static Route (A maximum 32 entries can be configured)". It contains a table with headers: Destination, Subnet Mask, Gateway, Interface, and Remove. Below the table are two buttons: "Add" and "Remove".

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

The screenshot shows the "Routing -- Static Route Add" configuration screen. It includes the same sidebar menu as the previous screen. The main content area has a title "Routing -- Static Route Add" and a instruction: "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." Below this are input fields for "Destination Network Address:" and "Subnet Mask:". There are two checkboxes: "Use Gateway IP Address" (unchecked) and "Use Interface" (checked). The "Use Interface" checkbox is followed by a dropdown menu showing "pppoe\_1\_35\_1/ppp\_1\_35\_1". At the bottom right is a "Save/Apply" button.

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

## 6.6.3 RIP

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





**COMTREND ADSL Router**

**Routing -- RIP Configuration**

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

Global RIP Mode ☒ Disabled ☐ Enabled

| Interface  | VPI/VCI | Version | Operation | Enabled                  |
|------------|---------|---------|-----------|--------------------------|
| br0        | (LAN)   | 2       | Active    | <input type="checkbox"/> |
| ppp_1_35_1 | 1/35    | 2       | Passive   | <input type="checkbox"/> |

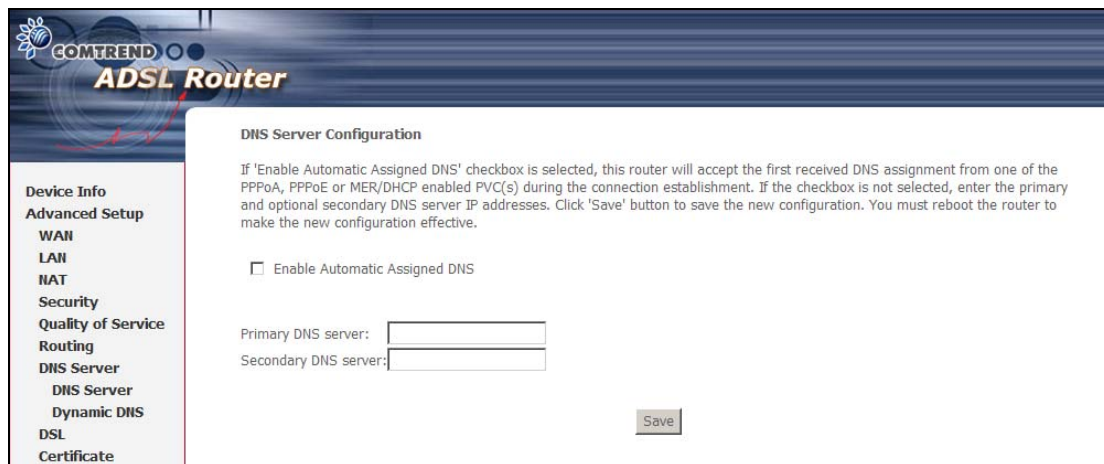
Save/Apply

**Device Info**  
**Advanced Setup**  
WAN  
LAN  
NAT  
Security  
Quality of Service  
Routing  
Default Gateway  
Static Route  
**RIP**

## 6.7 DNS Server

### 6.7.1 DNS Server

If the **Enable Automatic Assigned DNS** checkbox ☒ is selected, this router will accept the first received DNS assignment from one of the DHCP enabled PVC(s). If the checkbox ☒ is not selected, enter the primary and optional secondary DNS server IP addresses. Click **Save** to save the new configuration.



**COMTREND ADSL Router**

**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

Primary DNS server:

Secondary DNS server:

Save

**Device Info**  
**Advanced Setup**  
WAN  
LAN  
NAT  
Security  
Quality of Service  
Routing  
**DNS Server**  
DNS Server  
Dynamic DNS  
DSL  
Certificate

**NOTE:** You must reboot the router to make the new configuration effective.

### 6.7.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the CT-5071T to be more easily accessed from various locations on the Internet.

**COMTREND ADSL Router**

**Dynamic DNS**

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

Choose Add or Remove to configure Dynamic DNS.

| Hostname  | Username | Service | Interface | Remove |
|---|----------|---------|-----------|--------|
| <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div> |          |         |           |        |

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

**COMTREND ADSL Router**

**Add dynamic DDNS**

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

D-DNS provider:

Hostname:

Interface:

**DynDNS Settings**

Username:

Password:

Consult the table below for field descriptions.

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

## 6.8 DSL

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

**COMTREND ADSL Router**

**DSL Settings**

Select the modulation below.

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

Select the phone line pair below.

- ☒ Inner pair
- ☐ Outer pair

Capability

- ☒ Bitswap Enable
- ☐ SRA Enable

Apply

| DSL Mode         | Data Transmission Rate - Mbit/s (Megabits per second)           |                      |
|------------------|---|----------------------|
| G.Dmt            | Downstream: 12 Mbit/s   | Upstream: 1.3 Mbit/s |
| G.lite           | Downstream: 4 Mbit/s  | Upstream: 0.5 Mbit/s |
| T1.413           | Downstream: 8 Mbit/s  | Upstream: 1.0 Mbit/s |
| ADSL2            | Downstream: 12 Mbit/s   | Upstream: 1.0 Mbit/s |
| AnnexL           | Supports longer loops but with reduced transmission rates       |                      |
| ADSL2+           | Downstream: 24 Mbit/s   | Upstream: 1.0 Mbit/s |
| AnnexM           | Downstream: 24 Mbit/s   | Upstream: 3.5 Mbit/s |
| Options          | Description   |                      |
| Inner/Outer Pair | Select the inner or outer pins of the twisted pair (RJ11 cable) |                      |
| Bitswap Enable   | Enables adaptive handshaking functionality                      |                      |
| SRA Enable       | Enables Seamless Rate Adaptation (SRA)                          |                      |



## 6.9 Certificate

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

### 6.9.1 Local

The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS Server, DSL, Certificate (highlighted in red), Local, and Trusted CA. The main content area is titled "Local Certificates" and contains 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 headers: Name, In Use, Subject, Type, and Action. Under the table are two buttons: "Create Certificate Request" and "Import Certificate".

#### CREATE CERTIFICATE REQUEST

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

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

The screenshot shows the "Create new certificate request" form in the COMTREND ADSL Router web interface. The form includes the following fields: Certificate Name, Common Name, Organization Name, State/Province Name, and Country/Region Name (a dropdown menu currently showing "US (United States)"). Below the fields is an "Apply" button. A note at the top of the form states: "To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate."

The following table is provided for your reference.

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

## IMPORT CERTIFICATE

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

The screenshot shows the 'Import certificate' page in the COMTREND ADSL Router web interface. The sidebar on the left contains the following navigation links: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS Server, DSL, Certificate (selected), Local, Trusted CA, Diagnostics, and Management. The main content area is titled 'Import certificate' and includes the instruction 'Enter certificate name, paste certificate content and private key.' Below this, there are three input fields: 'Certificate Name' (a small text box), 'Certificate' (a large text area containing the placeholder text '-----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----'), and 'Private Key' (a large text area containing the placeholder text '-----BEGIN RSA PRIVATE KEY-----<br><insert private key here><br>-----END RSA PRIVATE KEY-----'). An 'Apply' button is located at the bottom right of the form.

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

## 6.9.2 Trusted CA

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

The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS Server, DSL, Certificate, Local, and Trusted CA. The 'Trusted CA' option is selected. The main content area is titled 'Trusted CA (Certificate Authority) Certificates'. Below the title, it says: '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. Below the table is a button labeled 'Import Certificate'.

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

The screenshot shows the 'Import CA certificate' page in the COMTREND ADSL Router web interface. The left navigation menu is the same as in the previous screenshot, with 'Trusted CA' selected. The main content area is titled 'Import CA certificate'. Below the title, it says: 'Enter certificate name and paste certificate content.' There are two input fields: 'Certificate Name:' with a text box, and 'Certificate:' with a large text area. The text area contains the following text: '-----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----'. At the bottom right of the page is an 'Apply' button.

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

# Chapter 7 Diagnostics

Diagnostics screens for PPPoE and Bridge connection types are shown below.

## PPPoE Connection

**COMTREND ADSL Router**

**Device Info**  
**Advanced Setup**  
**Diagnostics**  
**Management**

**pppoe\_1\_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(1-4) Connection: | PASS | <a href="#">Help</a> |
| Test your USB Connection:       | DOWN | <a href="#">Help</a> |

**Test the connection to your DSL service provider**

|                                  |      |                      |
|----------------------------------|------|----------------------|
| Test ADSL Synchronization:       | FAIL | <a href="#">Help</a> |
| Test ATM OAM F5 segment ping:    | FAIL | <a href="#">Help</a> |
| Test ATM OAM F5 end-to-end ping: | FAIL | <a href="#">Help</a> |

**Test the connection to your Internet service provider**

|                                  |      |                      |
|----------------------------------|------|----------------------|
| Test PPP server connection:      | FAIL | <a href="#">Help</a> |
| Test authentication with ISP:    | FAIL | <a href="#">Help</a> |
| Test the assigned IP address:    | FAIL | <a href="#">Help</a> |
| Ping default gateway:            | FAIL | <a href="#">Help</a> |
| Ping primary Domain Name Server: | PASS | <a href="#">Help</a> |

[Previous Connection](#)  
[Test](#) [Test With OAM F4](#)

## Bridge Connection

**COMTREND ADSL Router**

**Device Info**  
**Advanced Setup**  
**Diagnostics**  
**Management**

**br\_0\_35 Diagnostics**

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

**Test the connection to your local network**

|                                 |      |                      |
|---------------------------------|------|----------------------|
| Test your ENET(1-4) Connection: | PASS | <a href="#">Help</a> |
| Test your USB Connection:       | DOWN | <a href="#">Help</a> |

**Test the connection to your DSL service provider**

|                                  |      |                      |
|----------------------------------|------|----------------------|
| Test ADSL Synchronization:       | FAIL | <a href="#">Help</a> |
| Test ATM OAM F5 segment ping:    | FAIL | <a href="#">Help</a> |
| Test ATM OAM F5 end-to-end ping: | FAIL | <a href="#">Help</a> |

[Next Connection](#)  
[Test](#) [Test With OAM F4](#)

## General Information

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

The basic test set (no PVC configured) is described in the table below. For help with the other tests click on the [Help](#) link next to the test condition for guidance

| Test                 | Description   |
|----------------------|---|
| ENET Connection      | <b>Pass:</b> Indicates that the CT-5071T has detected the Ethernet interface on your computer.<br><b>Fail:</b> Indicates that the CT-5071T does not detect the Ethernet interface on your computer. |
| USB connection*      | <b>Pass:</b> Indicates that the CT-5071T has detected the USB interface on your computer.<br><b>Down:</b> Indicates that the CT-5071T does not detect the USB interface on your computer.           |
| ADSL Synchronization | <b>Pass:</b> Indicates that the CT-5071T has detected a DSL signal from the telephone company.<br><b>Fail:</b> Indicates that the CT-5071T does not detect a DSL signal from the telephone company. |

\* This device does not have a USB port.

# Chapter 8 Management

The Management menu has the following maintenance functions and processes:

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| <a href="#">8.1 Settings</a>      | <a href="#">8.5 Internet Time</a>   |
| <a href="#">8.2 System Log</a>    | <a href="#">8.6 Access Control</a>  |
| <a href="#">8.3 SNMP Agent</a>    | <a href="#">8.7 Update Software</a> |
| <a href="#">8.4 TR-069 Client</a> | <a href="#">8.8 Save and Reboot</a> |

## 8.1 Settings

This includes [Backup Settings](#), [Update Settings](#), and [Restore Default](#) screens.

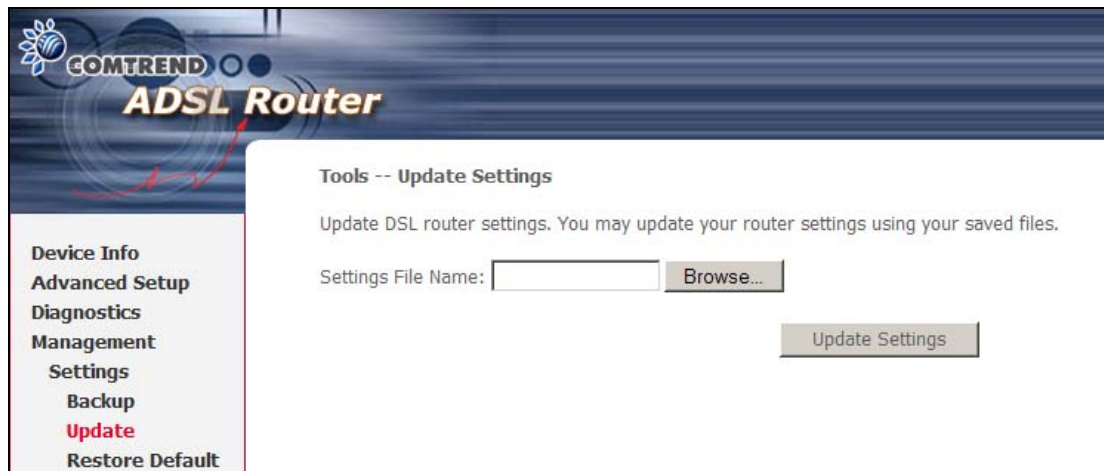
### 8.1.1 Backup Settings

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



### 8.1.2 Update Settings

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

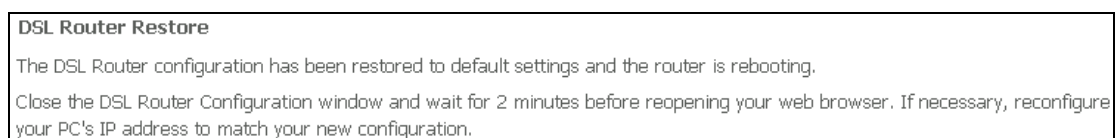


### 8.1.3 Restore Default

Click **Restore Default Settings** to restore the CT-5071T to factory default settings.



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



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

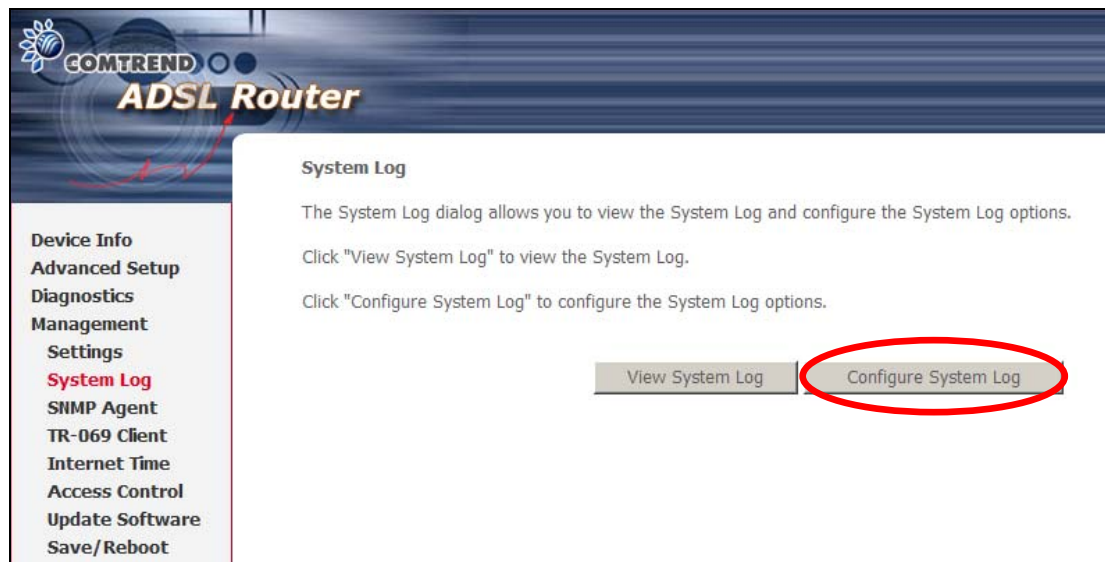
**NOTE:** This entry has the same effect as the **Reset** button. The CT-5071T board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.



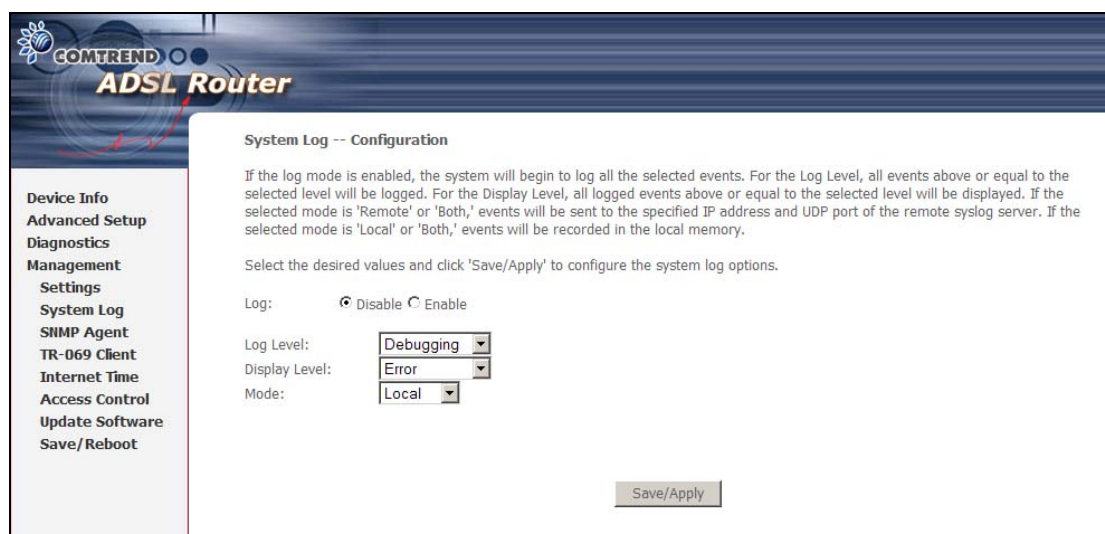
## 8.2 System Log

This function allows a system log to be kept and viewed upon request. Follow the steps below to configure, enable, and view the system log.

**Step 1:** Click **Configure System Log** as shown below.



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



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

| Option    | Description   |
|-----------|---|
| Log       | Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.  |
| Log level | Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-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. |



|               |   |
|---------------|---|
|               | <p>By default, the log level is "Debugging", which is the lowest critical level.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> <li>• Emergency = system is unusable</li> <li>• Alert = action must be taken immediately</li> <li>• Critical = critical conditions</li> <li>• Error = Error conditions</li> <li>• Warning = normal but significant condition</li> <li>• Notice= normal but insignificant condition</li> <li>• Informational= provides information for reference</li> <li>• Debugging = debug-level messages</li> </ul> <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 <b>View System Log</b> window for events of this level and above to the highest Emergency level.  |
| Mode          | Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.  |

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

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

## 8.3 SNMP Agent

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

**COMTREND ADSL Router**

**SNMP - Configuration**

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

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

SNMP Agent ☒ Disable ☐ Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

**Save/Apply**

## 8.4 TR-069 Client

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

**COMTREND ADSL Router**

**TR-069 client - Configuration**

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

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

Inform ☒ Disable ☐ Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

☒ Connection Request Authentication

Connection Request User Name:

Connection Request Password:

**Save/Apply** **GetRPCMethods**

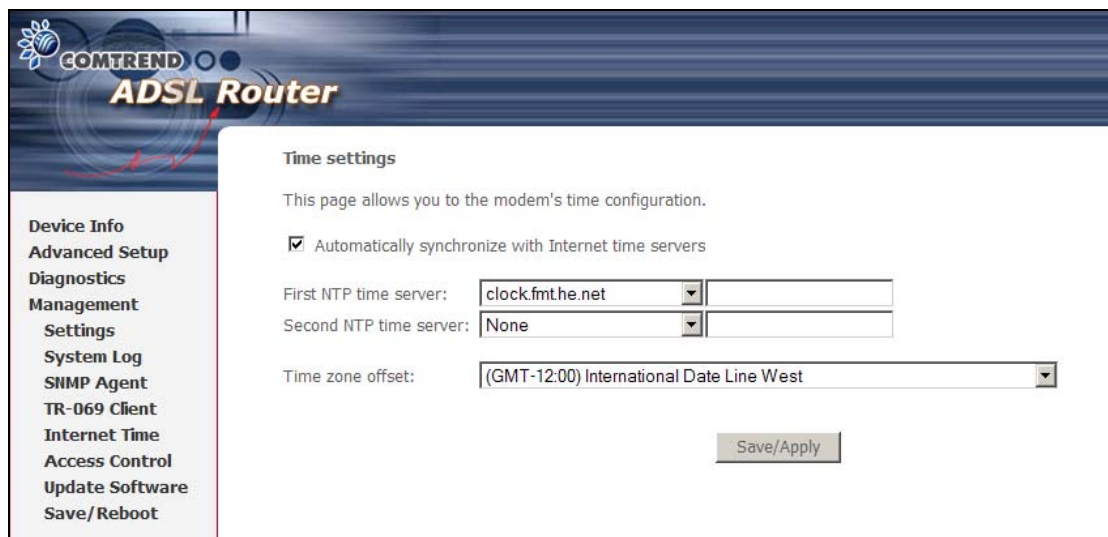
| Option          | Description  |
|-----------------|--|
| Inform          | Disable/Enable TR-069 client on the CPE.   |
| Inform Interval | The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method. |
| ACS URL         | URL for the CPE 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.                                      |
| <b>Connection Request</b> |  |
| Authorization             | Tick the checkbox <input checked="" type="checkbox"/> to enable.   |
| User Name                 | Username used to authenticate an ACS making a Connection Request to the CPE.   |
| Password                  | Password used to authenticate an ACS making a Connection Request to the CPE.   |

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

## 8.5 Internet Time

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



The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with options: Device Info, Advanced Setup, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Internet Time (highlighted), Access Control, Update Software, and Save/Reboot. The main content area is titled "Time settings" and contains the following configuration options:

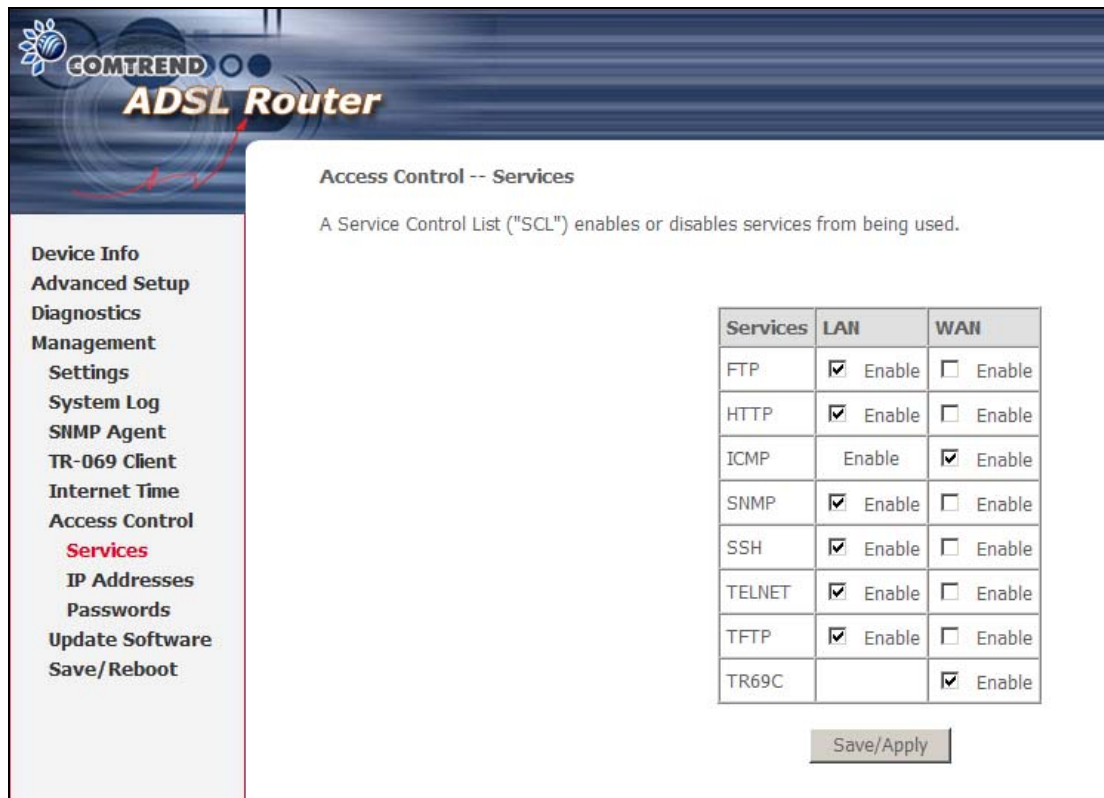
- A descriptive text: "This page allows you to the modem's time configuration."
- A checkbox labeled "Automatically synchronize with Internet time servers" which is checked.
- "First NTP time server:" with a dropdown menu showing "clock.fmtthe.net".
- "Second NTP time server:" with a dropdown menu showing "None".
- "Time zone offset:" with a dropdown menu showing "(GMT-12:00) International Date Line West".
- A "Save/Apply" button at the bottom right.

**NOTE:** Internet Time must be activated to use [Parental Control](#) (page 48). In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

## 8.6 Access Control

### 8.6.1 Services

This option controls the access services over the LAN or WAN. These services include FTP, HTTP, ICMP, SNMP, SSH, TELNET, TFTP, and TR69C (TR-069 client). Enable a service by ticking the corresponding checkbox ☒ under LAN or WAN.



**Comtrend ADSL Router**

**Access Control -- Services**

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

| Services | LAN  | WAN  |
|----------|--|--|
| FTP      | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| HTTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| ICMP     | <input type="checkbox"/> Enable            | <input checked="" type="checkbox"/> Enable |
| SNMP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| SSH      | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| TELNET   | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| TFTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable            |
| TR69C    | <input type="checkbox"/> Enable            | <input checked="" type="checkbox"/> Enable |

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

**NOTES** - 1. The WAN column only appears if a WAN connection is configured.  
2. [Appendix D](#) contains a quick introduction to one SSH client.

### 8.6.2 IP Addresses

This option limits access to the router by IP address. When **Access Control Mode** is enabled, only the IP addresses listed here can access the router.

**COMTREND ADSL Router**

**Access Control -- IP Address**

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

Access Control Mode: ☒ Disable ☐ Enable

| IP Address   | Subnet Mask | Interface | Remove |
|--|-------------|-----------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> |             |           |        |

Before enabling **Access Control Mode**, configure the IP addresses by clicking the **Add** button. Enter the IP address and subnet mask, and select an interface. Click **Save/Apply** to add this IP address to the access control list.

**COMTREND ADSL Router**

**Access Control**

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

| IP Address           | Subnet Mask          | Interface |
|----------------------|----------------------|-----------|
| <input type="text"/> | <input type="text"/> | none      |

### 8.6.3 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5071T is controlled through the following three user accounts:

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

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

**Access Control -- Passwords**

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

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

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

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

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

Username:

Old Password:

New Password:

Confirm Password:

**NOTE:** Passwords must be 16 characters or less.

## 8.7 Update Software

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

**Tools -- Update Software**

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

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

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

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

Software File Name:

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

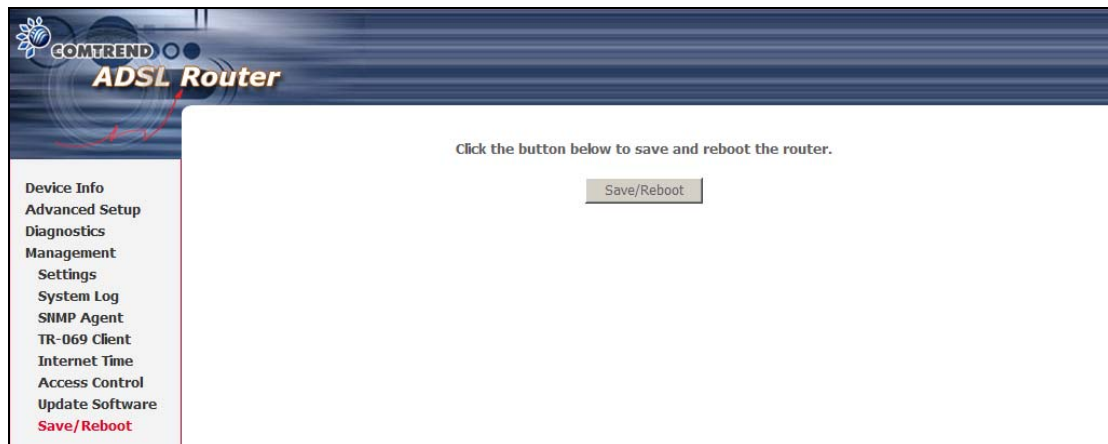
**Step 2:** Enter the path and filename of the firmware image file in the **Software File Name** field or click the **Browse** button to locate the image file.

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

**NOTE:** The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** at the top of the [Device Info](#) Summary screen with the firmware version installed, to confirm the installation was successful.

## 8.8 Save and Reboot

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



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

# Appendix A – Firewall

## STATEFUL PACKET INSPECTION

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

## DENIAL OF SERVICE ATTACK

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

## TCP/IP/PORT/INTERFACE FILTER

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

## OUTGOING IP FILTER

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

**Filter Name:** User defined Filter Name.

**Protocol:** TCP/UDP, TCP, UDP, or ICMP

### Source IP Address/Source Subnet Mask:

Packets with the specific "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 specific "Destination IP Address/Destination Subnet Mask" combination will be dropped.

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

**Example 1:**

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

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



**Example 2:**

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

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

### INCOMING IP FILTER

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

**Filter Name:** User defined Filter Name.

**Protocol:** TCP/UDP, TCP, UDP, or ICMP

**Source IP Address/Source Subnet Mask:** Packets with the specific "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 specific "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.

**Example 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/Subnet Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

**Example 2:**

|                    |                  |
|--------------------|------------------|
| Filter Name        | : In_Filter2     |
| Protocol           | : UDP            |
| Source Address     | : 210.168.219.45 |
| Source Subnet Mask | : 255.255.0.0    |
| Source Port        | : 5060:6060      |
| 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/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

### MAC LAYER FILTER

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

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

**Protocol Type:** PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, or 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:** (Select an interface on which this rule is applied)

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

**Example 1:**

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

Addition of this rule drops all PPPoE frames going from LAN to WAN with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address on the br\_0\_34 WAN interface. All other frames on this interface are forwarded.

**Example 2:** Global Policy : Blocked  
Protocol Type : PPPoE  
Dest. MAC Address : 00:12:34:56:78:90  
Source MAC Address : 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 to LAN with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56 on the br\_0\_34 WAN interface. All other frames on this interface are dropped.

### **DAYTIME PARENTAL CONTROL**

This feature restricts access of a selected LAN device to an outside Network through the CT-5071T, 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 when the restrictions are applied.

**Start Blocking Time:** The time when restrictions on the LAN device begin.

**End Blocking Time:** The time when restrictions on the LAN device end.

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

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

## Appendix B – Pin Assignments

### LINE PORT (RJ11)

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

### LAN Port (RJ45)

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

# Appendix C – Specifications

## Hardware Interface

RJ-11 X1 for ADSL2+, RJ-45 X 1 for LAN, Power Switch X 1, Power Jack X 1, ,  
Reset Button X 1

## WAN Interface

ITU-T G.994.1/G.992.5/G.992.3/G.992.2/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  
Auto-negotiation rate adaptation  
G.DMT / G.lite  
Annex M

## LAN Interface

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

## ATM Attributes

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

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

## Management

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

## Bridge Functions

Transparent bridging and learning..... IEEE 802.1d  
VLAN support ..... Yes  
Spanning Tree Algorithm ..... Yes

## Routing Functions

Static route, RIP v1/v2, NAT/PAT, DHCP Server/Relay/Client, DNS Proxy, ARP,  
IGMP Proxy

## Security Functions

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

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

### **Application Passthrough**

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

**Power Supply** ..... Input: 110 or 220 Vac  
Output: 18 Vac / 500 mA

### **Environment Condition**

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

**Dimensions** ..... 92 mm (W) x 34 mm (H) x 114 mm (D)

### **Kit Weight**

(1\*CT-5071T, 1\*RJ11 cable, 1\*RJ45 cable, 1\*power adapter, 1\*CD-ROM) = 0.65 kg

**Certifications** ..... FCC Part 15 class B, FCC Part 68

|  |
|--|
| <b>NOTE:</b> Specifications are subject to change without notice |
|--|

## Appendix D – SSH Client

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

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

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

To access the router using the Linux ssh client

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

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

To access the router using the Windows “putty” ssh client

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

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

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