COMTREND CORPORATION

CT-5072T

ADSL2+ Ethernet Router

User Manual

Version A1.0, May 19, 2009

261095-004

Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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

⚠ WARNING

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

Copyright

NOTE: This document is subject to change without notice.

Table of Contents

Chapter 1 Introduction

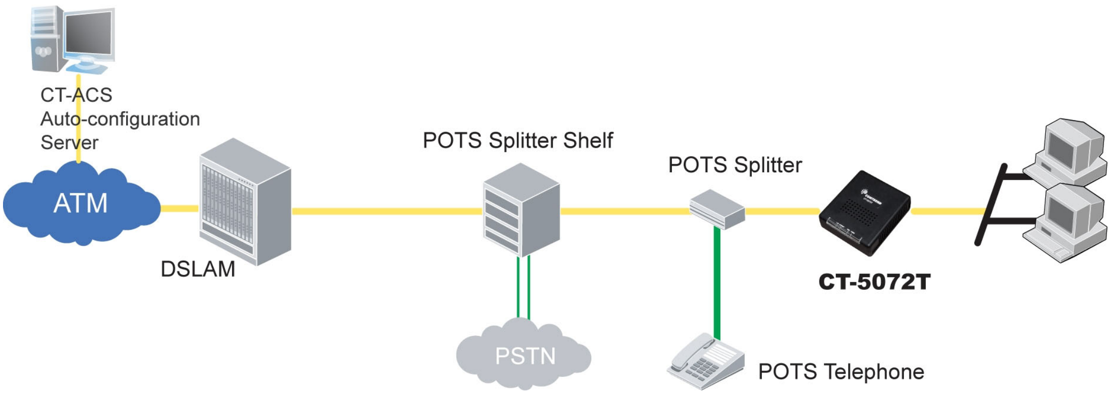
The CT-5072T (TR-069 compliant) ADSL2+ Ethernet Router provides one 10/100 Ethernet port and one ADSL port for Internet access. It features TR-068 compliant panels for easy setup and use. It supports LAN applications, such as Video on Demand, over a regular telephone line at speeds of up to 24 Mbps. It has full routing capabilities and advanced security functions, such as VPNs (Virtual Private Networks) with PPTP pass-through, L2TP pass-through, IPSec pass-through and firewall.

1.1 Features List

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

1.2 Application Diagram

The following diagram depicts the application of the CT-5072T.

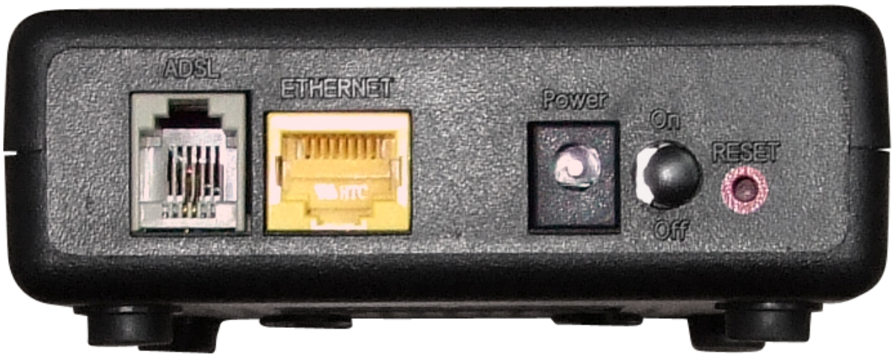


Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

The picture below shows the back panel of the CT-5072T.



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 2.2 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 2.2 LED Indicators for details).

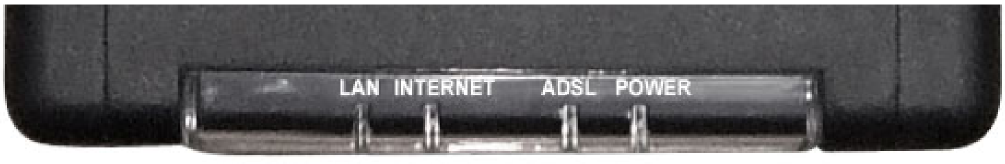
NOTE: If pressed down for more than 20 seconds, the CT-5072T will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

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

ADSL Port (Grey) - Connect the ADSL line to this port with RJ-11 cable.

2.2 LED Indicators

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



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

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: **disabled**
- 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** for PPPoA and PPPoE
  disabled for MER and IPoA
  not available for Bridge

- Firewall and NAT: **enabled** for PPPoE and PPPoA
  disabled for MER and IPoA
  not available for Bridge

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the CT-5072T powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

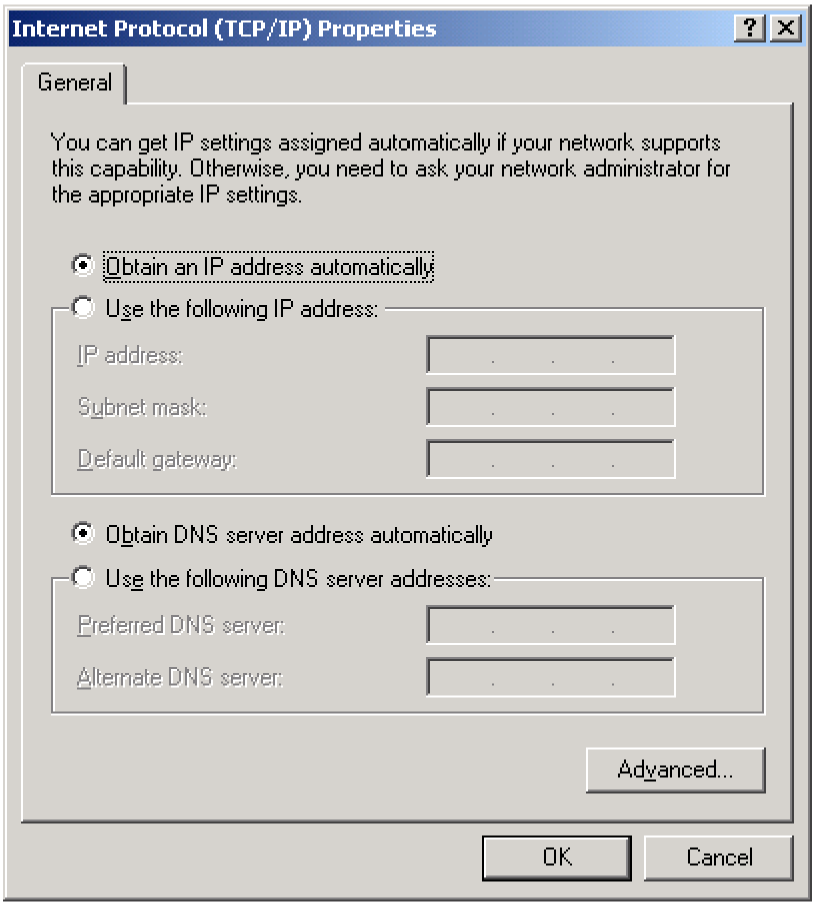
To obtain an IP address from the DCHP server, follow the steps provided below.

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

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

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

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



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

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

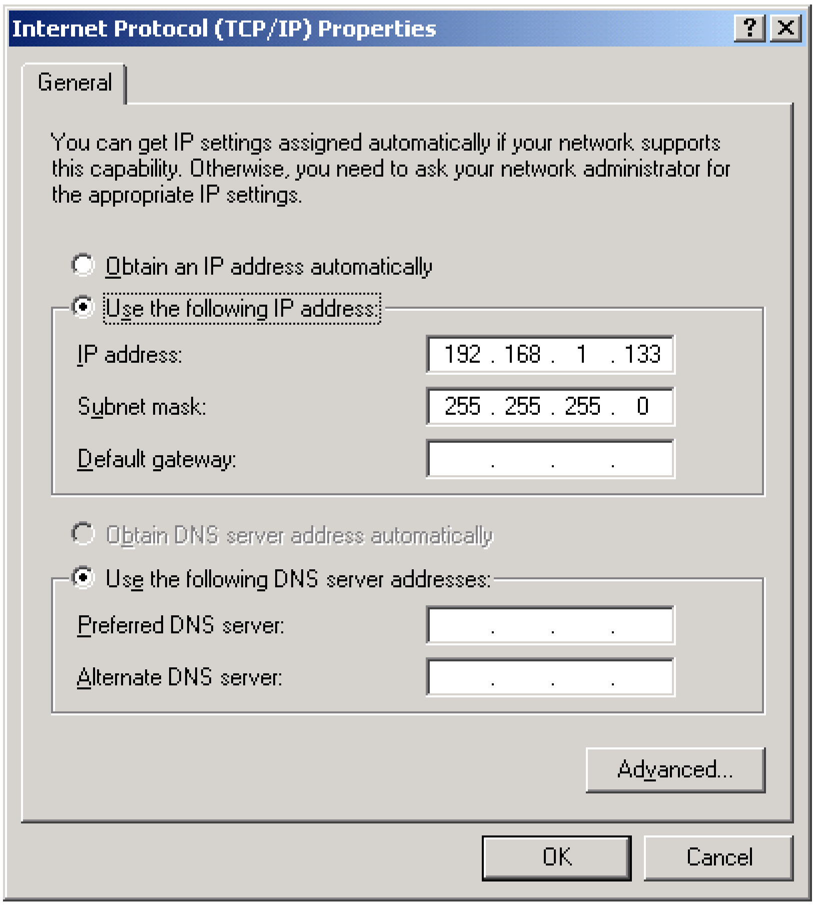
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

3.3 Login Procedure

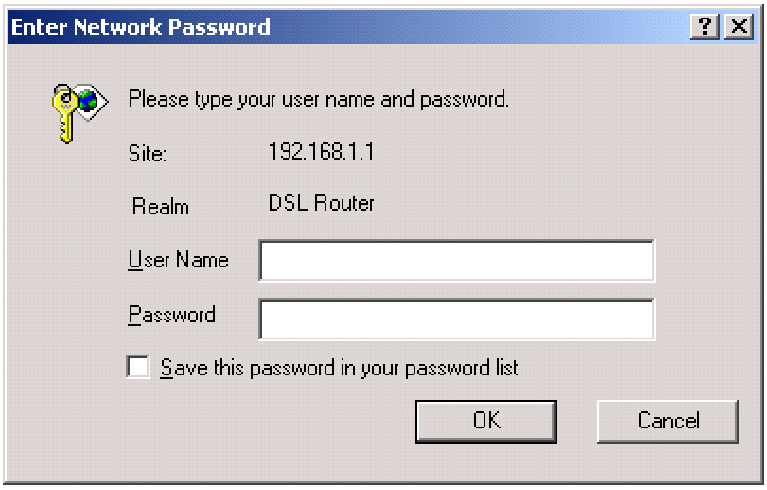
Perform the following steps to login to the web user interface.

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

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

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

STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm DSL Router

User Name

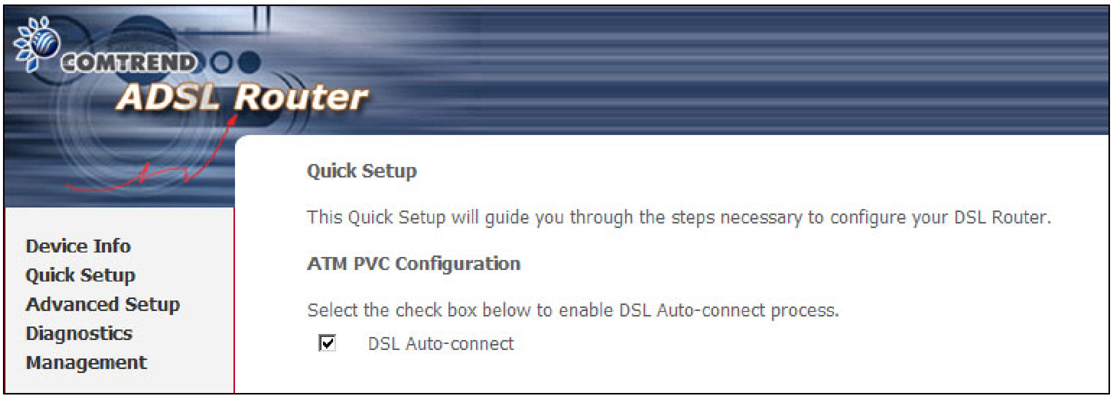
Password

☐ Save this password in your password list

Click **OK** to continue.

NOTE: The login password can be changed later (see section 8.6.3)

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



Quick Setup

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

ATM PVC Configuration

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

☑ DSL Auto-connect

NOTES: If a PVC connection already exists then this Quick Setup screen will be bypassed and the Device Information screen will display instead. The selections available on the main menu (onscreen at left) are based upon the configured connection(s) and user account privileges.

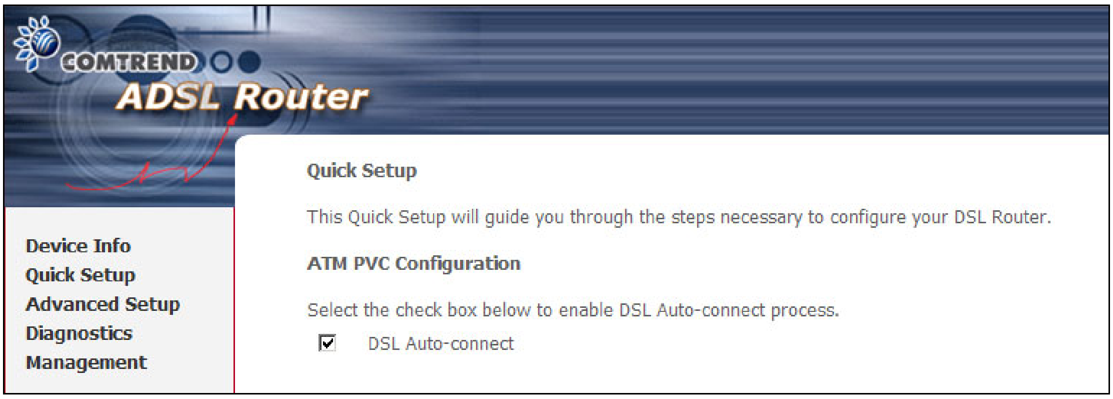
Chapter 4 Quick Setup

After the first login, the **Quick Setup** screen will appear. It is the default screen when no connections exist. It allows for the configuration of connection settings.

4.1 Auto Quick Setup

This function provides an automated process to quickly setup a WAN connection. The CT-5072T will auto-select the best available PVC profile, provided the ADSL link is up (see section 2.2). If you prefer manual connection setup, go to section 4.2.

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



Quick Setup

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

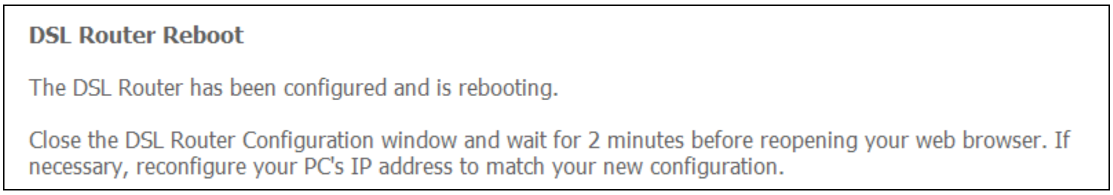
ATM PVC Configuration

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

☑ DSL Auto-connect

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

STEP 3: After setup is complete the CT-5072T will reboot and display this message.



DSL Router Reboot

The DSL Router has been configured and is rebooting.

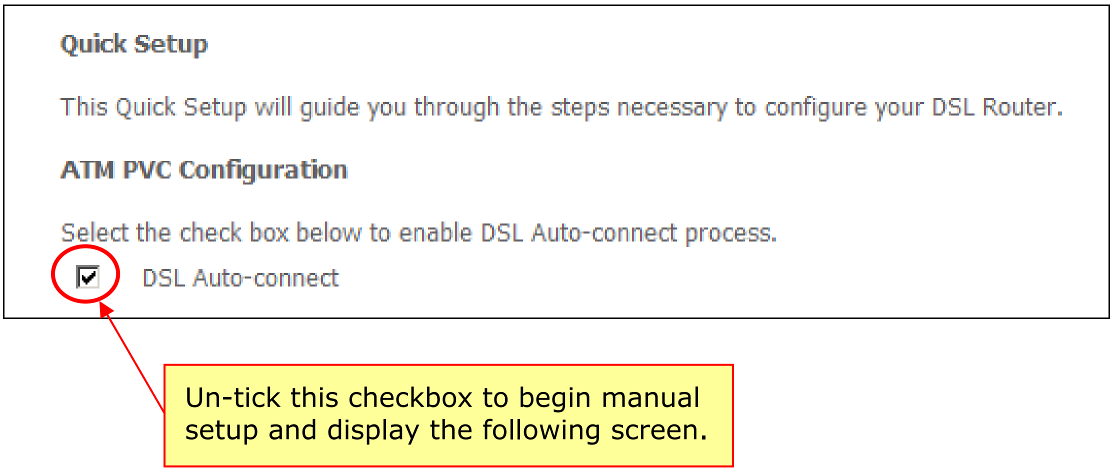
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

NOTE: After the device reboots, the Device Information screen should appear. If the browser does not refresh automatically, close it and restart.

4.2 Manual Quick Setup

To setup the WAN connection manually, follow these instructions:

STEP 1: Un-tick the **DSL Auto-connect** checkbox ☑ on the **Quick Setup** screen.



Quick Setup

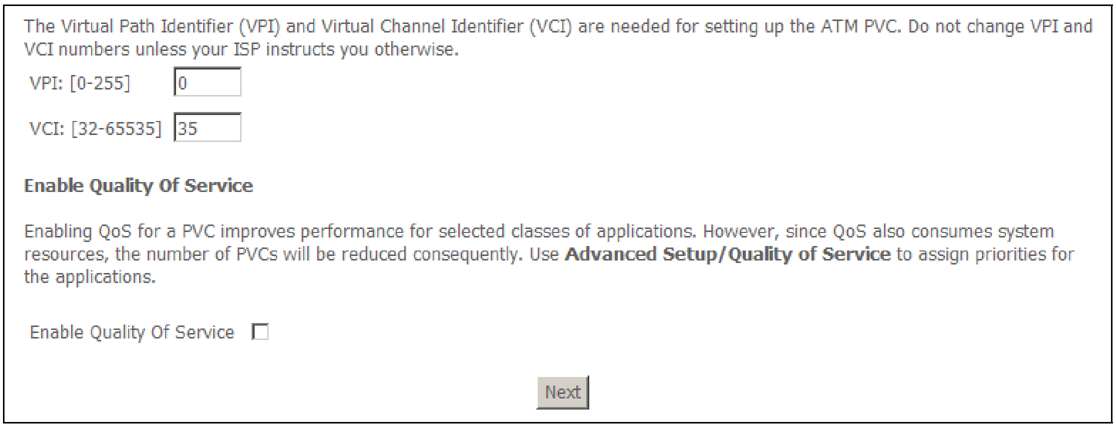
This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

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

☑ DSL Auto-connect

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



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

VPI: [0-255] 0

VCI: [32-65535] 35

Enable Quality Of Service

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

Enable Quality Of Service □

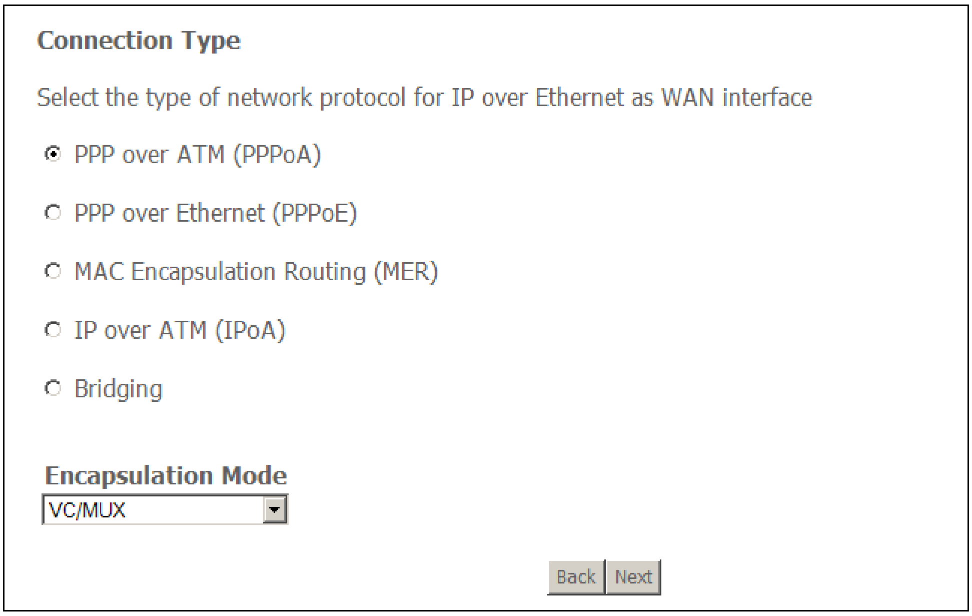
STEP 2: Adjust the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) settings for the connection you wish to establish. You can also **Enable Quality of Service** (QoS) with its checkbox ☑.

Click **Next** to continue.

STEP 3: On the next screen, you can choose the **Connection Type** and select the appropriate **Encapsulation Mode** using the drop-down box.

Here are the available encapsulations for each connection type:

- 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



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

● PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

○ Bridging

Encapsulation Mode

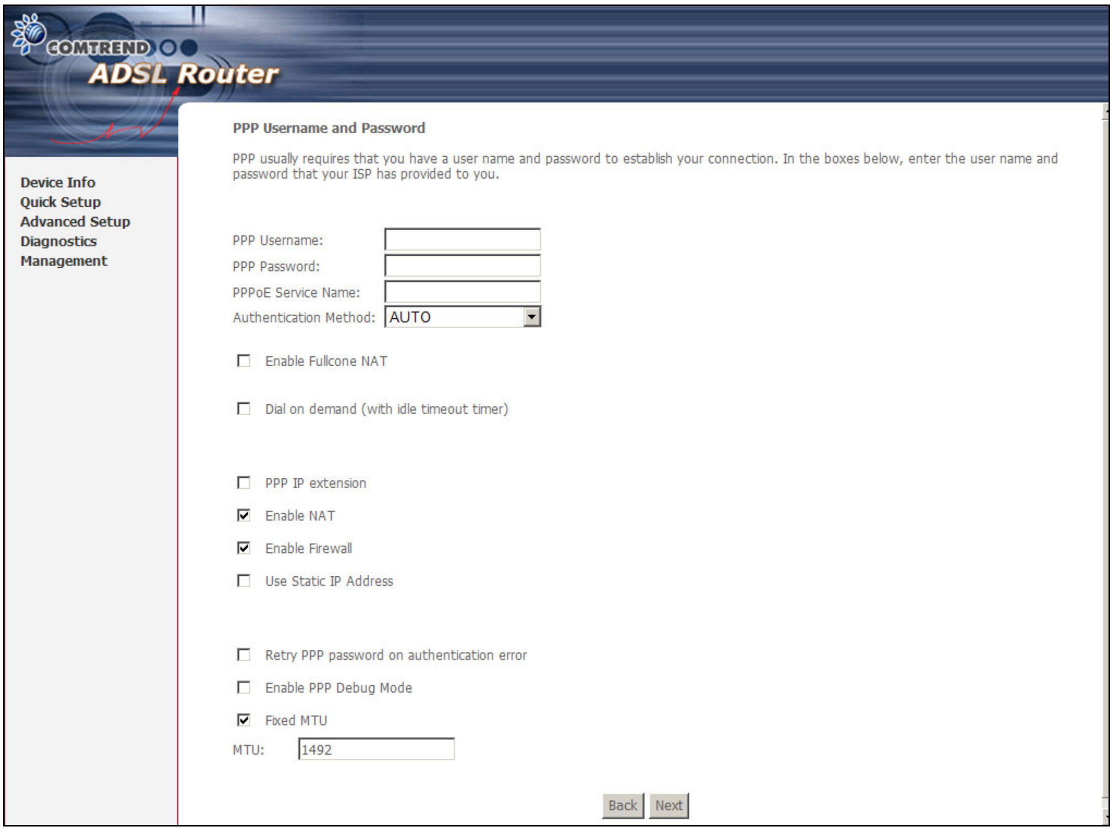
VC/MUX

Click **Next** to continue…

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

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

STEP 4: Enter the PPP settings as provided by your ISP. Click **Next** to continue.



PPP Username and Password

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

☑ Enable NAT

☑ Enable Firewall

□ Use Static IP Address

□ Retry PPP password on authentication error

□ Enable PPP Debug Mode

☑ Fixed MTU

MTU: 1492

PPP SETTINGS

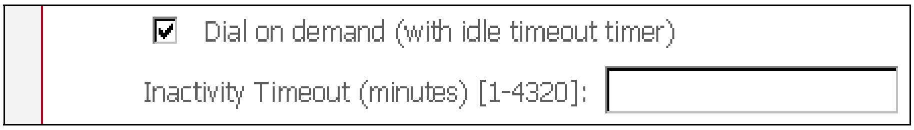
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The CT-5072T can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP EXTENSION

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

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- 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.
- 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.

ENABLE NAT

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

ENABLE FIREWALL

To enable IP packet filtering, tick this checkbox ☑. The Advanced Setup → Security → IP Filtering option will appear on the main menu after reboot. Disable this function when not required for improved performance.

USE STATIC IP ADDRESS

Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

RETRY PPP PASSWORD ON AUTHENTICATION ERROR

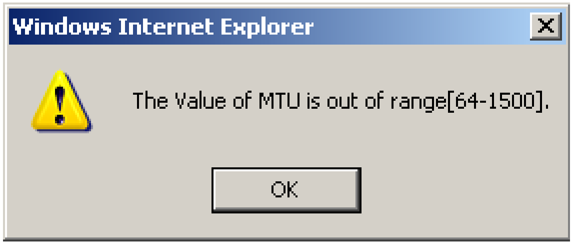
Tick the checkbox ☑ to enable this function.

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.

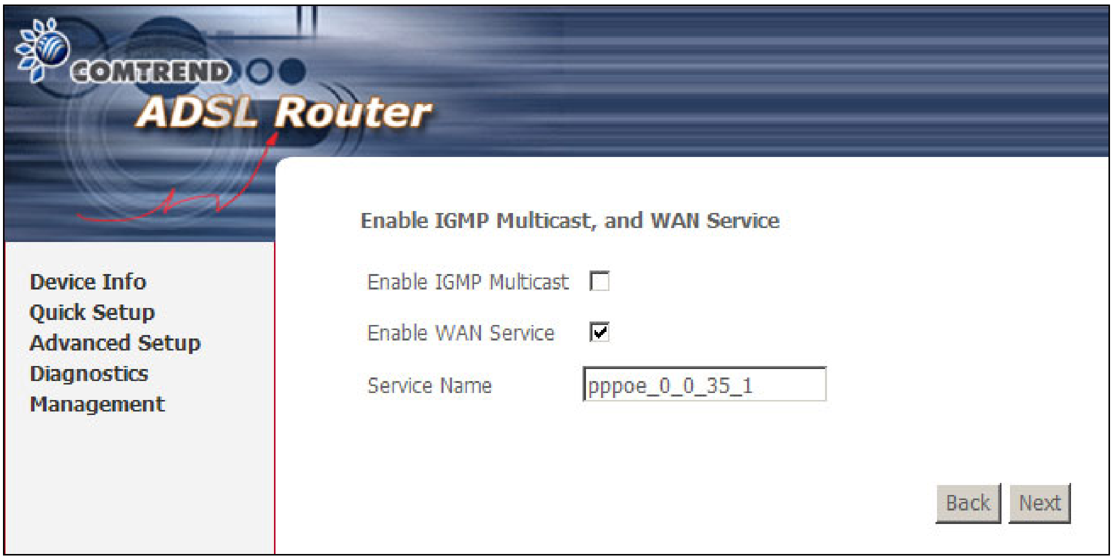
FIXED MTU

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.



The Value of MTU is out of range[64-1500].

STEP 5: This screen provides access to IGMP Multicast and WAN Service settings. Enable each service by selecting its checkbox ☑. Click **Next** to continue.



Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name pppoe_0_0_35_1

ENABLE IGMP MULTICAST

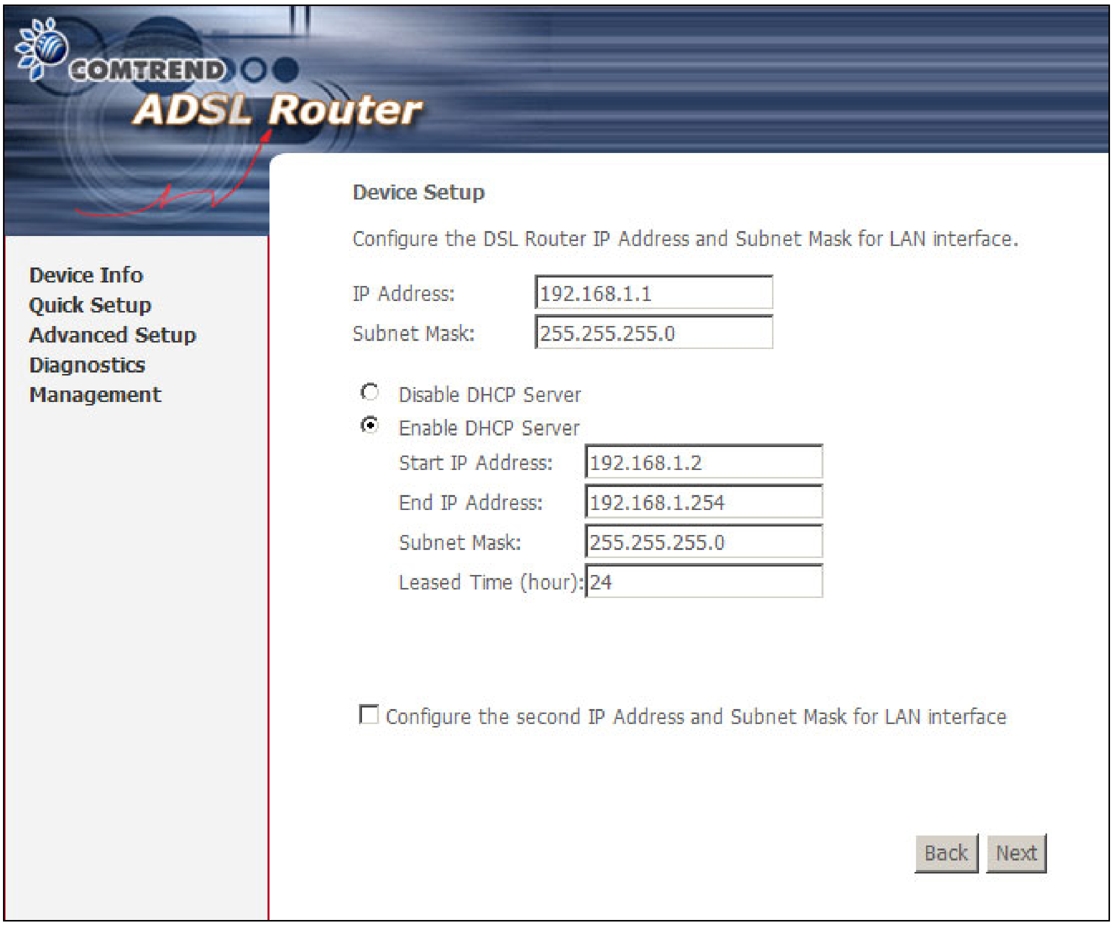
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IP hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE WAN SERVICE

Tick the checkbox ☑ to enable WAN service.

SERVICE NAME
This is the WAN Service label.

STEP 6: The Device Setup screen is used to configure LAN interface settings.



Device Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24

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

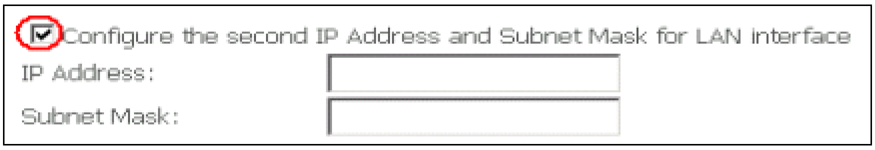
The IP address and Subnet Mask define the location of the CT-5072T on the LAN.

To auto-assign IP addresses, DNS server and default gateway to other LAN devices, select the **Enable DHCP server** radio button. You must also enter the Start and End IP address, Subnet Mask 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.

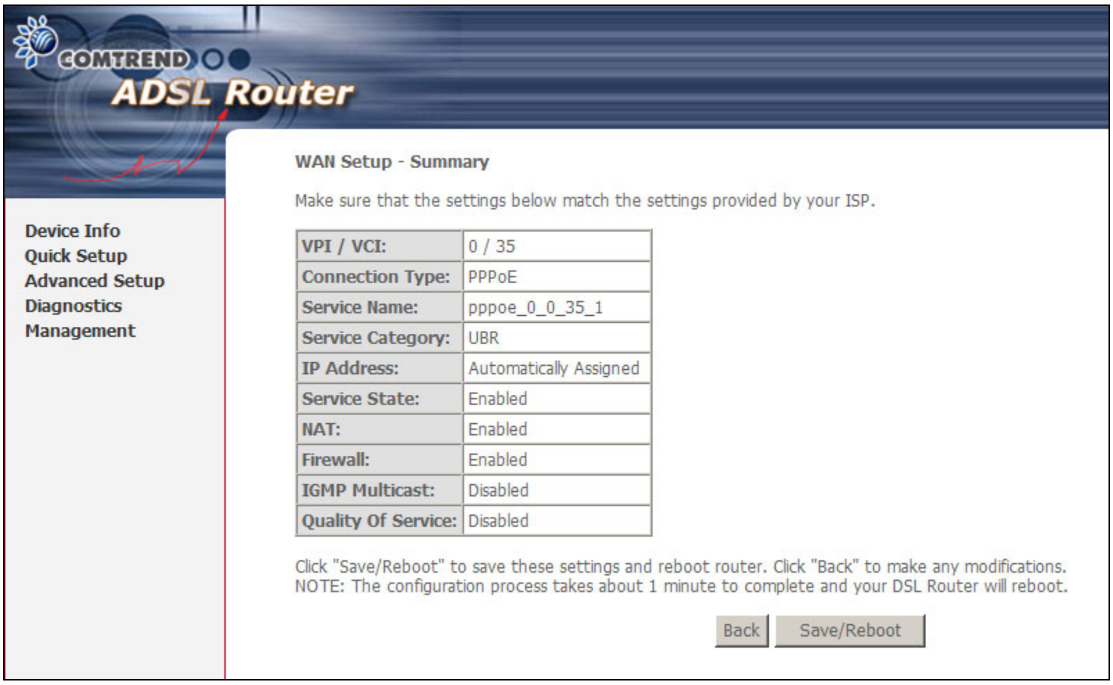
NOTE: **Enable DHCP Server Relay** will not display if NAT is enabled.

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 or click **Back** to modify these settings.



WAN Setup - Summary

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

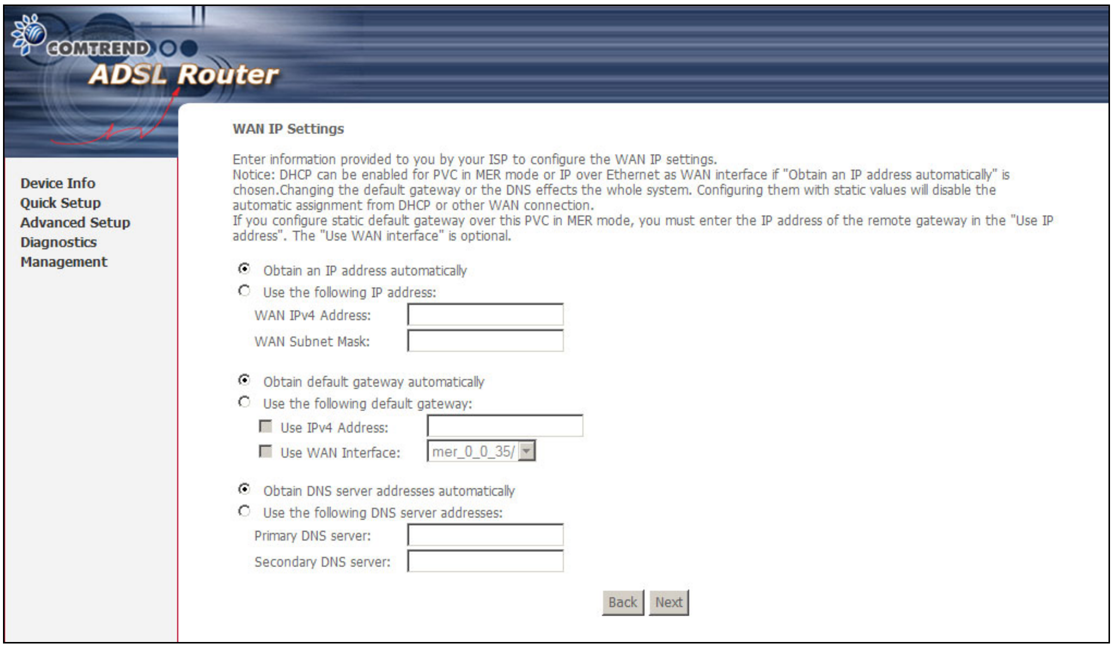
VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Save/Reboot**, the CT-5072T will save the configuration and reboot.

4.2.2 MAC Encapsulation Routing (MER)

STEP 4: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



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 IPv4 Address:
WAN Subnet Mask:

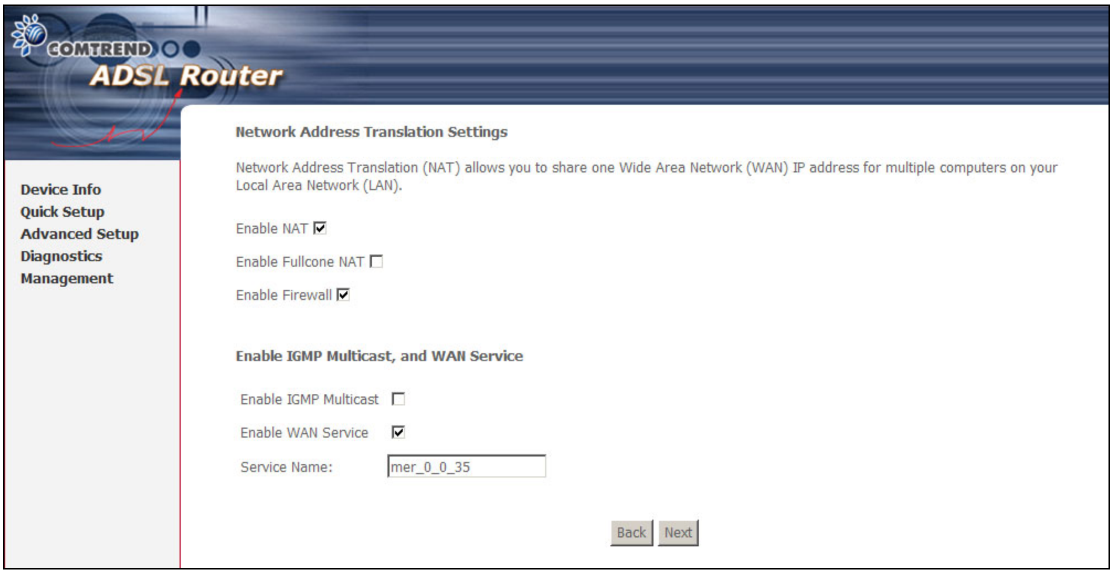
● Obtain default gateway automatically
○ Use the following default gateway:
□ Use IPv4 Address:
□ Use WAN Interface: mer_0_0_35/

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

Check the **Obtain an IP address automatically** checkbox ☑ to enable DHCP.

NOTE: Assigning the default gateway or DNS server with static values will disable their automatic assignment from DHCP or another WAN connection.

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



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 Fullcone NAT □

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: mer_0_0_35

ENABLE NAT

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

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL

To enable IP packet filtering, tick this checkbox ☑. The Advanced Setup → Security → IP Filtering option will appear on the main menu after reboot. Disable this function when not required for improved performance.

ENABLE IGMP MULTICAST

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

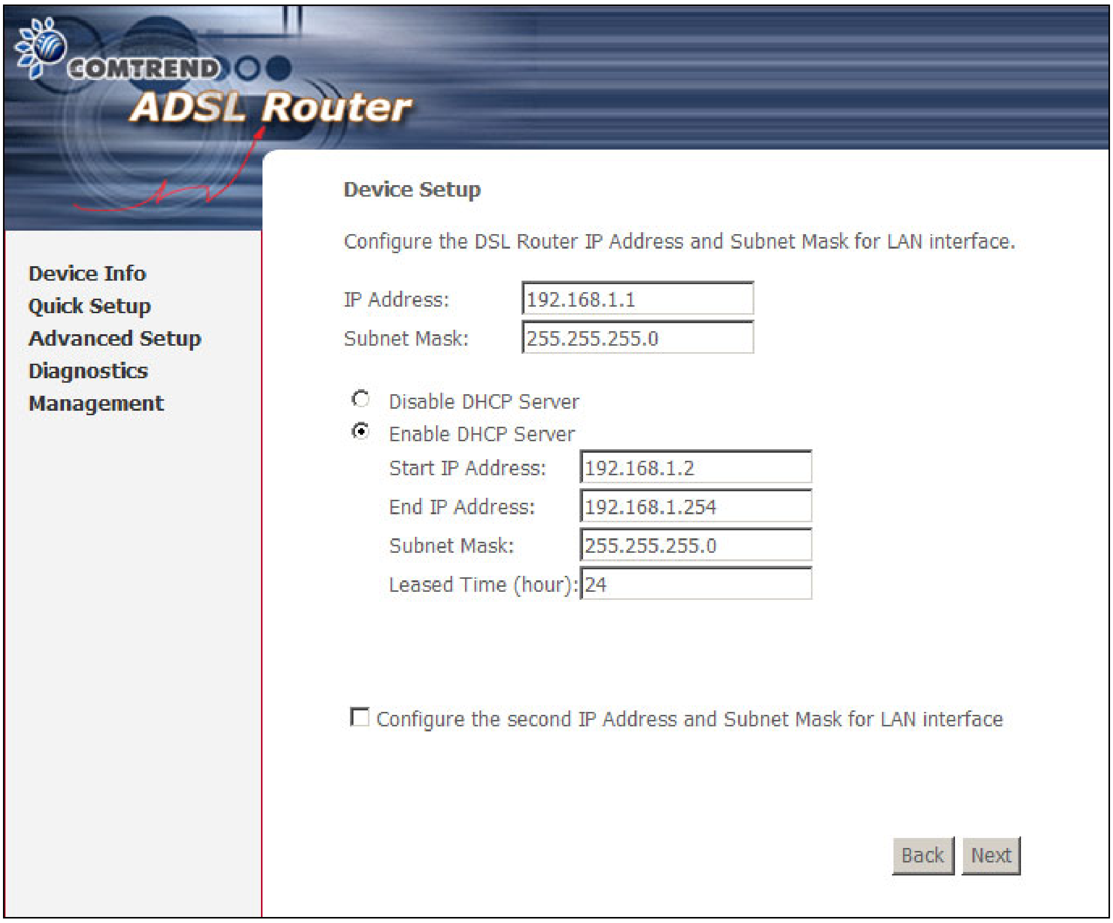
ENABLE WAN SERVICE

Tick the checkbox ☑ to enable WAN service.

SERVICE NAME

This is the WAN Service label.

STEP 6: The Device Setup screen is used to configure LAN interface settings.



Device Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0
Leased Time (hour): 24

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

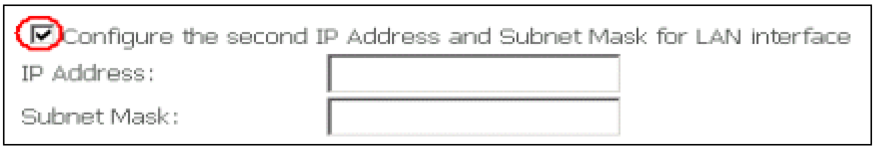
The IP address and Subnet Mask define the location of the CT-5072T on the LAN.

To auto-assign IP addresses, DNS server and default gateway to other LAN devices, select the **Enable DHCP server** radio button. You must also enter the start and end IP address, Subnet Mask and DHCP leased time.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the CT-5072T to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

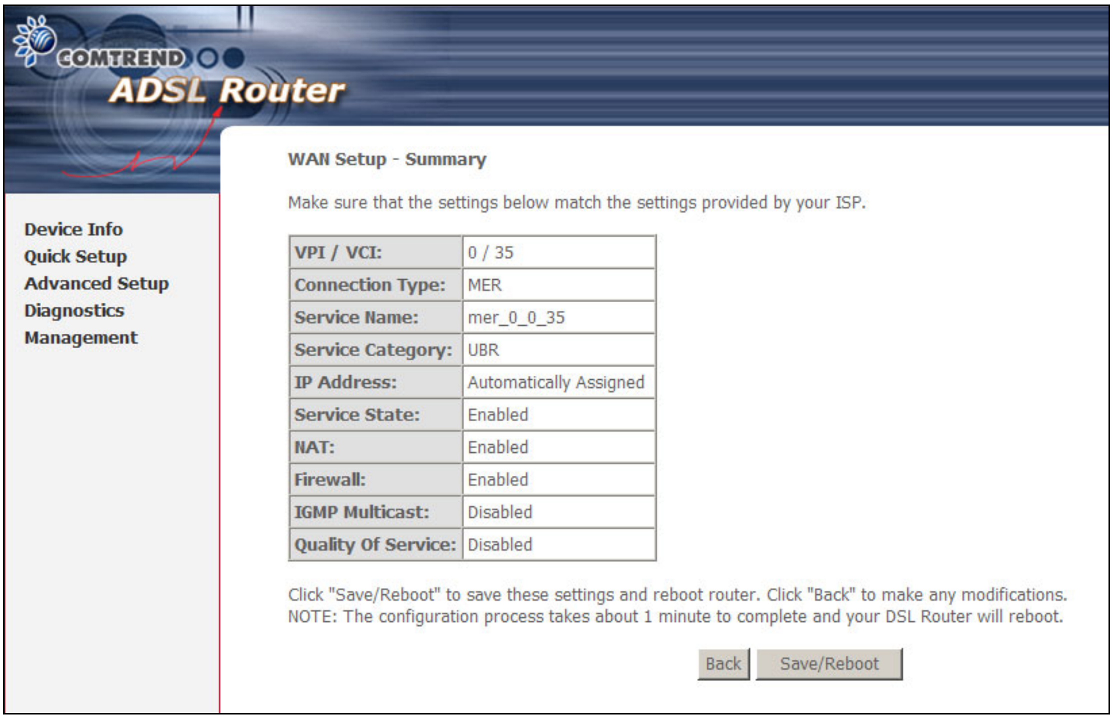
NOTE: **Enable DHCP Server Relay** will not display if NAT is enabled.

To configure a secondary IP address on the LAN, 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 or click **Back** to modify these settings.



WAN Setup - Summary

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

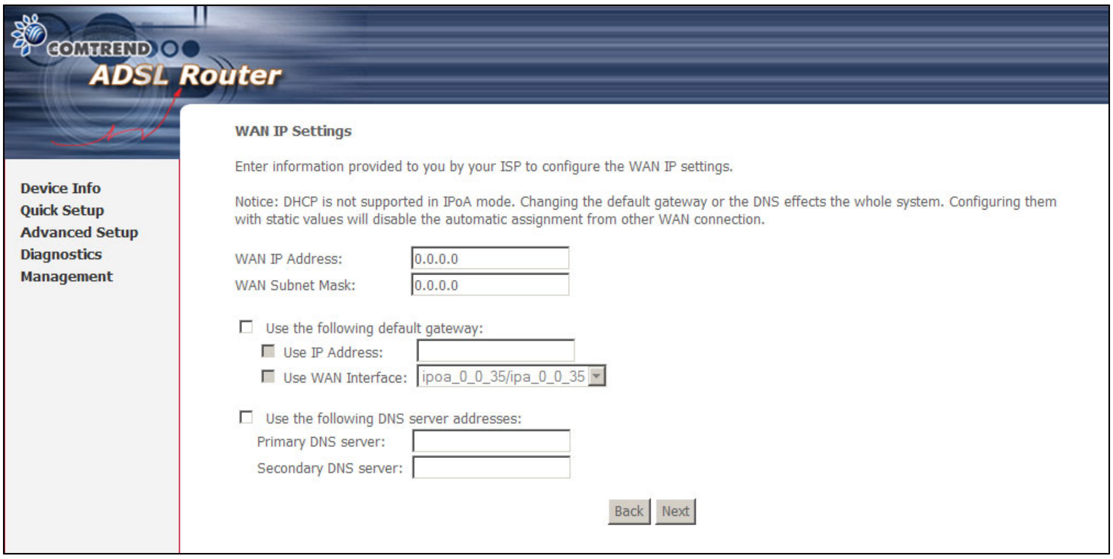
VPI / VCI:	0 / 35
Connection Type:	MER
Service Name:	mer_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Save/Reboot**, the CT-5072T will save the configuration and reboot.

4.2.3 IP Over ATM

STEP 4: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



WAN IP Settings

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

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

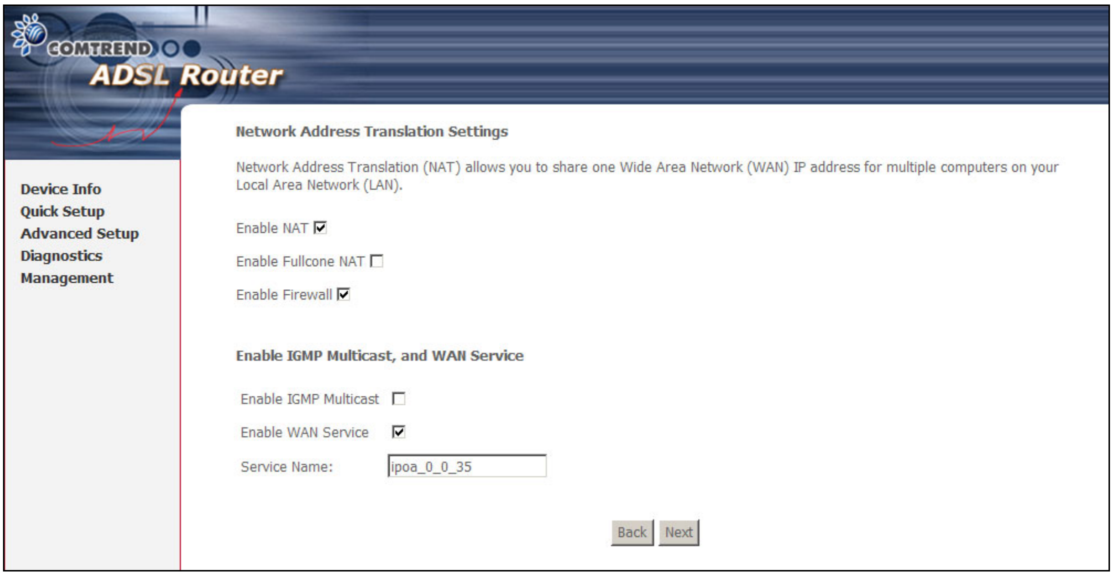
WAN IP Address: 0.0.0.0
WAN Subnet Mask: 0.0.0.0

□ Use the following default gateway:
□ Use IP Address:
□ Use WAN Interface: ipoa_0_0_35/ipa_0_0_35

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

NOTE: Since DHCP is not supported over IPoA connections, the default gateway settings and DNS server addresses must be assigned manually.

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



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 Fullcone NAT □

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: ipoa_0_0_35

ENABLE NAT

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

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host by sending a packet to the mapped external address.

ENABLE FIREWALL

To enable IP packet filtering, tick this checkbox ☑. The Advanced Setup → Security → IP Filtering option will appear on the main menu after reboot. Disable this function when not required for improved performance.

ENABLE IGMP MULTICAST

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

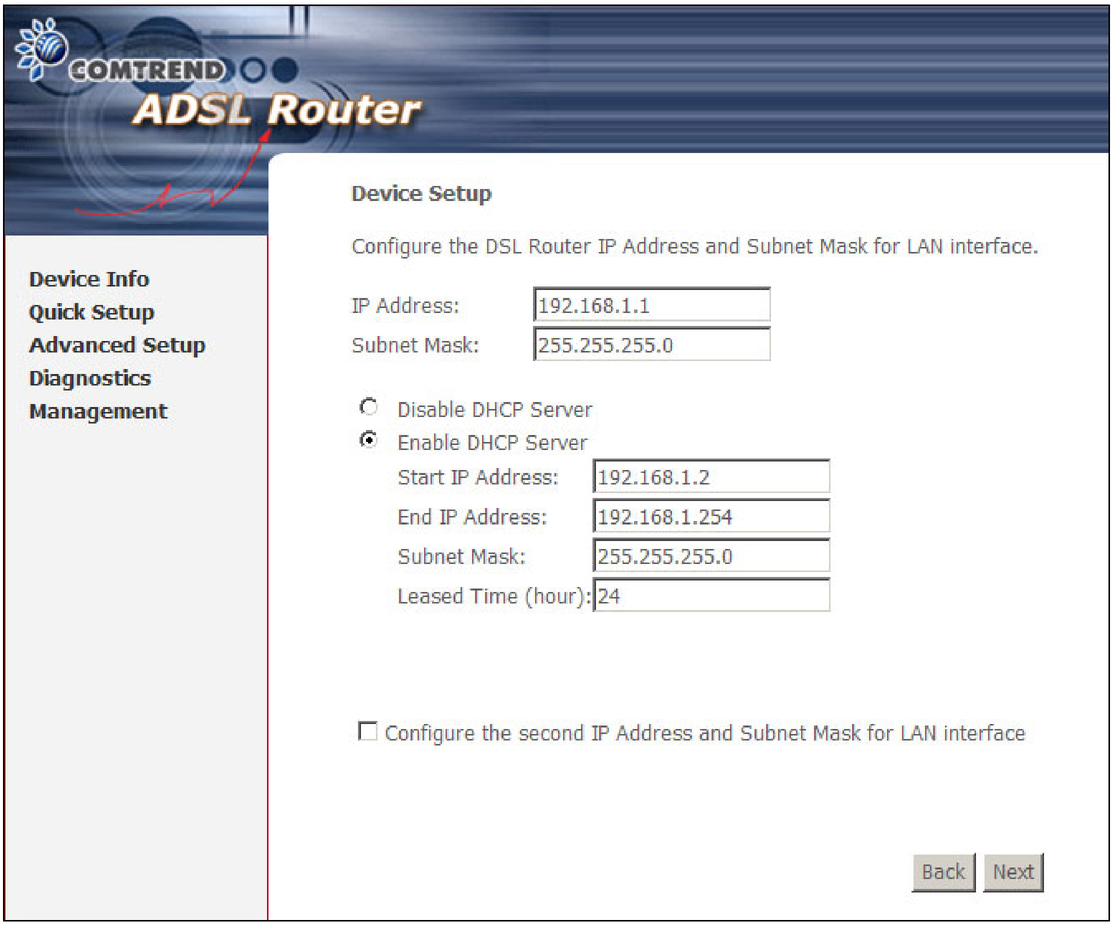
ENABLE WAN SERVICE

Tick the checkbox ☑ to enable WAN service.

SERVICE NAME

This is the WAN Service label.

STEP 6: The Device Setup screen is used to configure LAN interface settings.



Device Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Leased Time (hour): 24

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

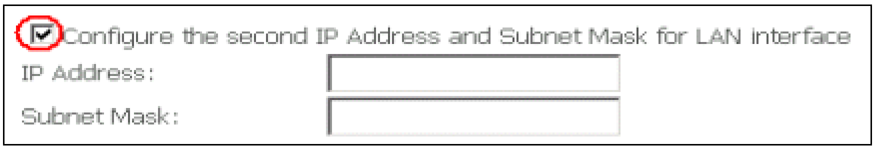
The IP address and Subnet Mask define the location of the CT-5072T on the LAN.

To auto-assign IP addresses, DNS server and default gateway to LAN devices, select the **Enable DHCP server** radio button. You must also enter the start and end IP address, Subnet Mask and DHCP leased time.

Select **Enable DHCP Server Relay** (if required), and enter the DHCP Server IP Address. This allows the CT-5072T 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.

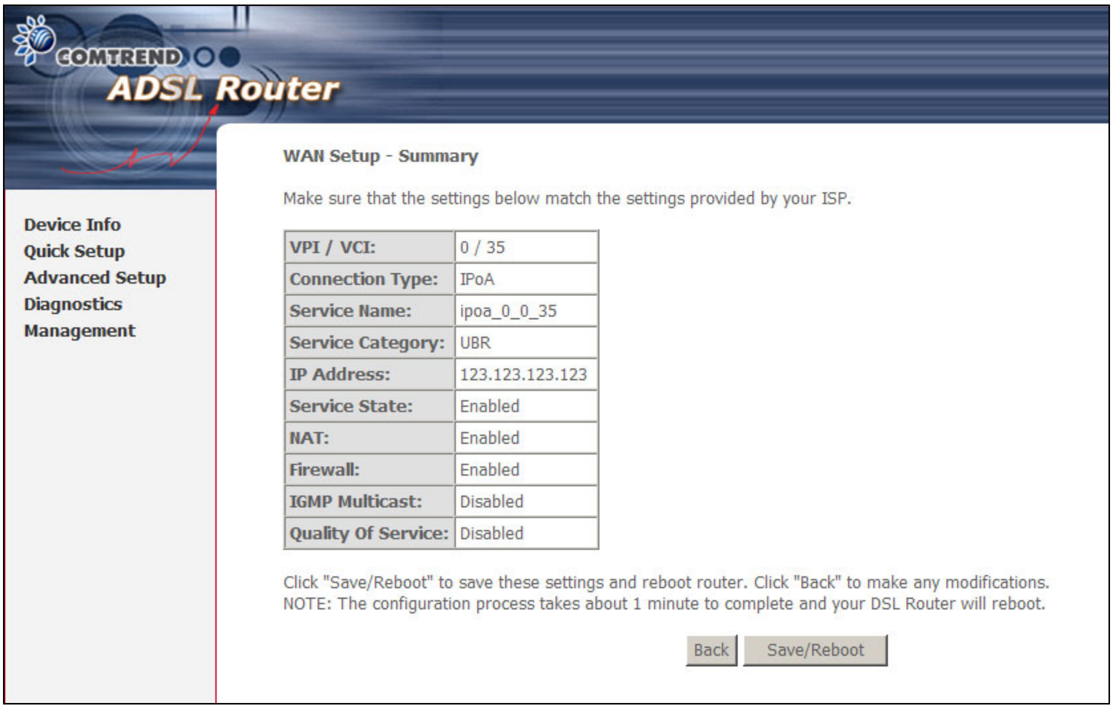


☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

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



WAN Setup - Summary

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

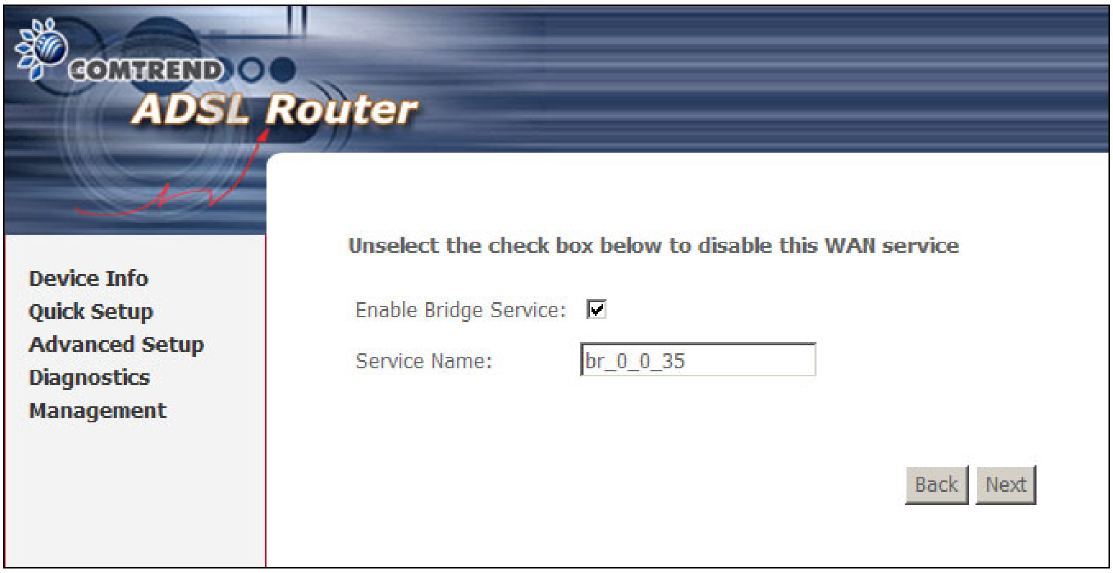
VPI / VCI:	0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	123.123.123.123
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Save/Reboot**, the CT-5072T will save the configuration and reboot.

4.2.4 Bridging

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



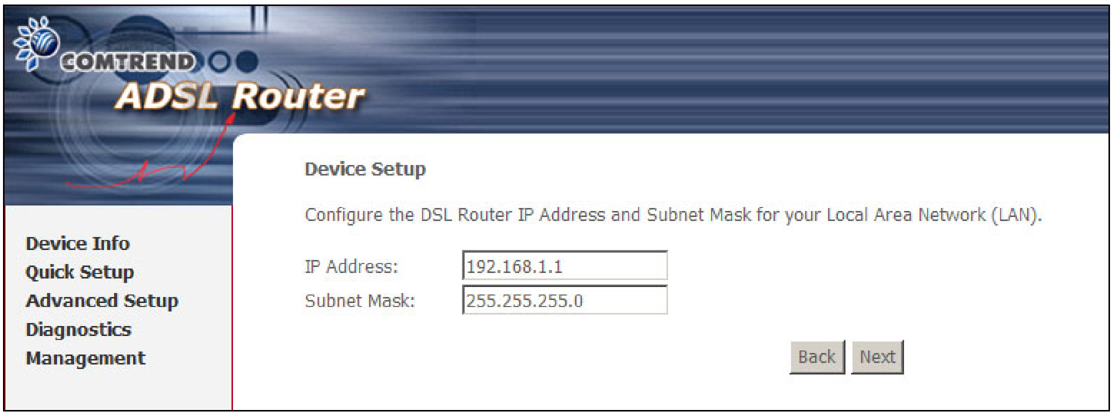
Unselect the check box below to disable this WAN service

Enable Bridge Service: ☑

Service Name: br_0_0_35

Click **Next** to continue.

STEP 5: The Device Setup screen is used to configure LAN interface settings.



Device Setup

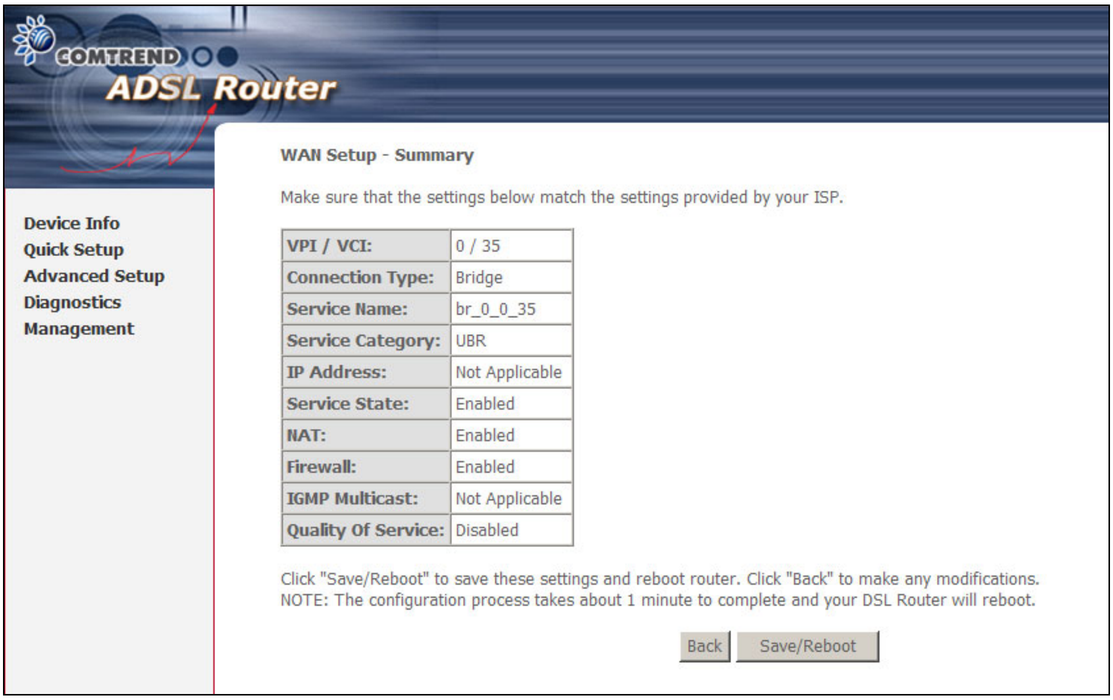
Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN).

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Enter an IP Address and Subnet Mask for the CT-5072T LAN interface.

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



WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
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 and reboot.

NOTES: To access the web user interface (WUI) after reboot, your PC IP settings will need to be assigned using the STATIC IP method (see section 3.2), since the on-board DHCP server is not active in bridge mode.

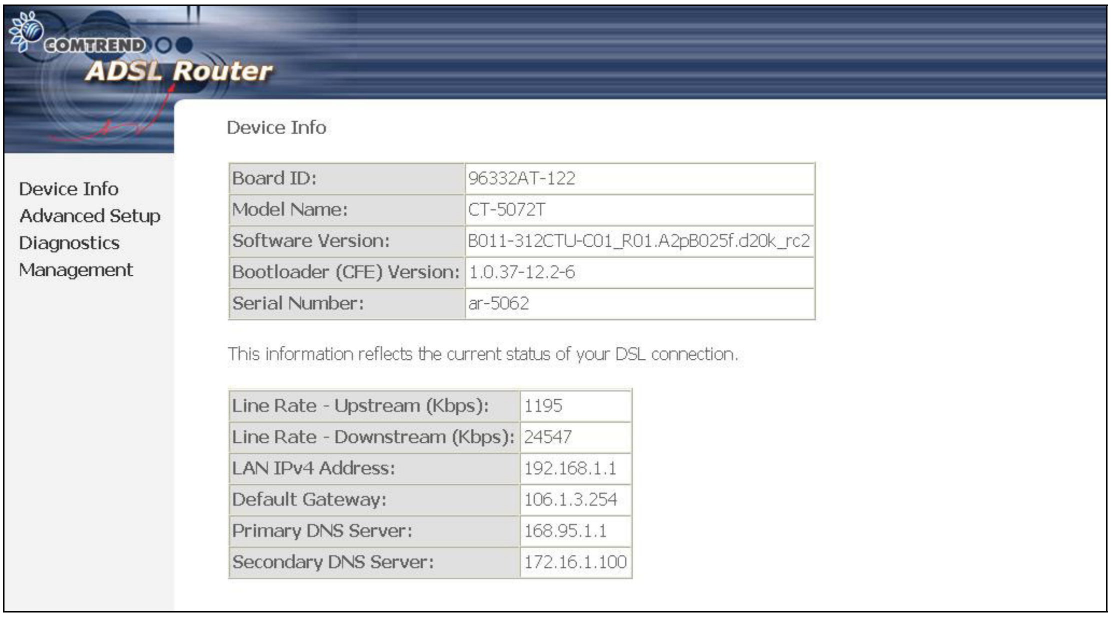
Similarly, the CT-5072T cannot be accessed from the WAN, for remote management or technical support, since no WAN IP address is available.

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(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

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



Device Info

Board ID:	96332AT-122
Model Name:	CT-5072T
Software Version:	B011-312CTU-C01_R01.A2pB025f.d20k_rc2
Bootloader (CFE) Version:	1.0.37-12.2-6
Serial Number:	ar-5062

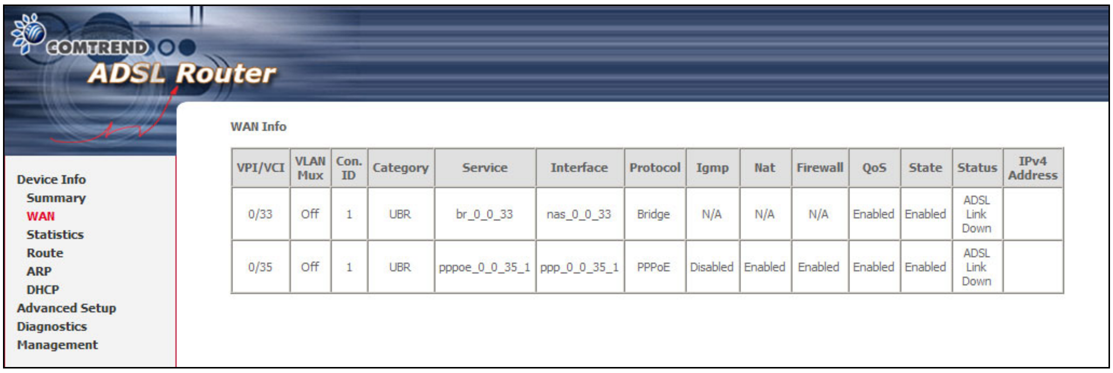
This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	1195
Line Rate - Downstream (Kbps):	24547
LAN IPv4 Address:	192.168.1.1
Default Gateway:	106.1.3.254
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	172.16.1.100

The Device Info Summary screen will display at startup, if a PVC connection exists. This screen shows hardware, software, IP settings and other important information.

5.1 WAN

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



WAN Info

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	Firewall	QoS	State	Status	IPv4 Address
0/33	Off	1	UBR	br_0_0_33	nas_0_0_33	Bridge	N/A	N/A	N/A	Enabled	Enabled	ADSL Link Down	
0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	Enabled	Enabled	ADSL Link Down	

Heading	Description
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
IGMP	Shows Internet Group Management Protocol (IGMP) status
Nat	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
QoS	Shows Quality of Service (QoS) status
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address

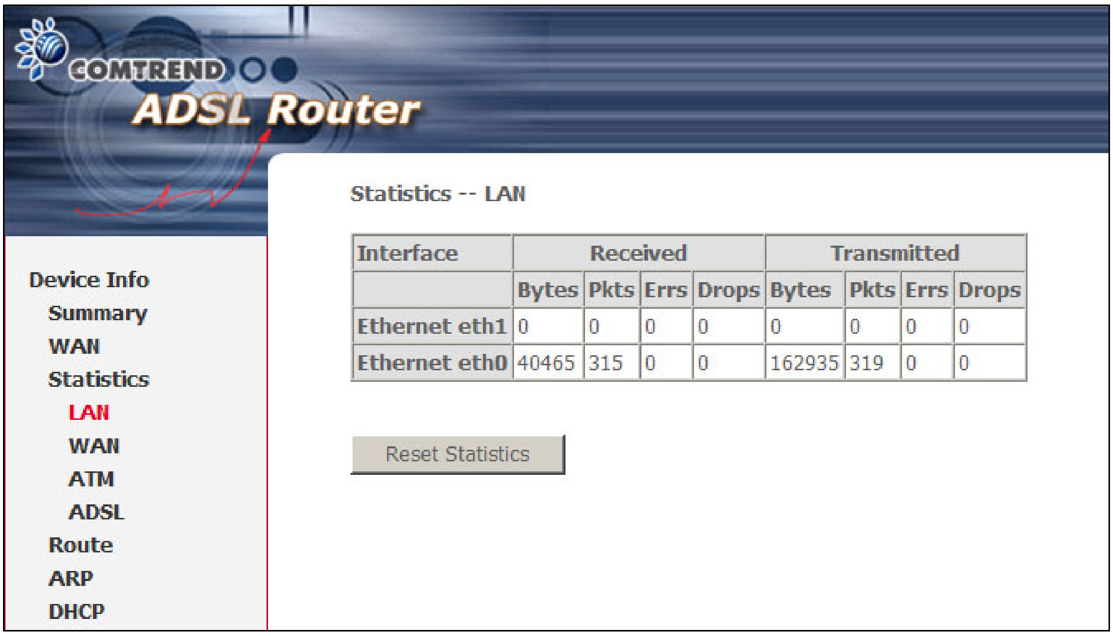
5.2 Statistics

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

NOTE: These screens are updated every 15 seconds.

5.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



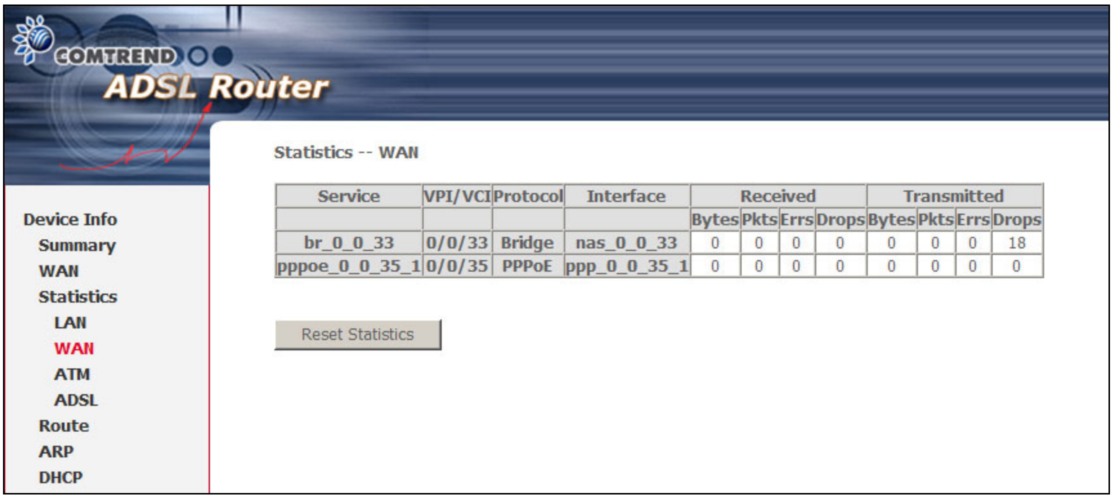
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth1	0	0	0	0	0	0	0	0
Ethernet eth0	40465	315	0	0	162935	319	0	0

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

5.2.2 WAN Statistics

This screen shows data traffic statistics for each WAN interface.



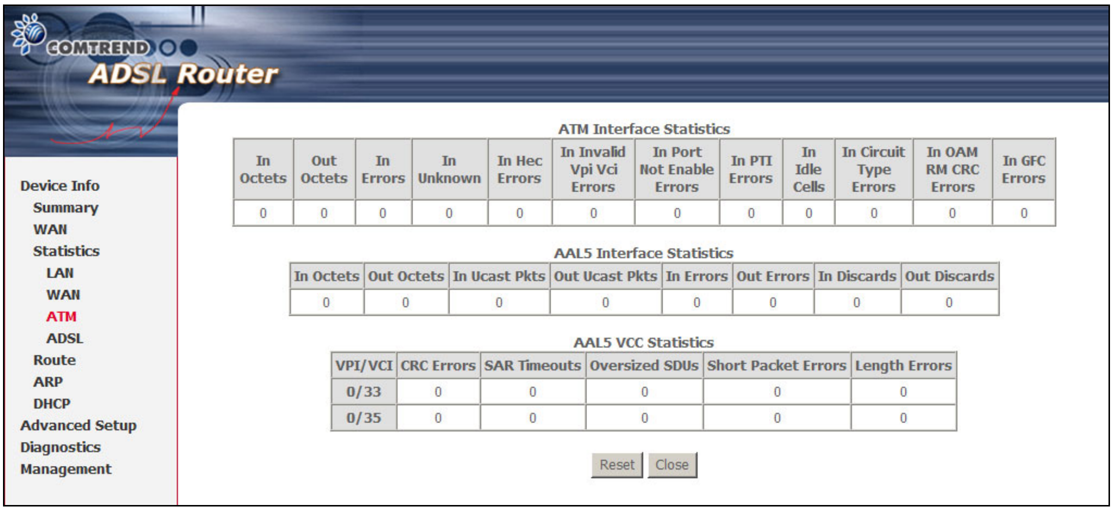
Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
br_0_0_33	0/0/33	Bridge	nas_0_0_33	0	0	0	0	0	0	0	18
pppoe_0_0_35_1	0/0/35	PPPoE	ppp_0_0_35_1	0	0	0	0	0	0	0	0

Heading		Description
Service		WAN service label
VPI/VCI		ATM Virtual Path/Channel Identifiers
Protocol		Connection type (e.g. PPPoE, IPoA, Bridge)
Interface		WAN interfaces
Received/Transmitted	- Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.2.3 ATM statistics

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



ATM Interface Statistics

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

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/33	0	0	0	0	0
0/35	0	0	0	0	0

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

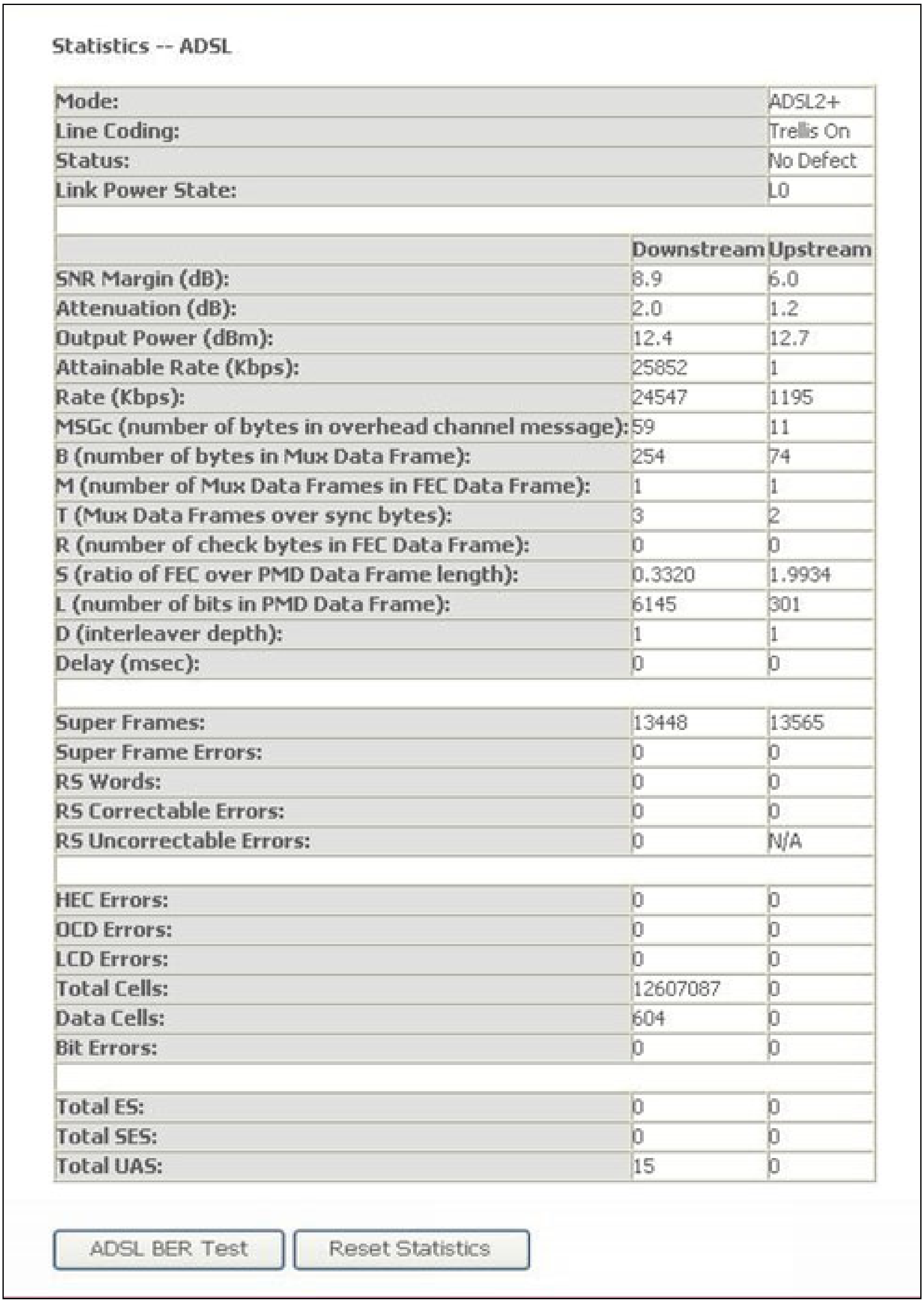
Heading	Description
In Errors	Number of received AAL5/AAL0 CPCS PDUs received that contain an error. These errors include CRC-32 errors.
Out Errors	Number of received AAL5/AAL0 CPCS PDUs that could not be transmitted due to errors.
In Discards	Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
Out Discards	This field is not currently used

AAL5 VCC Statistics

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

5.2.4 ADSL Statistics

The ADSL Statistics screen is shown below with a reference table that follows.



Statistics -- ADSL

Mode:		ADSL2+
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	8.9	6.0
Attenuation (dB):	2.0	1.2
Output Power (dBm):	12.4	12.7
Attainable Rate (Kbps):	25852	1
Rate (Kbps):	24547	1195
MSGc (number of bytes in overhead channel message):	59	11
B (number of bytes in Mux Data Frame):	254	74
M (number of Mux Data Frames in FEC Data Frame):	1	1
T (Mux Data Frames over sync bytes):	3	2
R (number of check bytes in FEC Data Frame):	0	0
S (ratio of FEC over PMD Data Frame length):	0.3320	1.9934
L (number of bits in PMD Data Frame):	6145	301
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	13448	13565
Super Frame Errors:	0	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	12607087	0
Data Cells:	604	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	15	0

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.

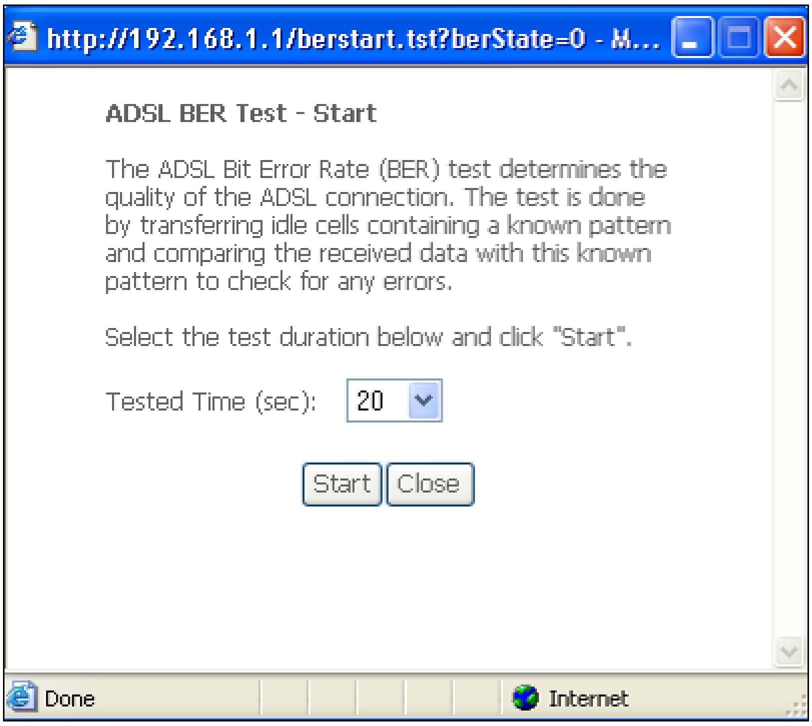
MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver 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**.



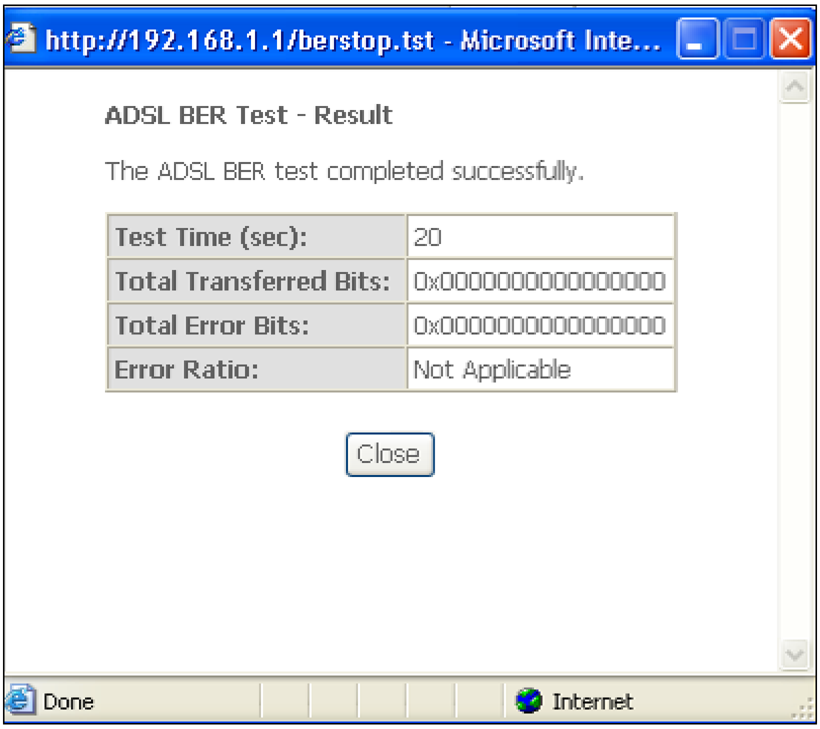
ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

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



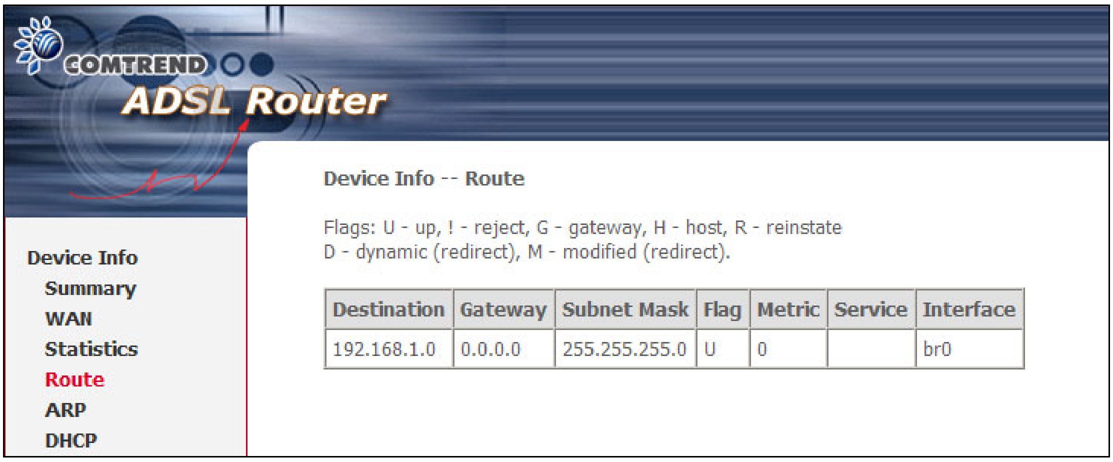
ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000000000000
Total Error Bits:	0x0000000000000000
Error Ratio:	Not Applicable

5.3 Route

Choose **Route** to display the routes that the CT-5072T has found.



Device Info -- Route

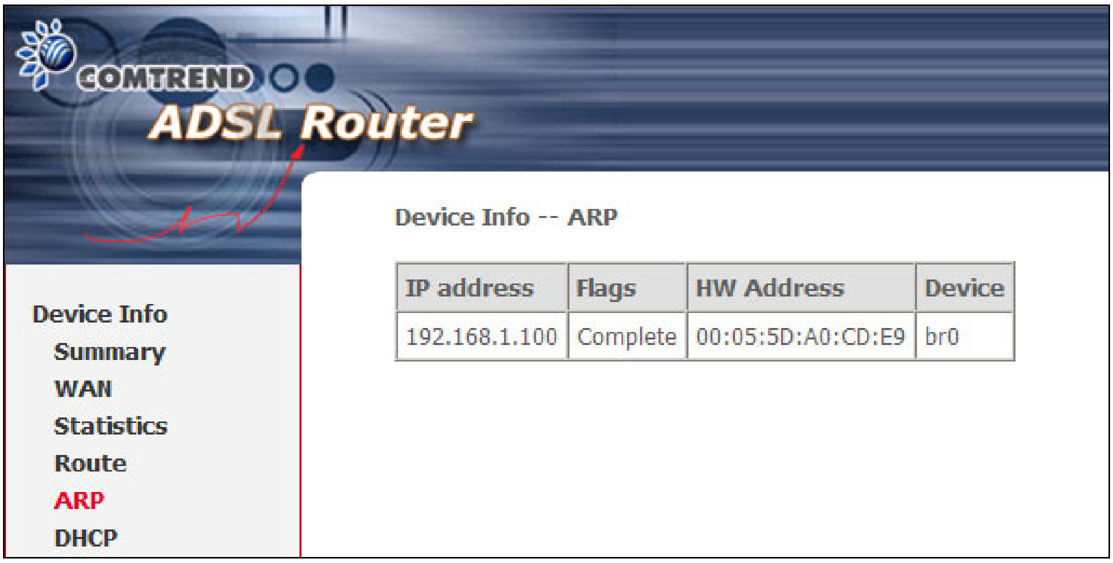
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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

5.4 ARP

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



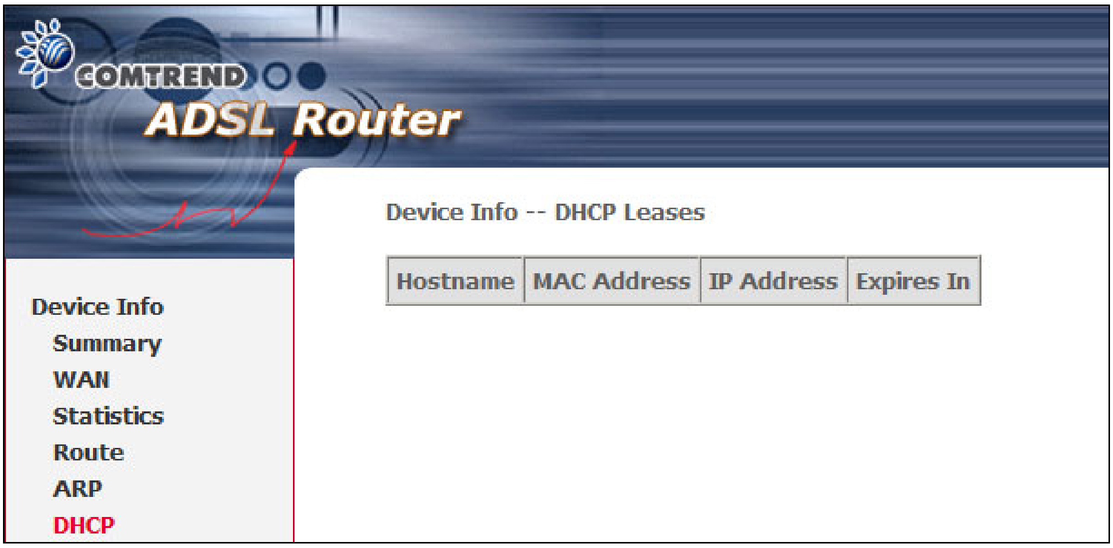
Device Info -- ARP

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.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

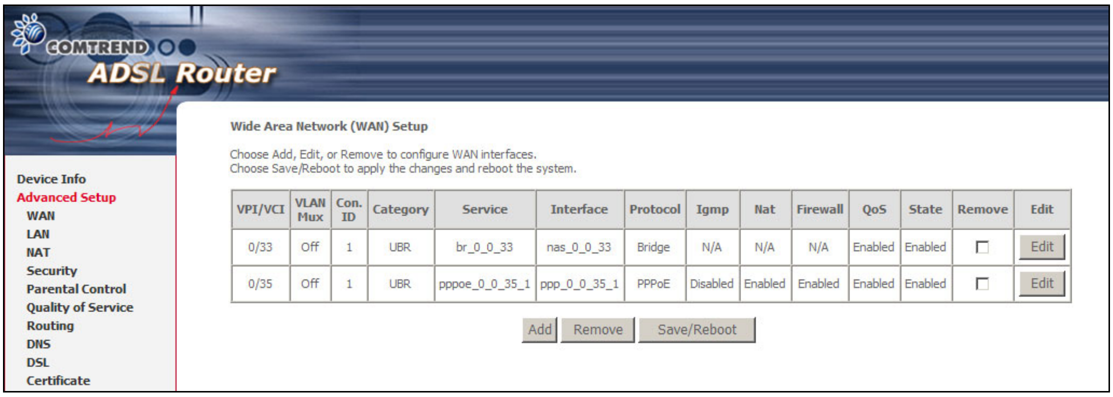
Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

Chapter 6 Advanced Setup

This chapter explains the following screens:

6.1 WAN

This screen allows for the configuration of WAN interfaces.



Wide Area Network (WAN) Setup

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

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	Firewall	QoS	State	Remove	Edit
0/33	Off	1	UBR	br_0_0_33	nas_0_0_33	Bridge	N/A	N/A	N/A	Enabled	Enabled	□	Edit
0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	Enabled	Enabled	□	Edit

To **Add** a new WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection. To complete the **Add** or **Edit** go to **STEP 2** in section 4.2.

NOTE: Up to 8 PVC profiles can be configured and saved in flash memory.

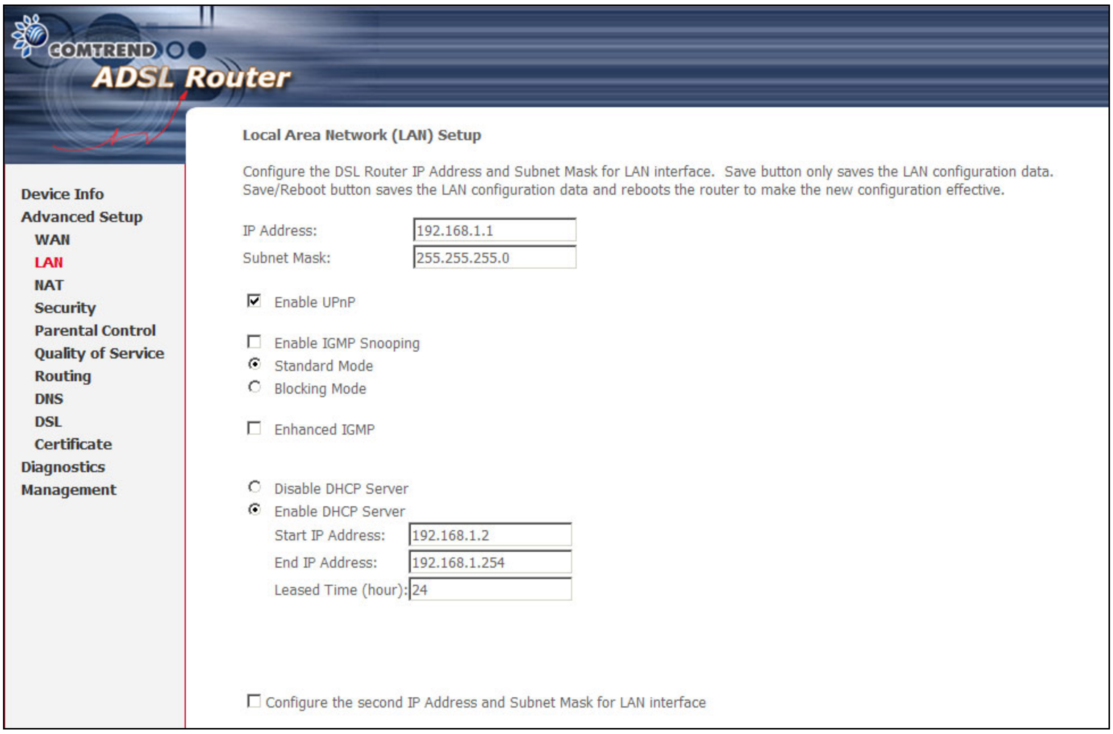
To remove a connection select its radio button under the **Remove** column in the table and click the **Remove** button under the table.

Heading	Description
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
VLAN Mux	Shows 802.1Q VLAN ID
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection

Heading	Description
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
Firewall	Shows the status of Firewall
QoS	Shows Quality of Service (QoS) status
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.



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

☑ Enable UPnP

☐ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

☐ Enhanced IGMP

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

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

NOTE: NAT is enabled so the **Enable UPnP** checkbox ☑ is shown above while the **DHCP Server Relay** option is hidden (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: Enable by ticking the checkbox ☑.

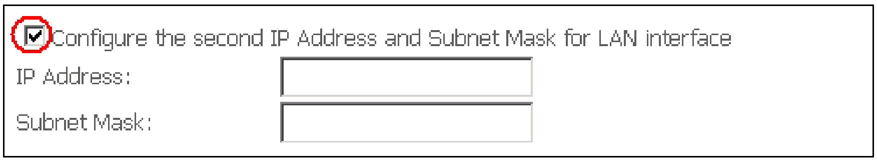
Standard Mode**:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

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

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter 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 or when the router is configured with only one Bridge PVC*.

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.

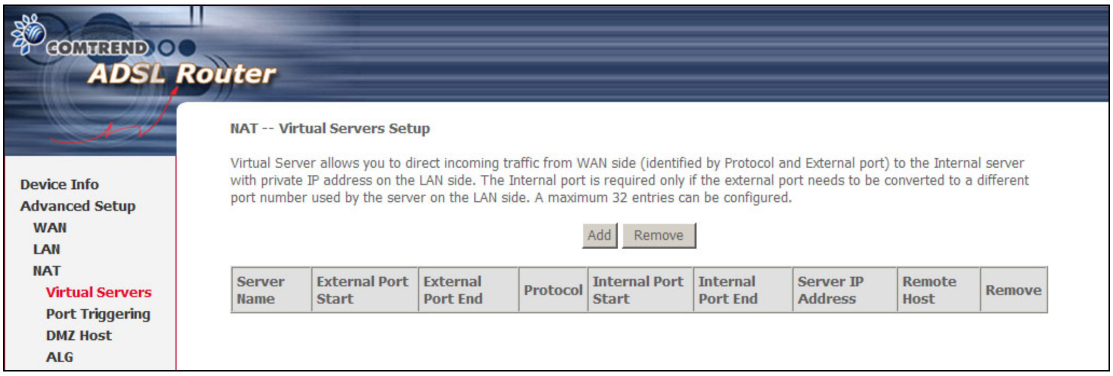
NOTE: The **Save** button simply saves changes, while the **Save/Reboot** button both saves and reboots the device to make any changes effective.

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.

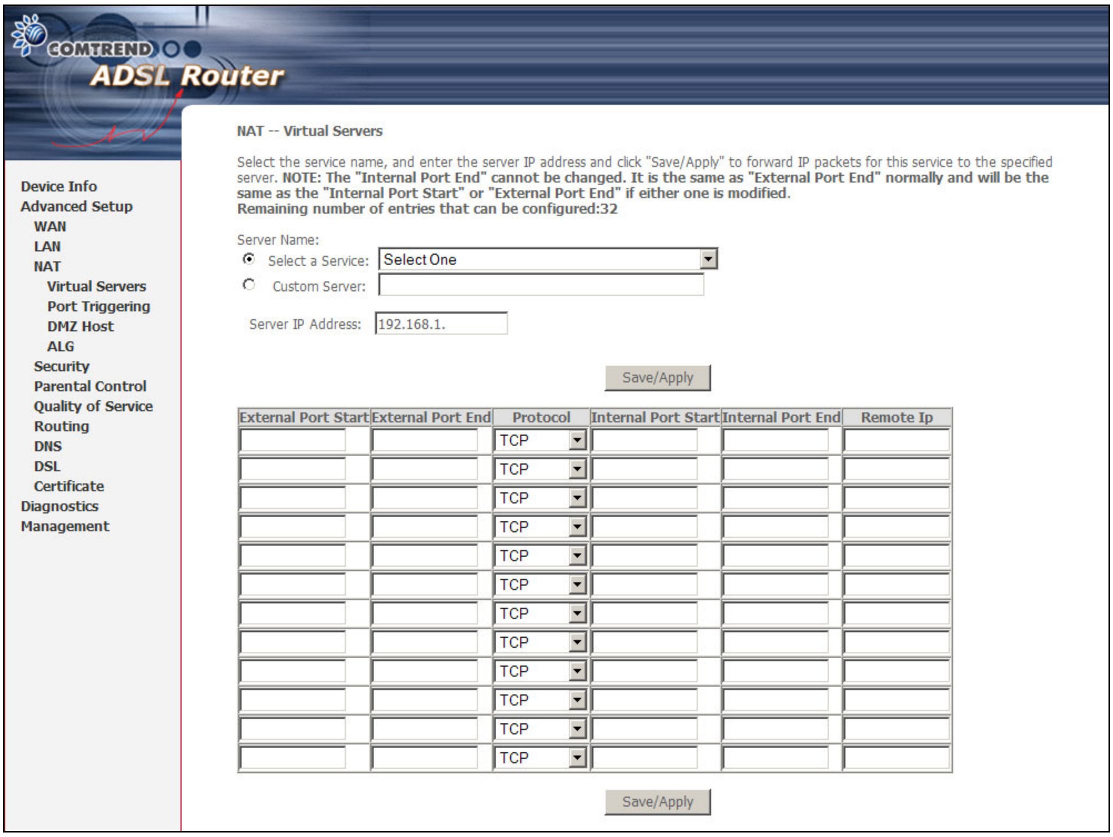


NAT -- Virtual Servers Setup

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	Remote Host	Remove

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



NAT -- Virtual Servers

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

Server Name:
● Select a Service: Select One
○ Custom Server:

Server IP Address: 192.168.1.

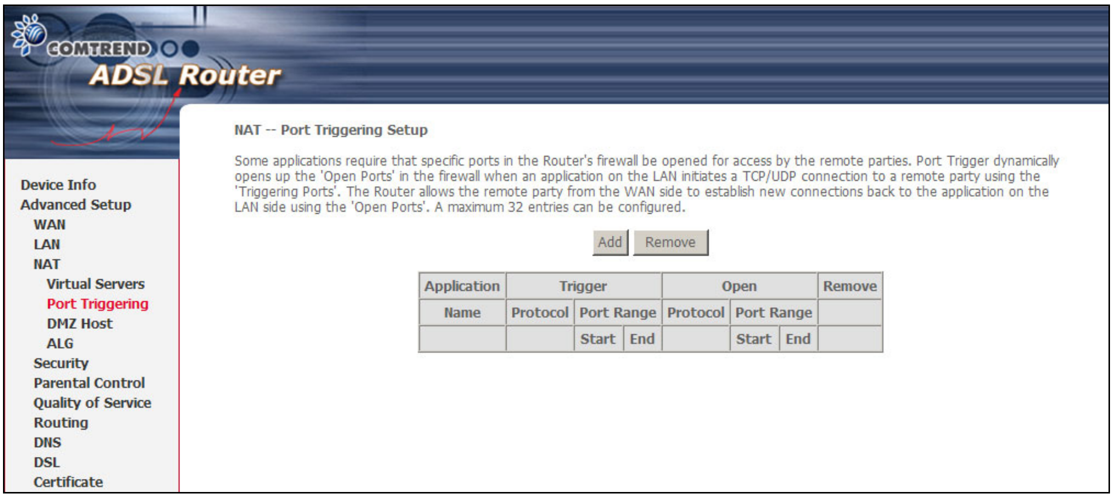
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Consult the table below for field and header descriptions.

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

6.3.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port 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.

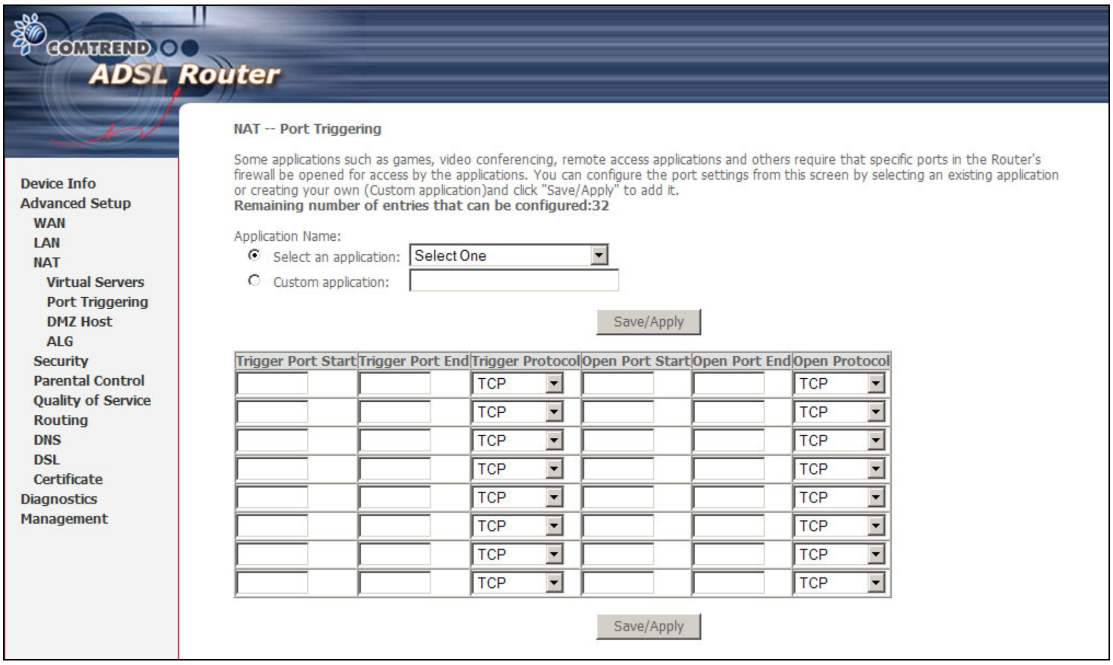


NAT -- Port Triggering Setup

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

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

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



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:32

Application Name:
● Select an application: Select One
○ Custom application:

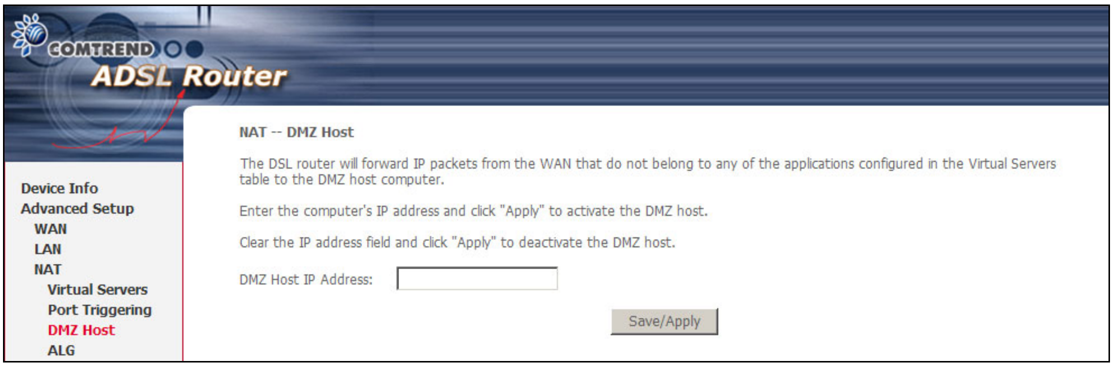
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Consult the table below for field and header descriptions.

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

6.3.3 DMZ Host

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



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:

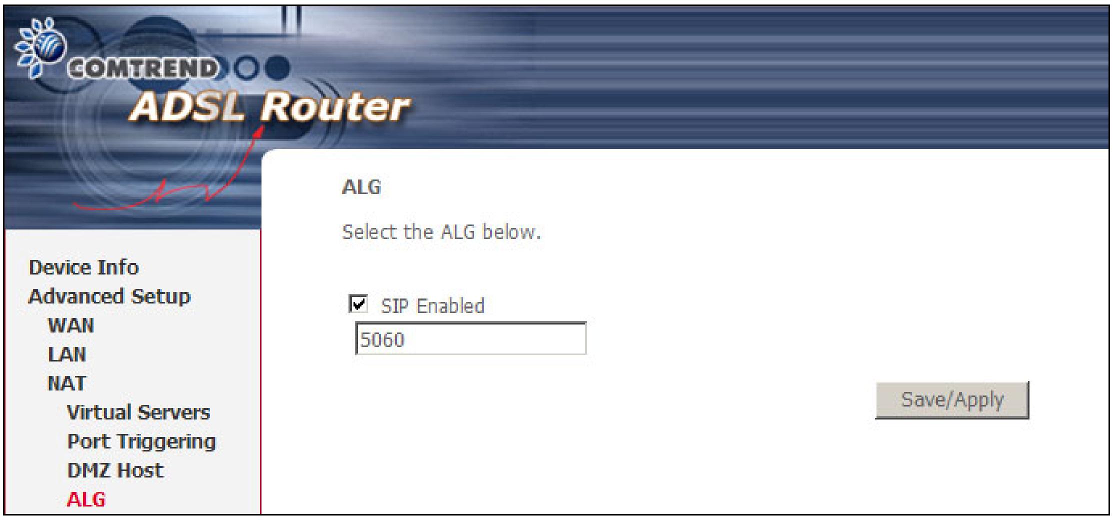
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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**.



ALG

Select the ALG below.

☑ SIP Enabled

5060

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.

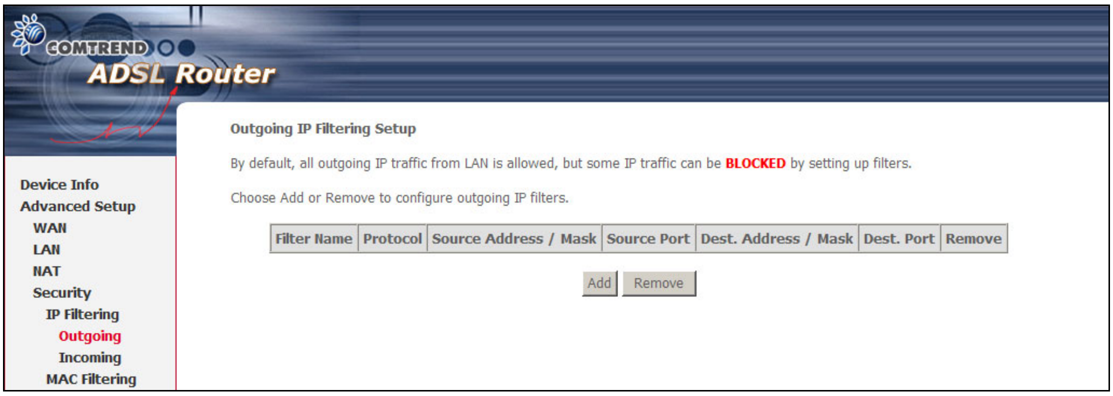
6.4.1 IP Filtering

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. 44) performs a similar function.

OUTGOING IP FILTER

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



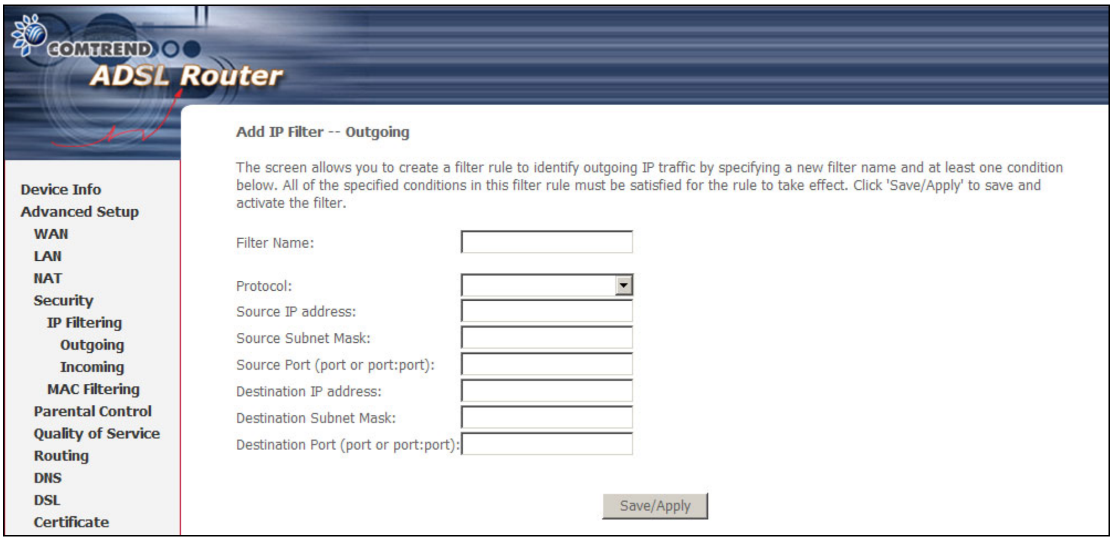
Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

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

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



Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

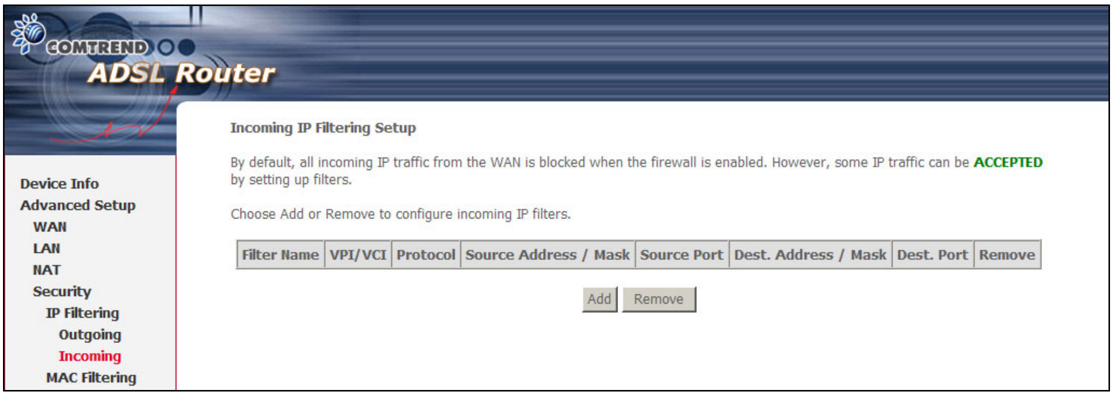
Destination Port (port or port:port):

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.



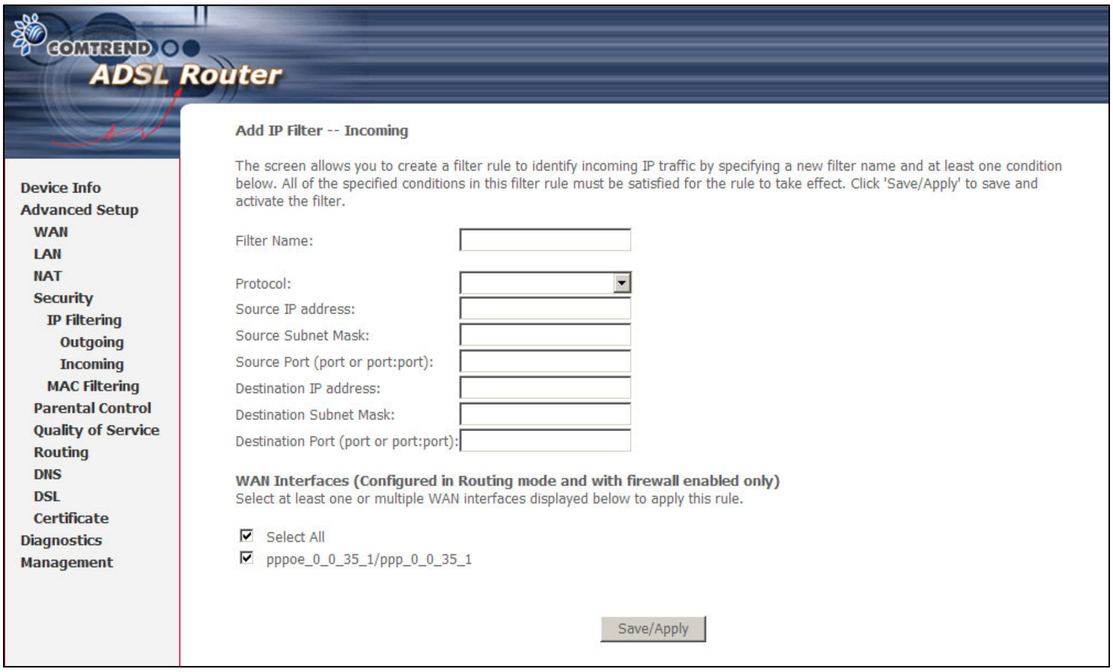
Incoming IP Filtering Setup

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

Choose Add or Remove to configure incoming IP filters.

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

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



Add IP Filter -- Incoming

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

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

☑ Select All
☑ pppoe_0_0_35_1/ppp_0_0_35_1

For detailed field descriptions, please reference the previous table.

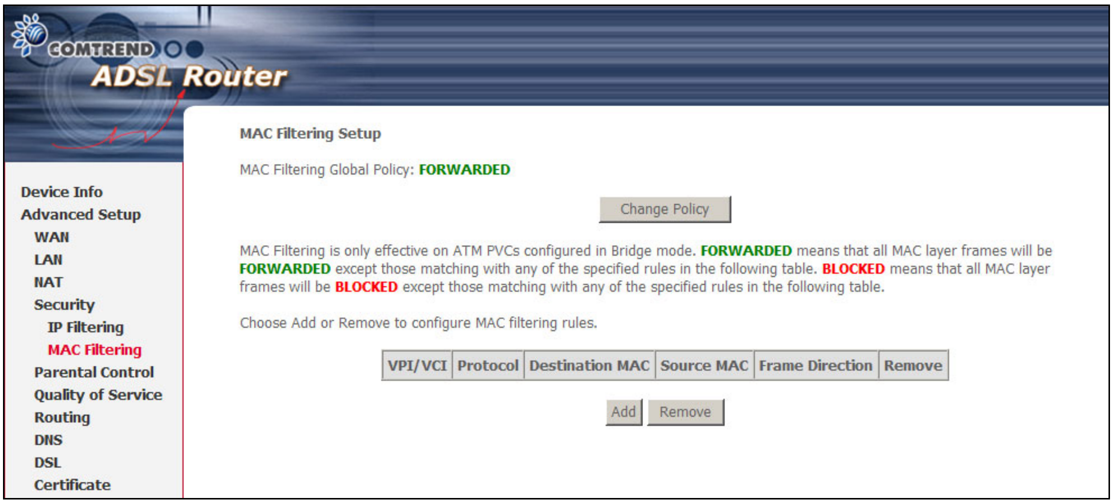
Under **WAN Interfaces**, select the PVCs (All routing modes with firewall ON) where the filter rule will apply. You may select all PVCs or just a subset. Filter rules are arranged by PVC as shown under the VPI/VCI heading on the previous screen.

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. 42) 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-5072T 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.



MAC Filtering Setup

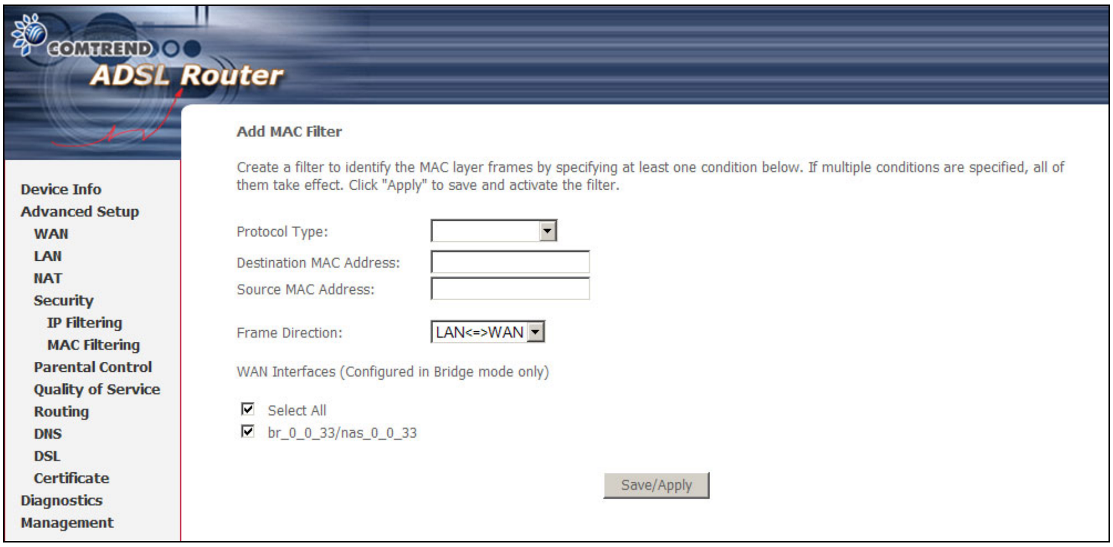
MAC Filtering Global Policy: FORWARDED

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

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

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.



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: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

☑ Select All

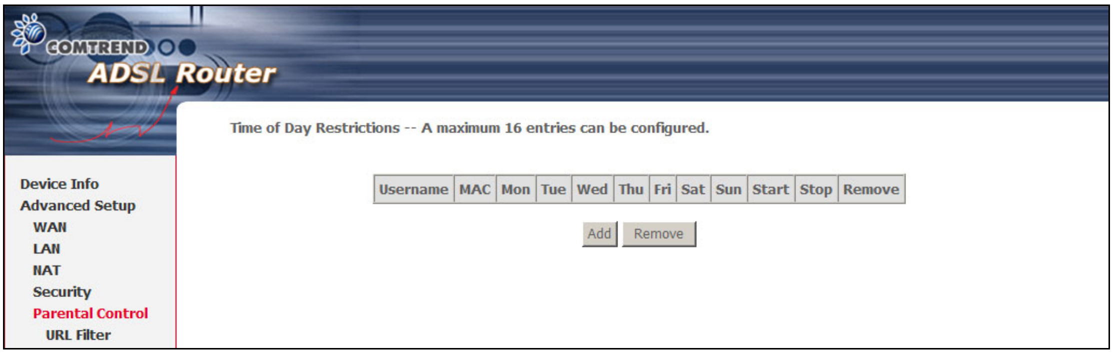
☑ br_0_0_33/nas_0_0_33

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.

6.5 Parental Control

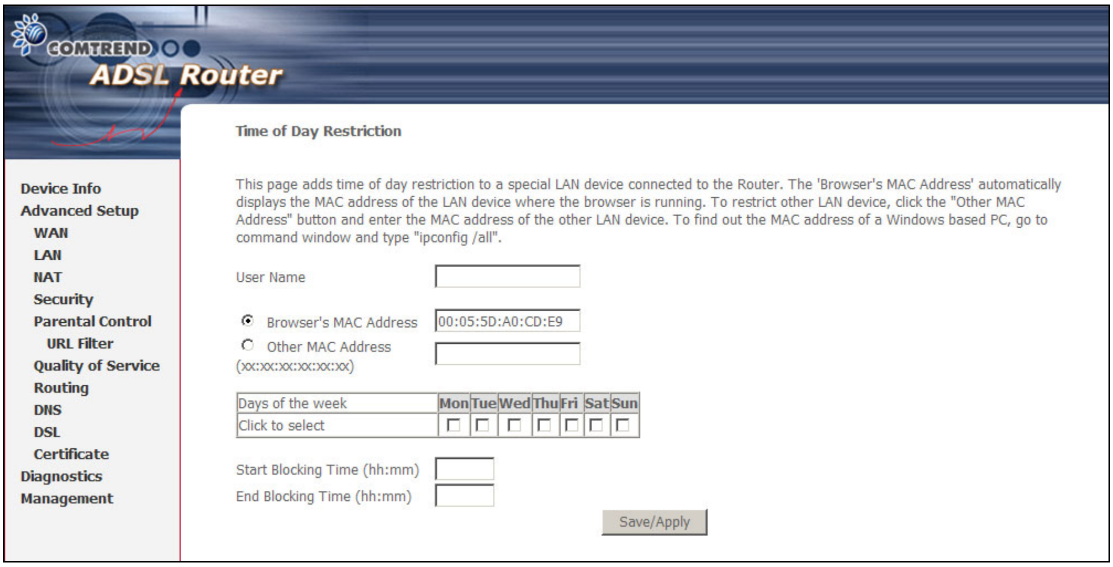
This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.5, so that the scheduled times match your local time.



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

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

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



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
(xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

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.

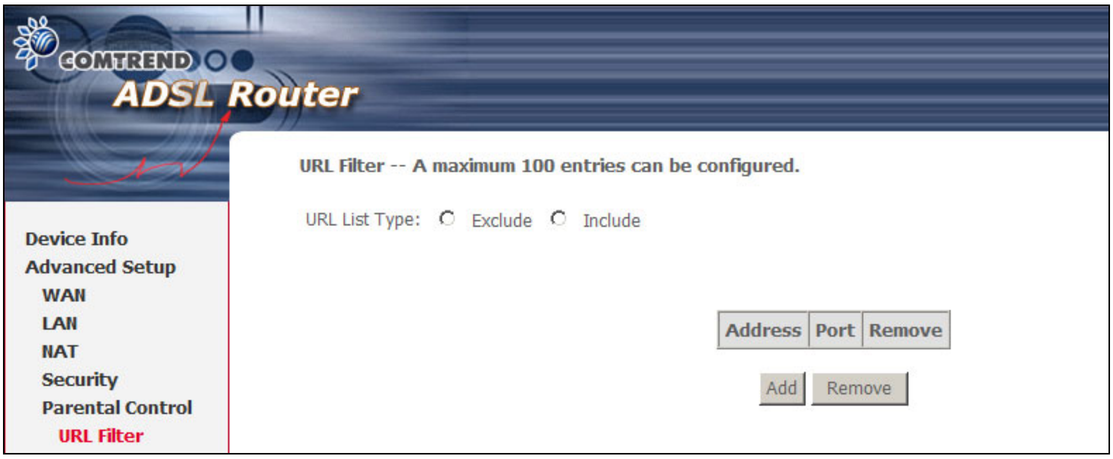
Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

End Blocking Time: The time the restrictions end.

6.5.1 URL Filter

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

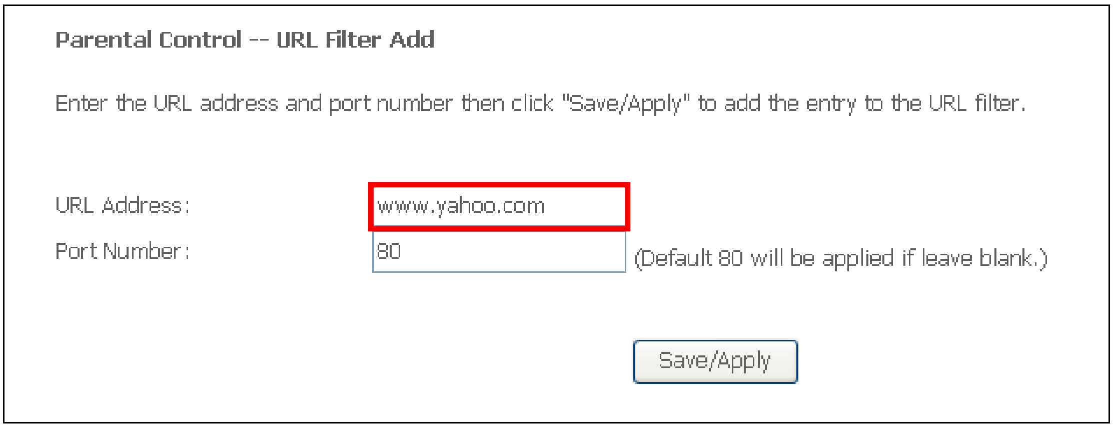


URL Filter -- A maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove

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



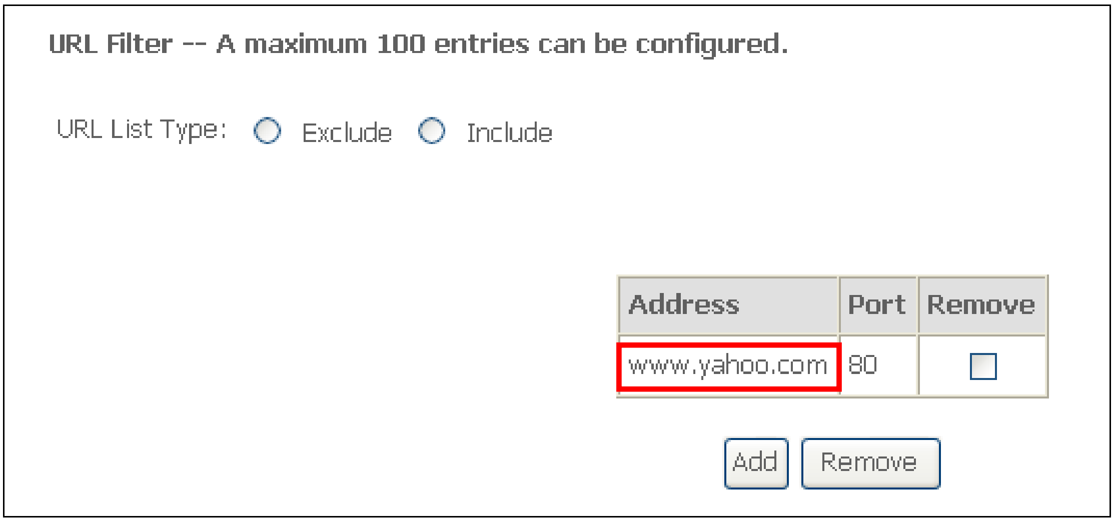
Parental Control -- URL Filter Add

Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.

URL Address: www.yahoo.com

Port Number: 80 (Default 80 will be applied if leave blank.)

Enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter.   URL Addresses begin with "www", as shown in this example.



URL Filter -- A maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove
www.yahoo.com	80	□

A maximum of 100 entries can be added to the URL Filter list.
Tick the **Exclude** radio button to deny access to the websites listed.
Tick the **Include** radio button to restrict access to only those listed websites.

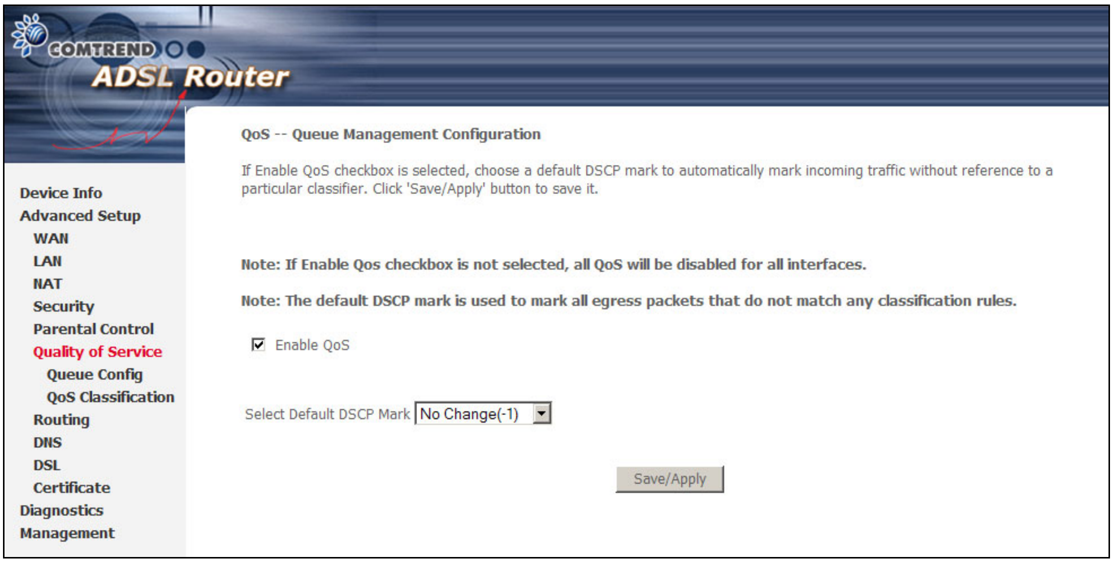
6.6 Quality of Service

NOTE: QoS must be enabled in at least one PVC to display this option.
(see Manual Quick Setup for detailed PVC setup instructions).

6.6.1 Queue Management Configuration

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

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



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

Select Default DSCP Mark No Change(-1)

Save/Apply

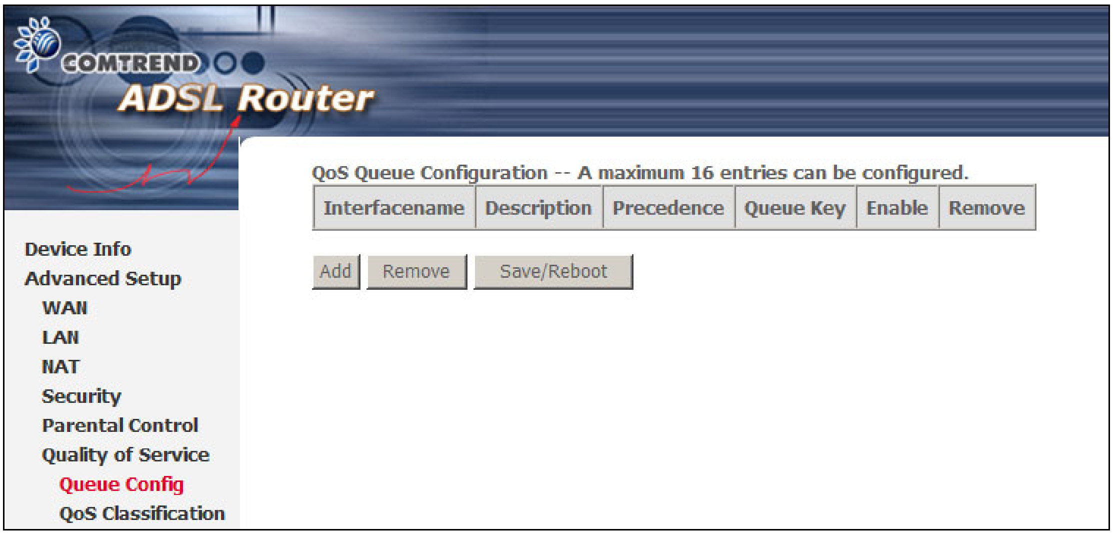
QoS and **DSCP Mark** are defined as follows:

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

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

6.6.2 Queue Configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

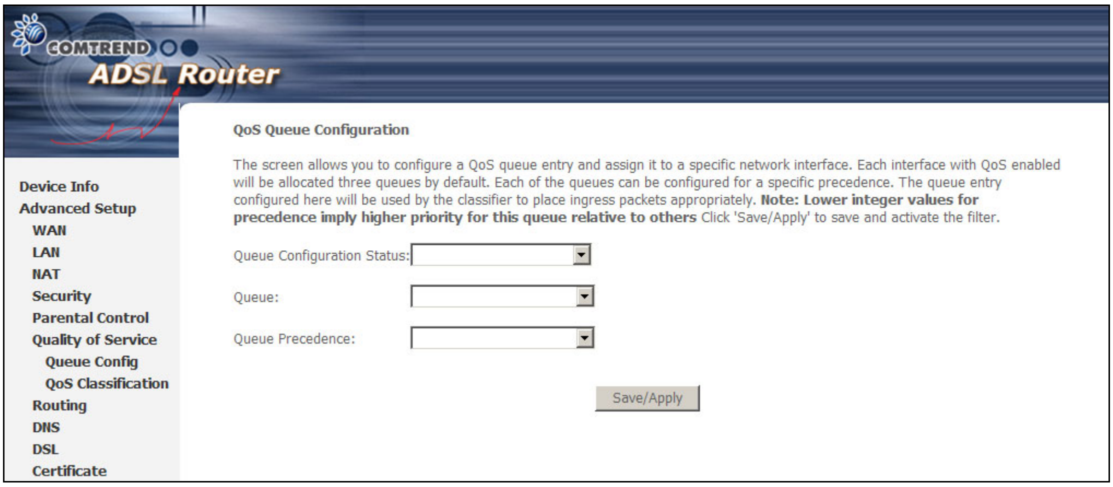


QoS Queue Configuration -- A maximum 16 entries can be configured.

Interfacename	Description	Precedence	Queue Key	Enable	Remove

Add Remove Save/Reboot

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



QoS Queue Configuration

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

Queue Configuration Status:

Queue:

Queue Precedence:

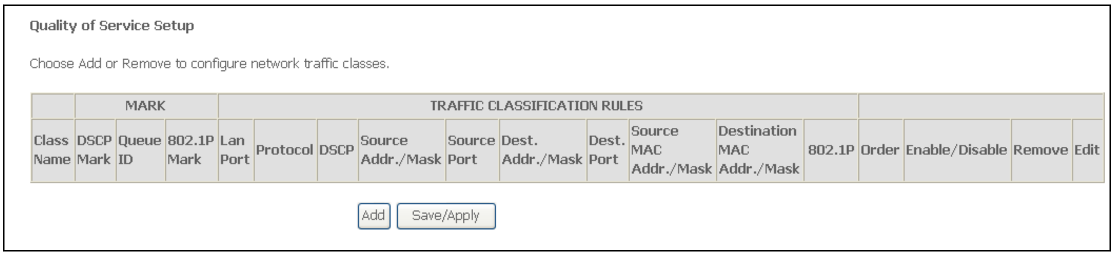
Queue Configuration Status: Enable/Disable the Queue entry.

Queue: Assign the entry to a specific network interface (QoS must be enabled).

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

6.6.3 QoS Classification

The network traffic classes are listed in the following table.



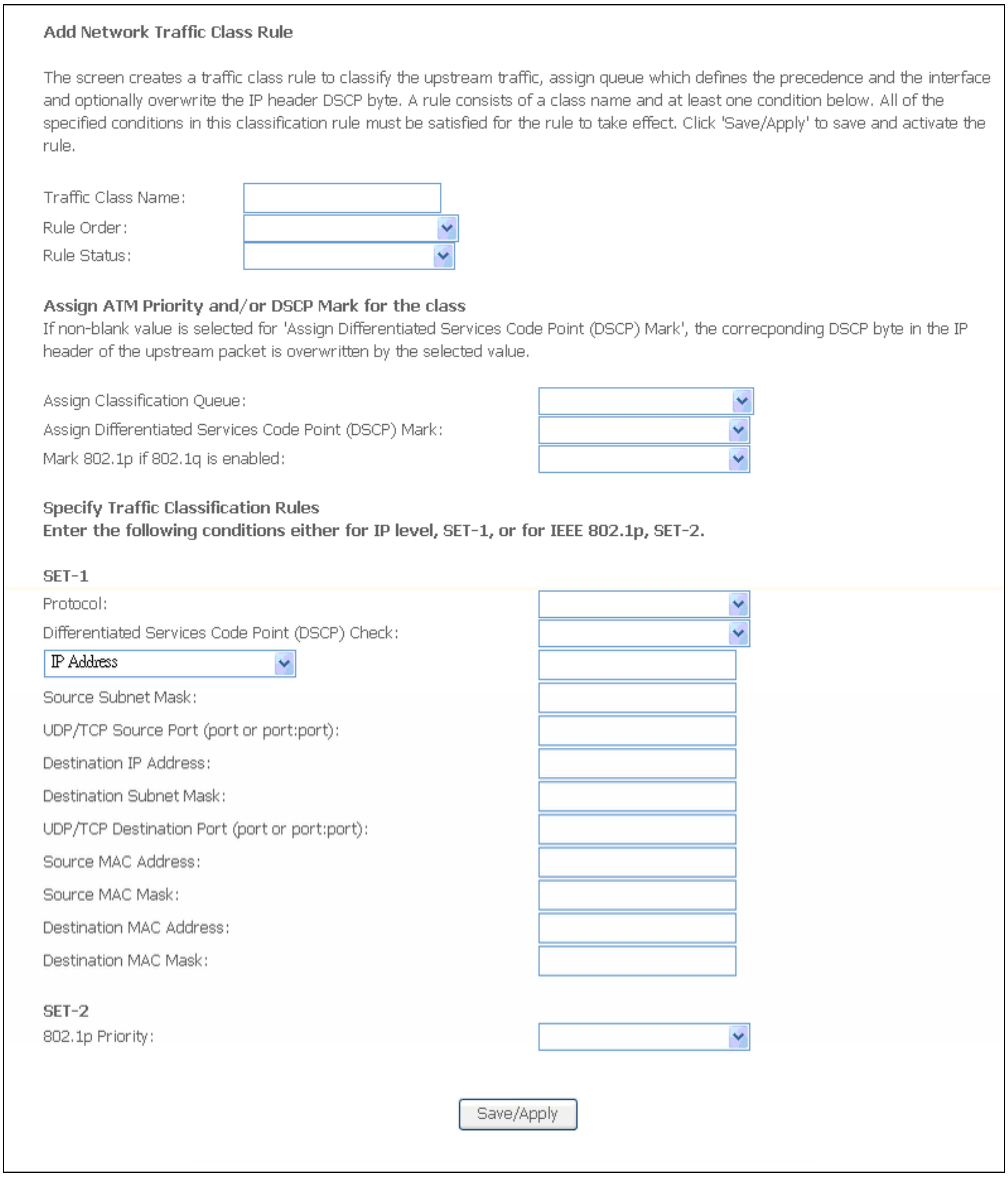
Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

Click **Add** to configure a network traffic class rule and **Save/Apply** to activate it.

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



Add Network Traffic Class Rule

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

Traffic Class Name:
Rule Order:
Rule Status:

Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:

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

SET-1
Protocol:
Differentiated Services Code Point (DSCP) Check:
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:

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last or null are the only options.
Rule Status	Disable or enable the rule.
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece P&Queue Q" where P and Q are the Precedence and Queue Key values for the corresponding Interface as listed on the Queue Config screen.
Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Mark 802.1p if 802.1q is enabled	Select between 0-7. The lower the digit shows the higher the priority.

Field	Description
SET-1	
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Differentiated Services Code Point (DSCP) Check	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Static IP or DHCP ID drop-down box	Select IP Address, Vendor Class ID (DHCP Option 60), or User Class ID (DHCP Option 77)
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
UDP/TCP Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
UDP/TCP Destination Port (port or port:port)	Enter destination port number or port range.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

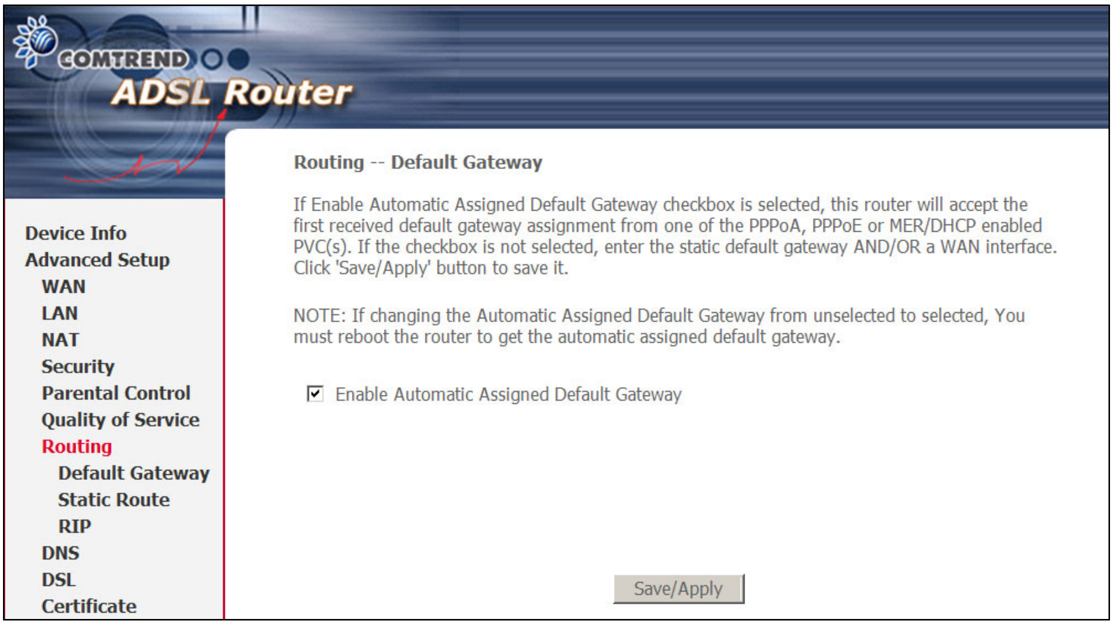
6.7 Routing

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

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

6.7.1 Default Gateway

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



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.

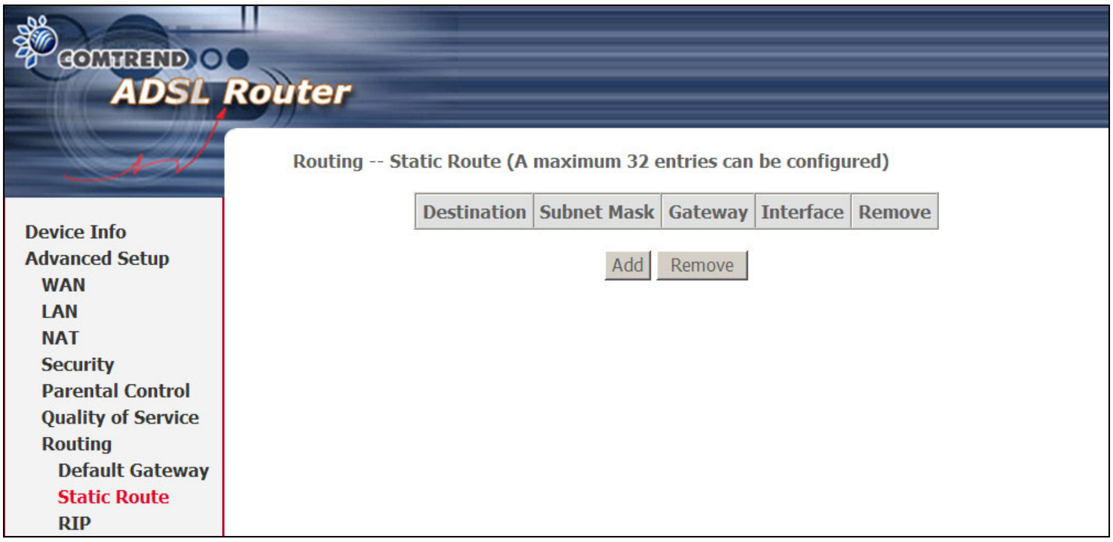
☑ Enable Automatic Assigned Default Gateway

Save/Apply

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

6.7.2 Static Route

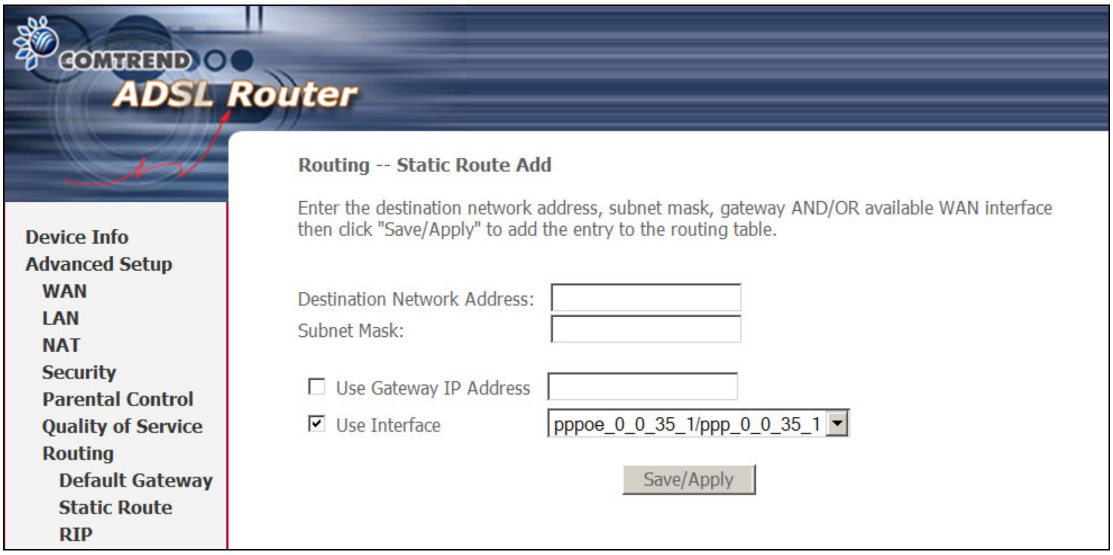
This option allows for the configuration of static routes. Click **Add** to create a new static route. Click **Remove** to delete the selected static route.



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

Destination	Subnet Mask	Gateway	Interface	Remove

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



Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

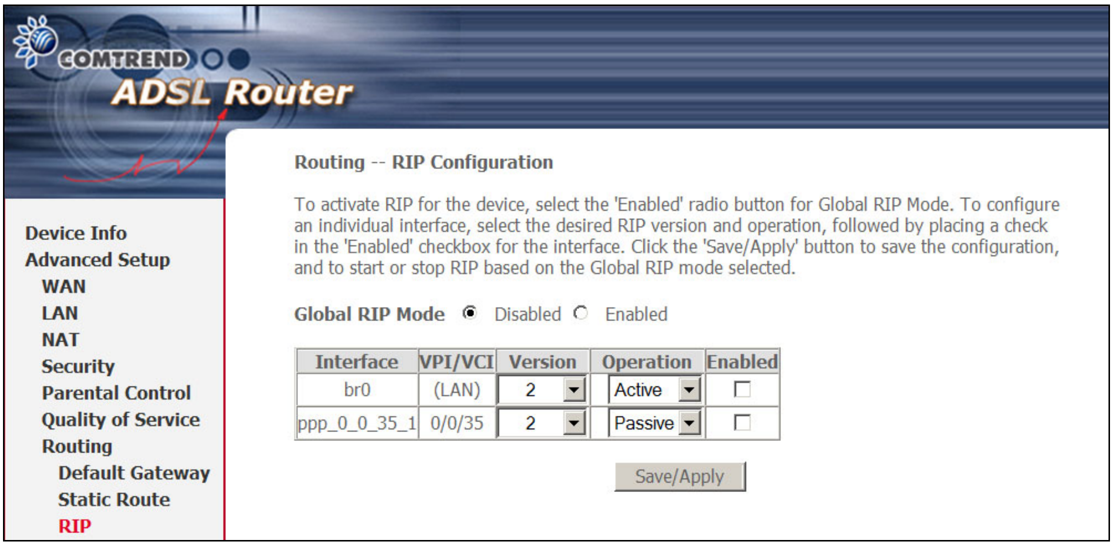
□ Use Gateway IP Address

☑ Use Interface pppoe_0_0_35_1/ppp_0_0_35_1

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

6.7.3 RIP

To activate RIP, 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).



Routing -- RIP Configuration

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

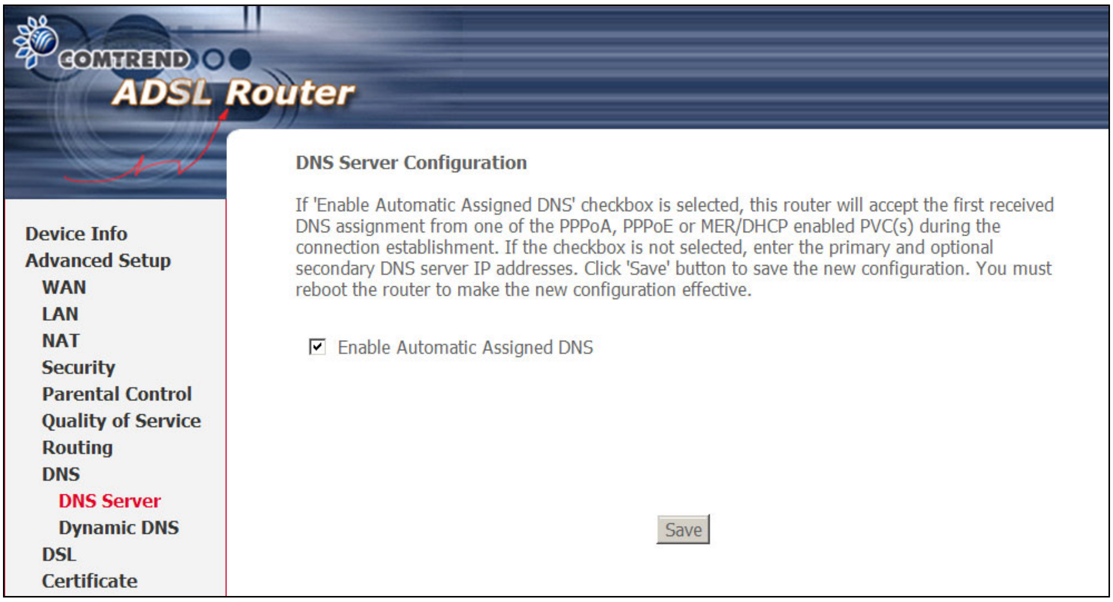
Global RIP Mode ● Disabled ○ Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	□
ppp_0_0_35_1	0/0/35	2	Passive	□

6.8 DNS

6.8.1 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.



DNS Server Configuration

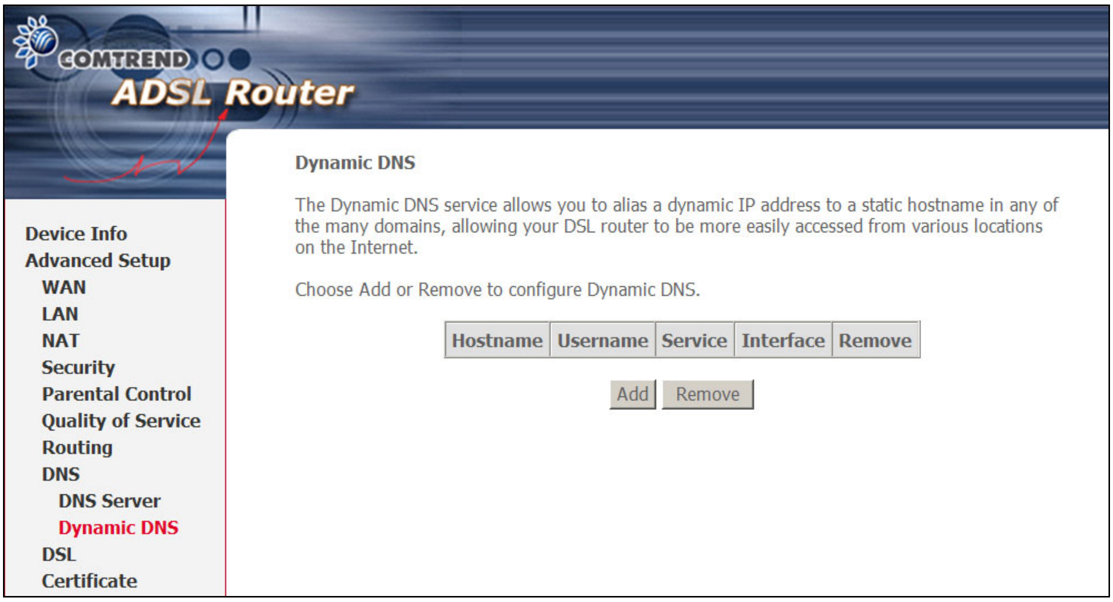
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.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

☑ Enable Automatic Assigned DNS

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

6.8.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the CT-5072T to be more easily accessed from various locations on the Internet.



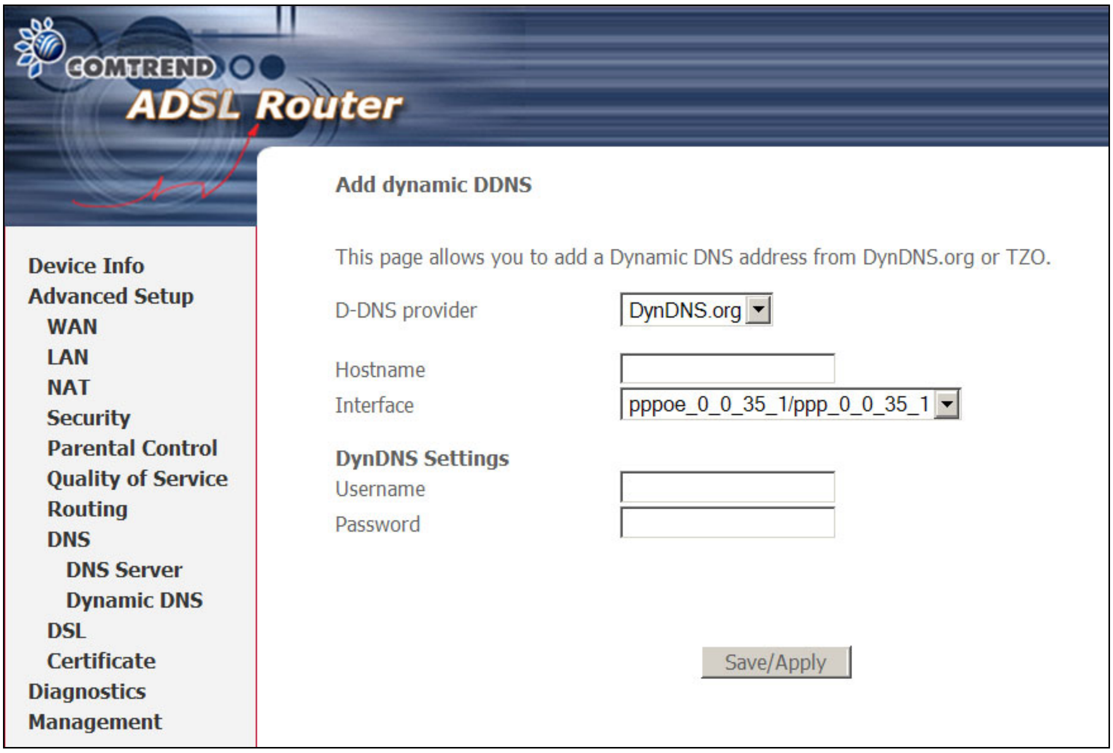
Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

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



Add dynamic DDNS

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

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_0_35_1/ppp_0_0_35_1

DynDNS Settings

Username:

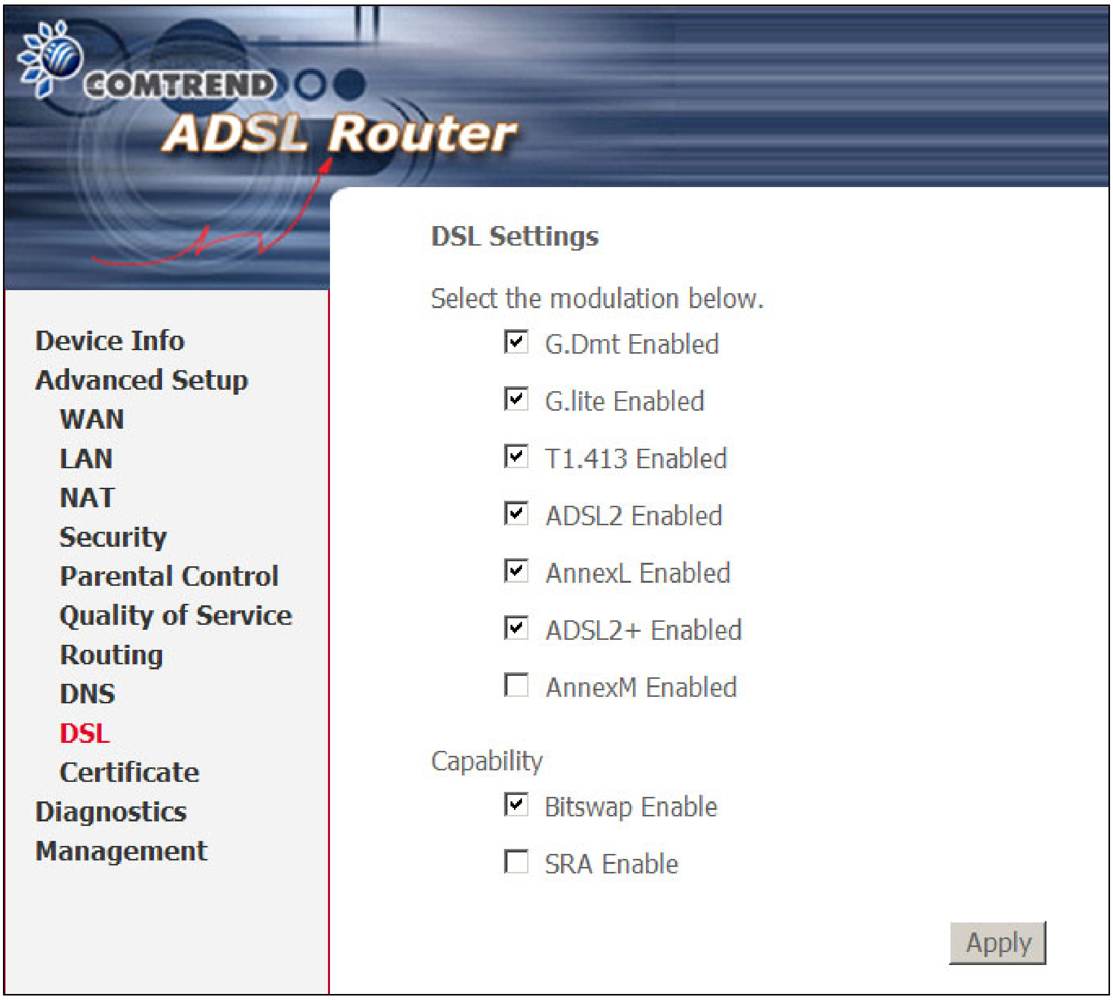
Password:

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

6.9 DSL

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



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled

☑ G.lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ AnnexL Enabled

☑ ADSL2+ Enabled

□ AnnexM Enabled

Capability

☑ Bitswap Enable

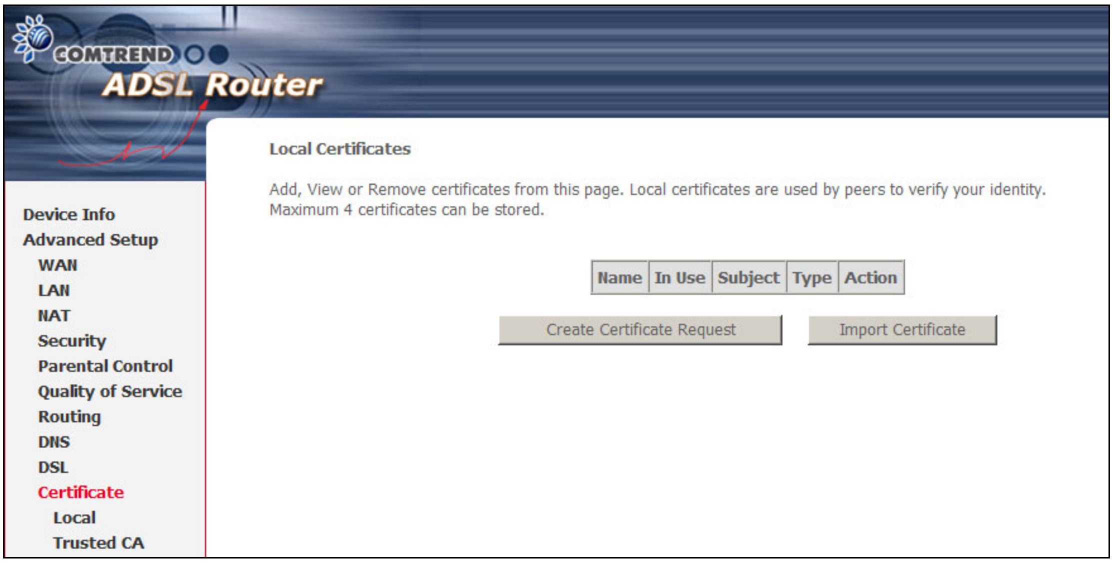
□ SRA Enable

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

6.10 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.

6.10.1 Local



Local Certificates

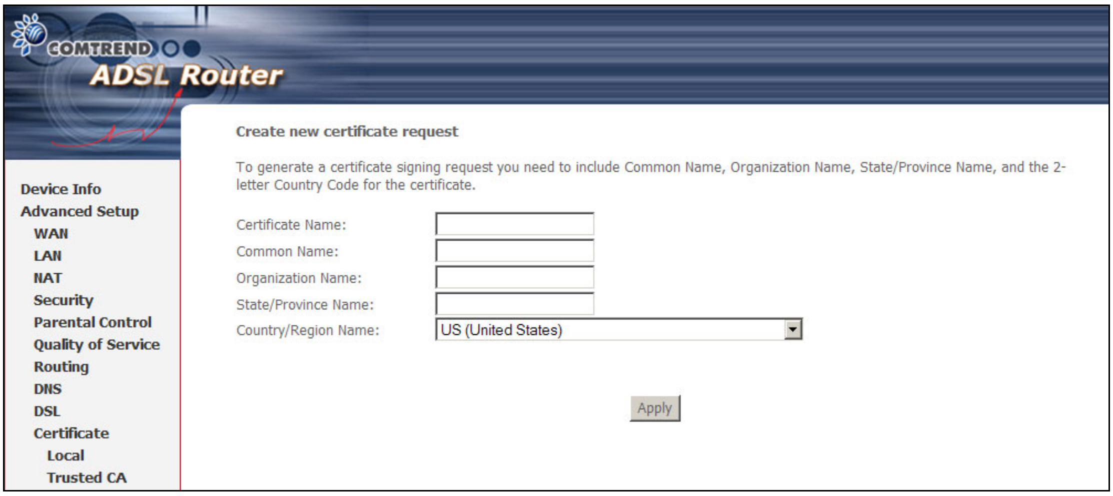
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

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.



Create new certificate request

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

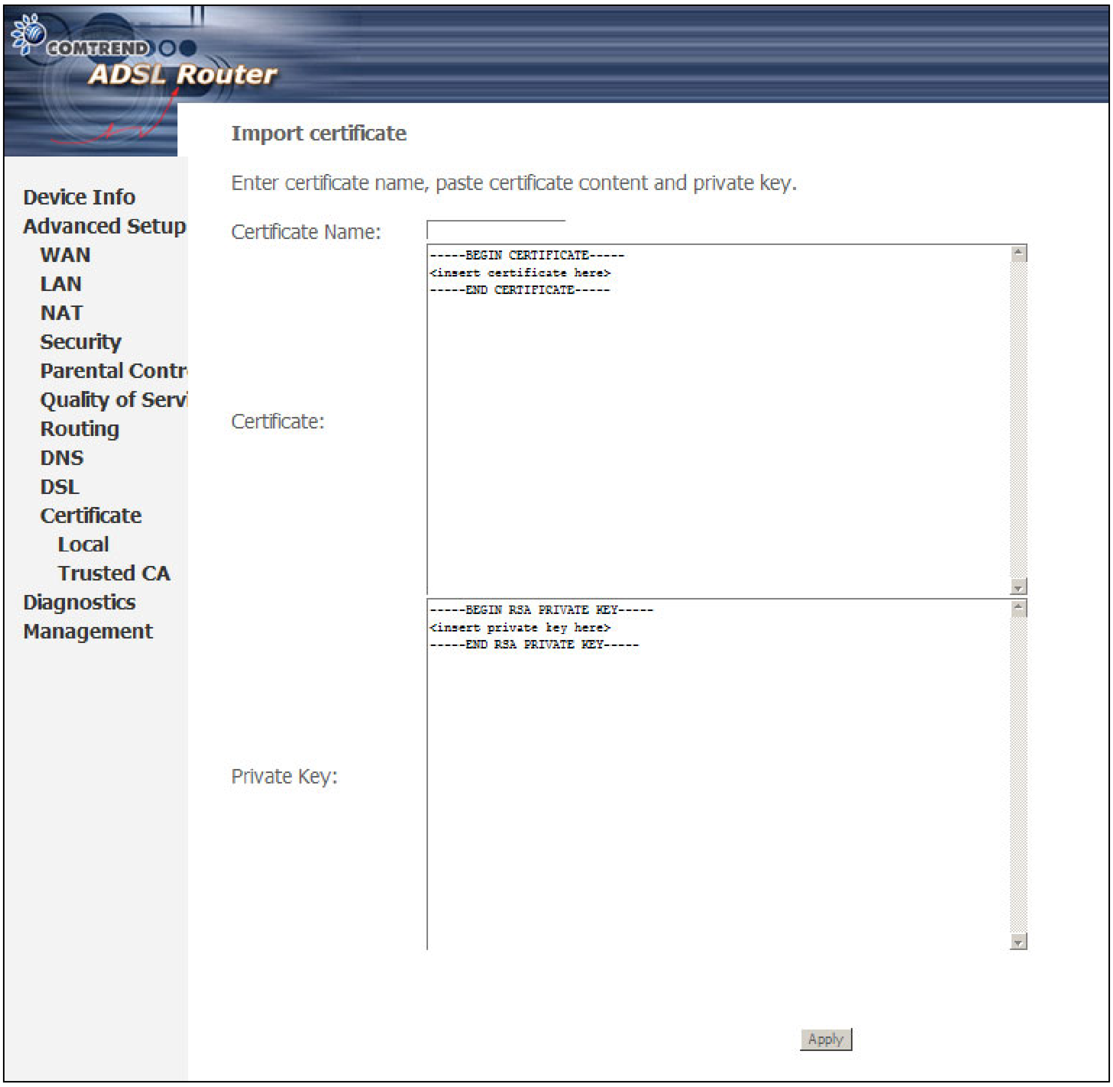
Certificate Name:
Common Name:
Organization Name:
State/Province Name:
Country/Region Name: US (United States)

The following table is provided for your reference.

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

IMPORT CERTIFICATE

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



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

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

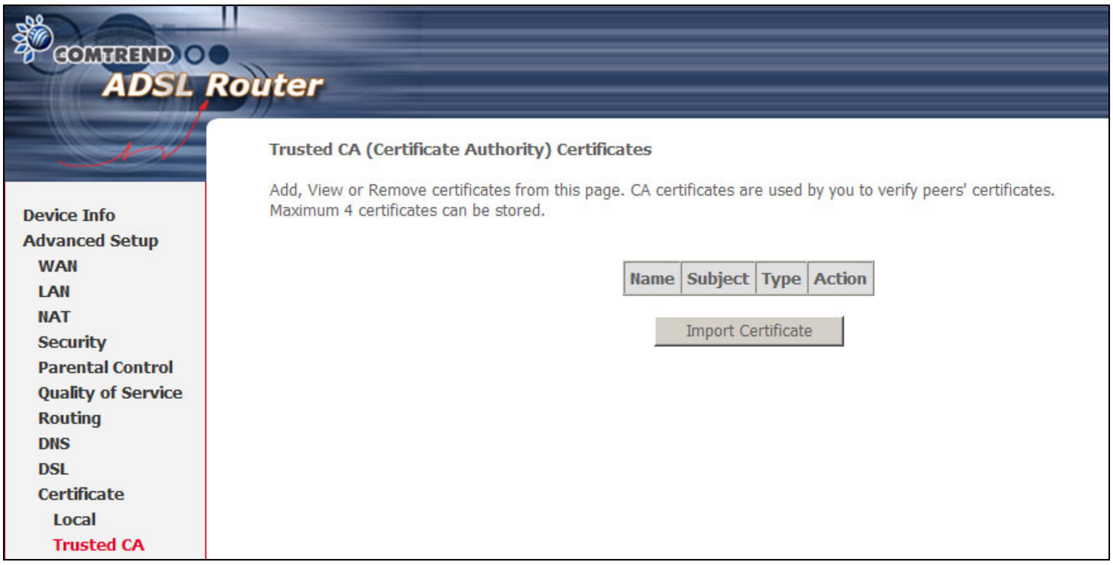
Private Key:

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

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

6.10.2 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.

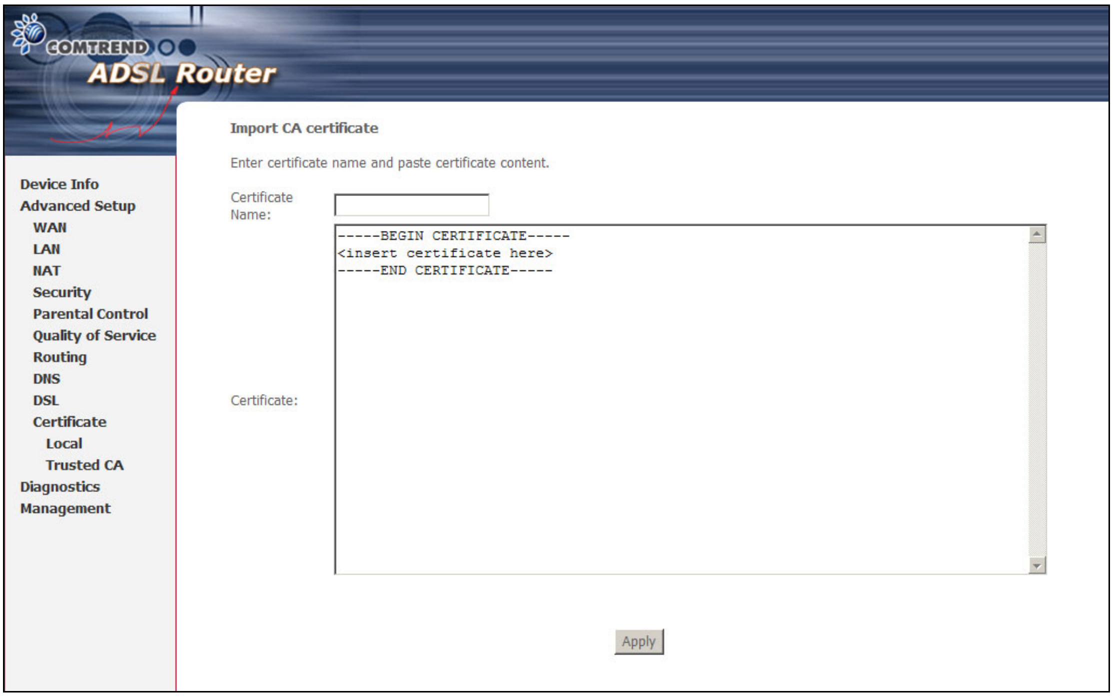


Trusted CA (Certificate Authority) Certificates

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

Name	Subject	Type	Action

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



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

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

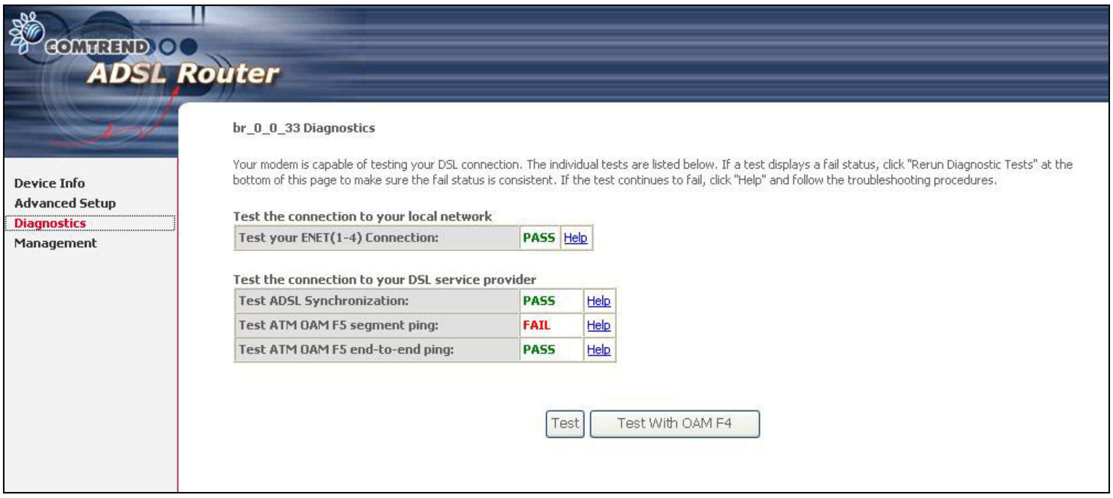
Enter a certificate name and click **Apply** to import the CA certificate.

Chapter 7 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-5072T. The basic tests (no PVC configured) are described in the table below. If a test displays a fail status, click the **Test** button to retest and confirm the error. If the test continues to fail, click Help and follow the troubleshooting procedures provided.

Test	Description
ENET Connection	**Pass:** Indicates that the CT-5072T has detected the Ethernet interface on your computer. **Fail:** Indicates that the CT-5072T does not detect the Ethernet interface on your computer.
ADSL Synchronization	**Pass:** Indicates that the CT-5072T has detected a DSL signal from the telephone company. **Fail:** Indicates that the CT-5072T does not detect a DSL signal from the telephone company.

Bridge Diagnostic



br_0_0_33 Diagnostics

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

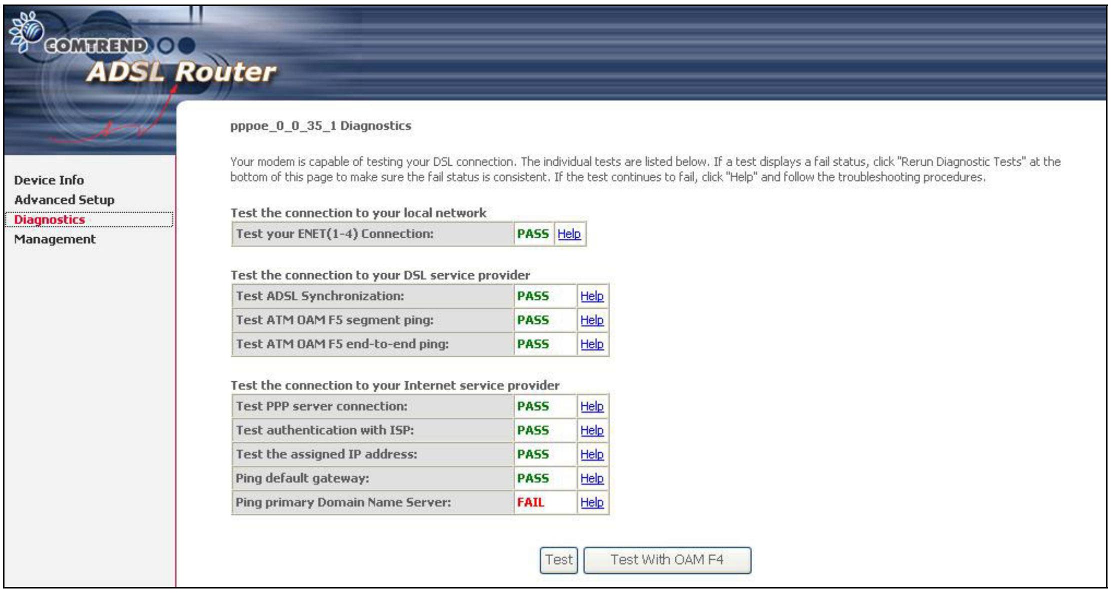
Test the connection to your local network

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

Test the connection to your DSL service provider

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

PPPoE Connection



pppoe_0_0_35_1 Diagnostics

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

Test the connection to your local network

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

Test the connection to your DSL service provider

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

Test the connection to your Internet service provider

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

Chapter 8 Management

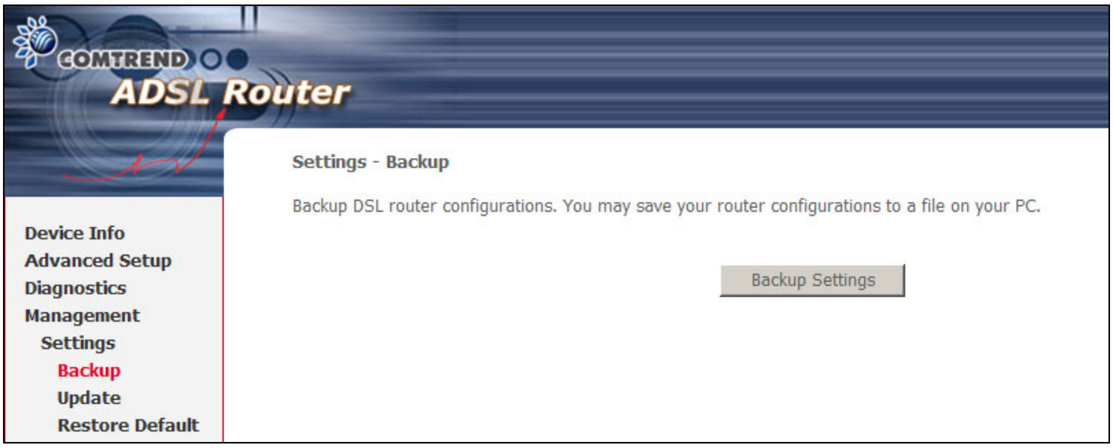
The Management menu has the following maintenance functions and processes:

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.

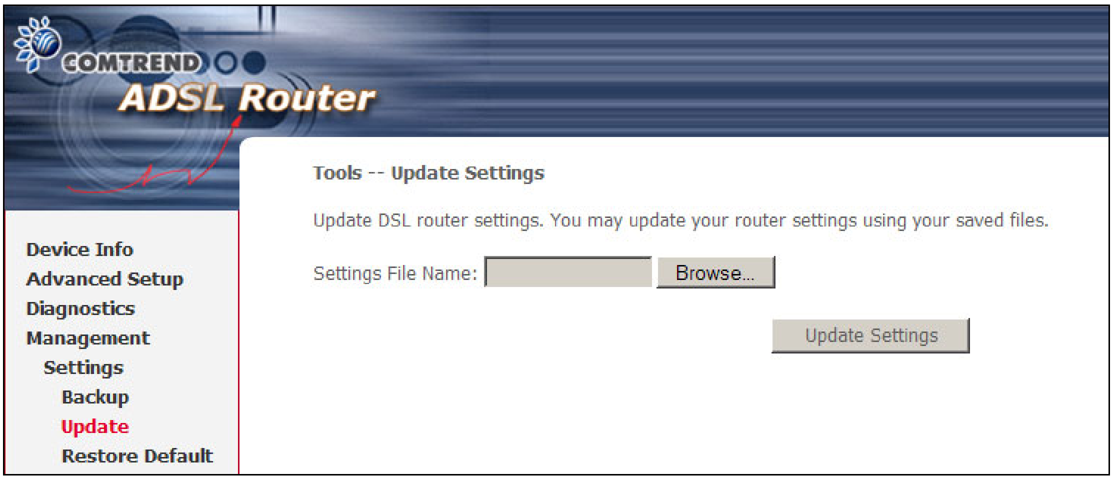


Settings - Backup

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

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.



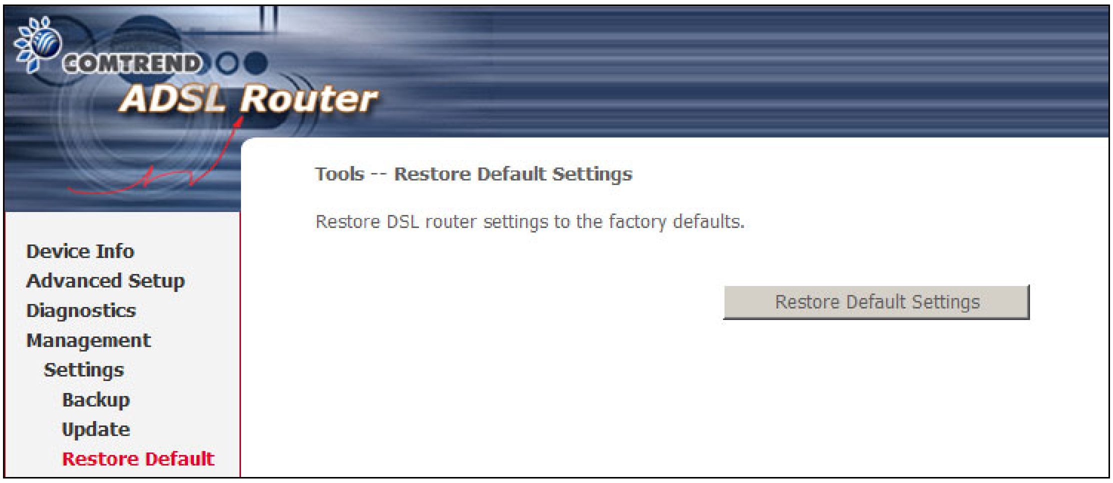
Tools -- Update Settings

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

Settings File Name:

8.1.3 Restore Default

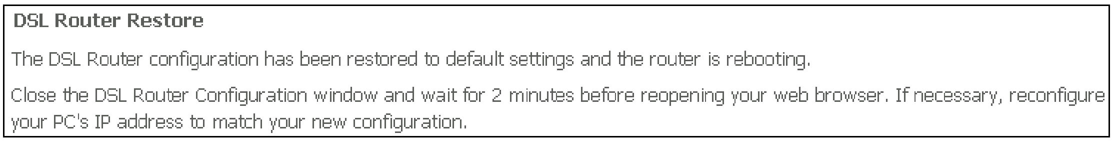
Click **Restore Default Settings** to restore the CT-5072T to factory default settings.



Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

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



DSL Router Restore

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

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

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.

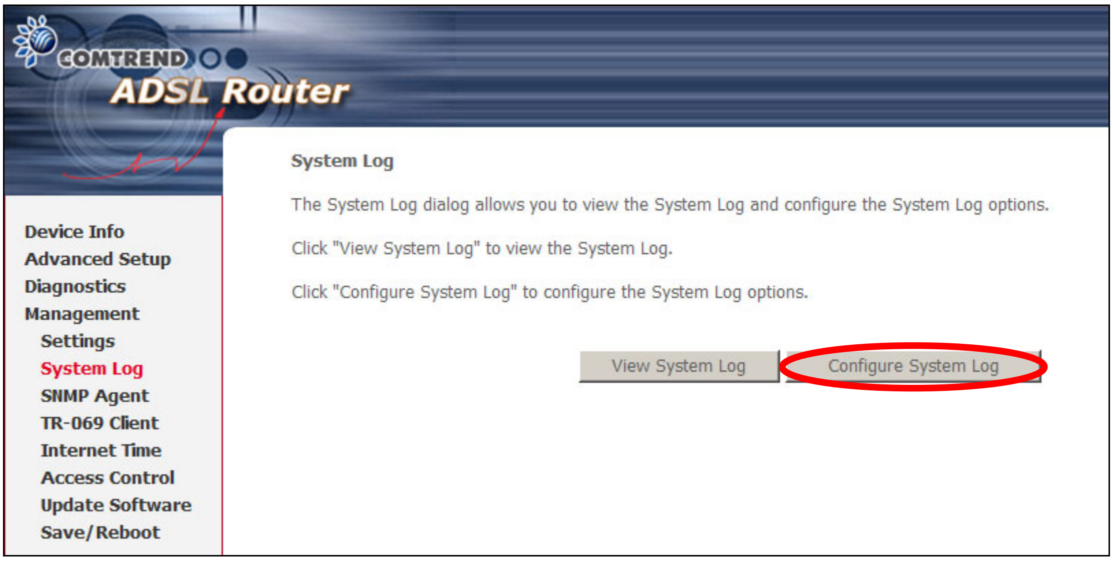
NOTE: This entry has the same effect as the **Reset** button. The CT-5072T board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

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 (circled in **Red**).



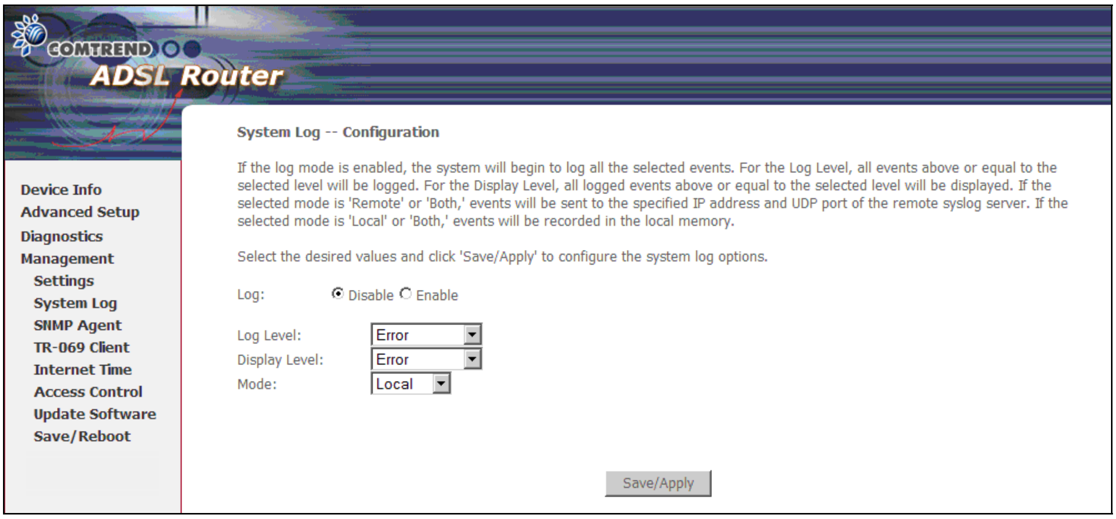
System Log

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

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

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

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



System Log -- Configuration

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

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

Log: ● Disable ○ Enable

Log Level: Error

Display Level: Error

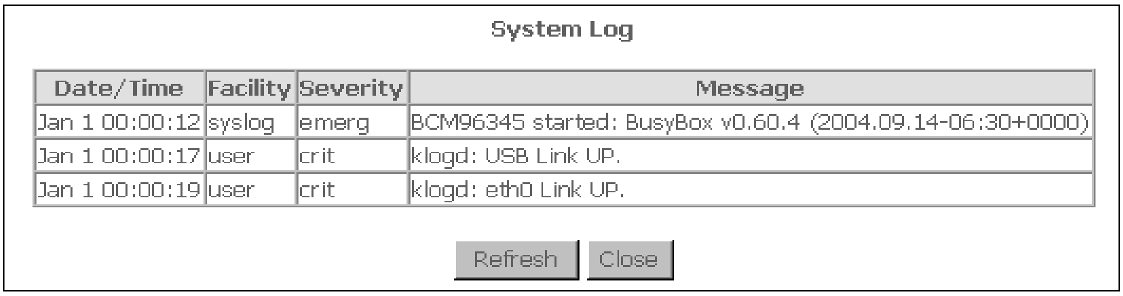
Mode: Local

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, select the **Enable** radio button and then click **Save/Apply**.

Option	Description
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5072T SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or 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.

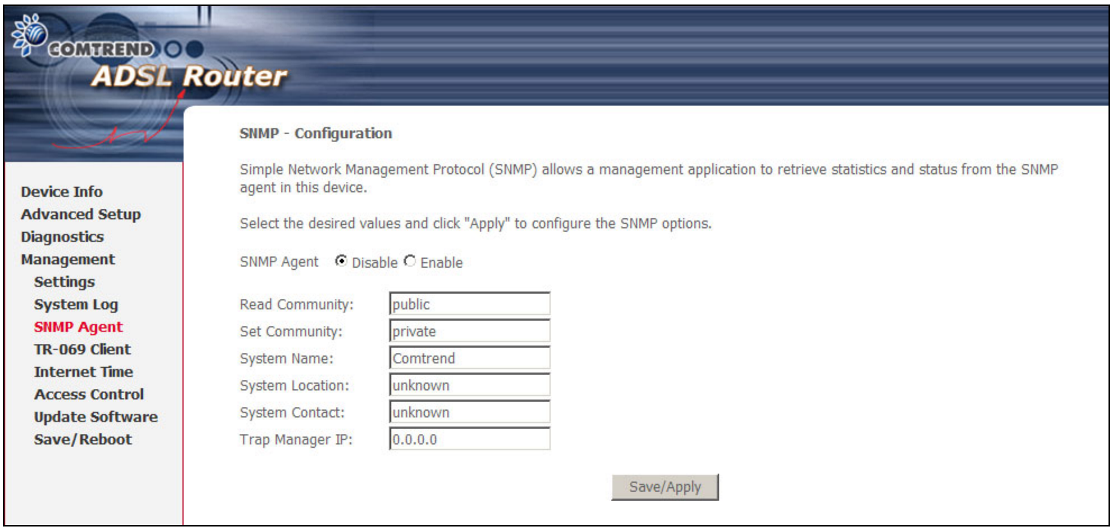


System Log

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.



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.

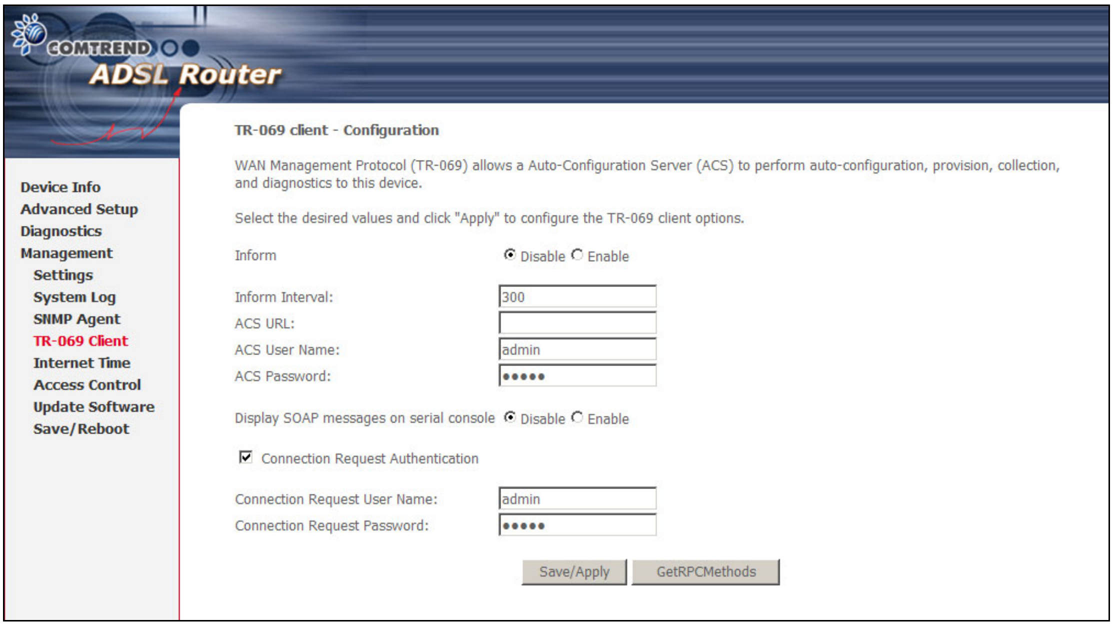
SNMP Agent ● Disable ○ Enable

Read Community: public
Set Community: private
System Name: Comtrend
System Location: unknown
System Contact: unknown
Trap Manager IP: 0.0.0.0

Options	Description
SNMP Agent	Use the radio buttons to Enable or Disable the SNMP Agent
Read Community	Default is "public"
Set Community	Default is "private"
System Name	Default determined from the hostname.
System Location	Shows the location of the host system.
System Contact	Shows who should be contacted about the host system.
Trap Manager IP	Supports a monitor and alarm via port 162 from Agent.

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. Select desired values and click **Save/Apply** to configure TR-069 client options.



TR-069 client - Configuration

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

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

Inform ● Disable ○ Enable

Inform Interval: 300

ACS URL:

ACS User Name: admin

ACS Password: •••••

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name: admin

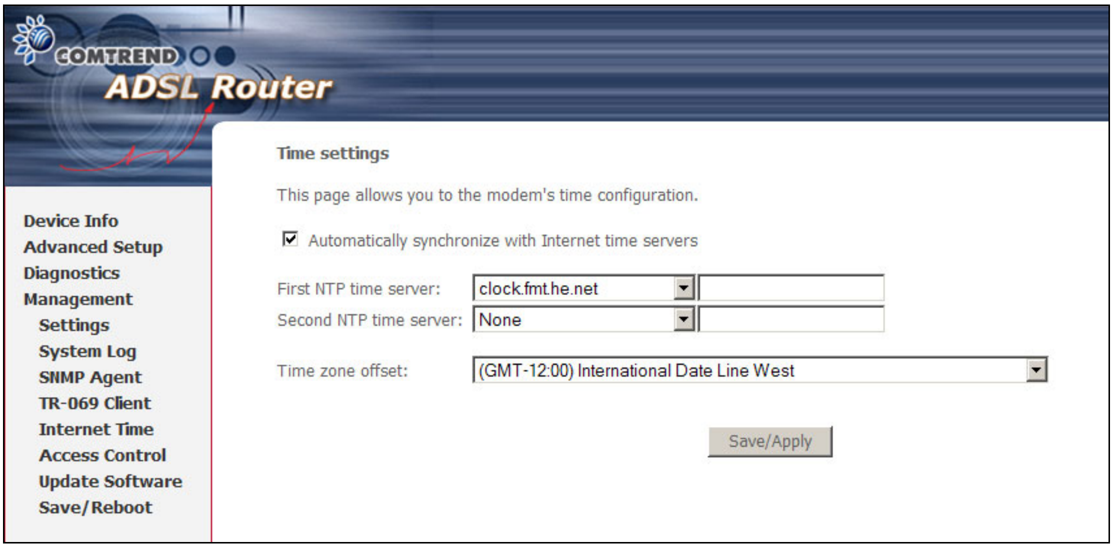
Connection Request Password: •••••

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

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

8.5 Internet Time

This option 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**.



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: clock.fmt.he.net

Second NTP time server: None

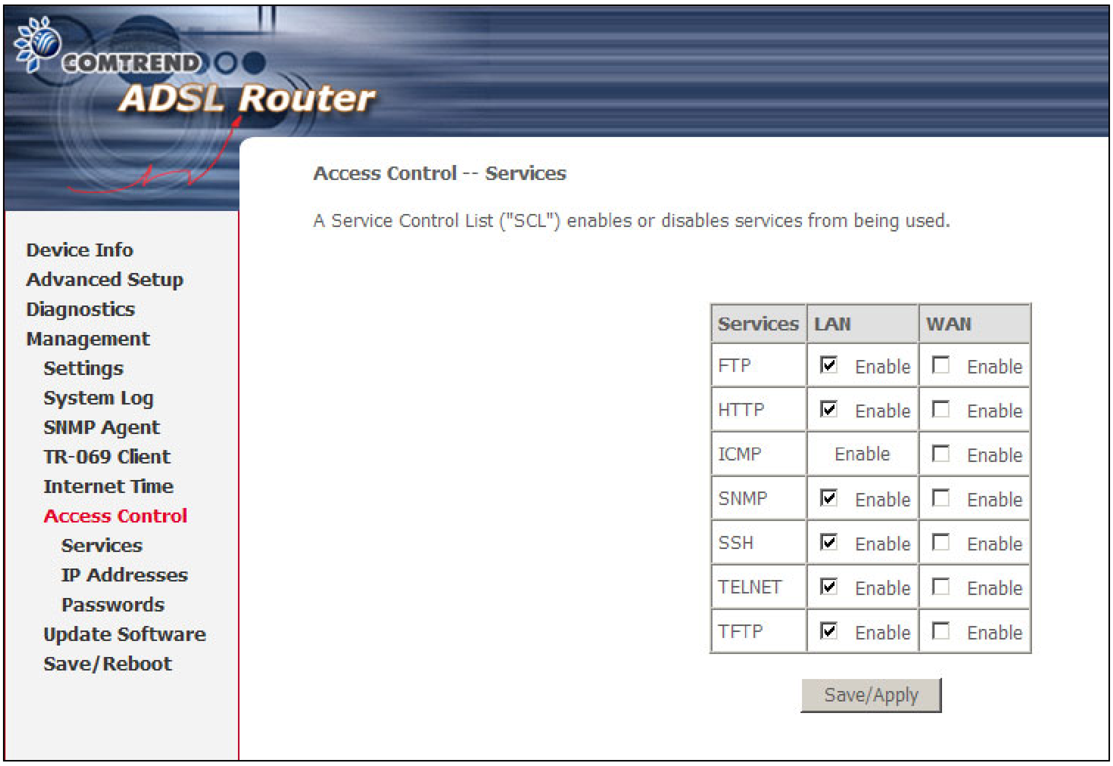
Time zone offset: (GMT-12:00) International Date Line West

NOTE:	Internet Time must be activated to use Parental Control (page 45). 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

The Service Control List provides access options to the CT-5072T over the LAN or WAN. To enable a service, tick its checkbox ☑ under LAN or WAN and click **Save/Apply**.



Access Control -- Services

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

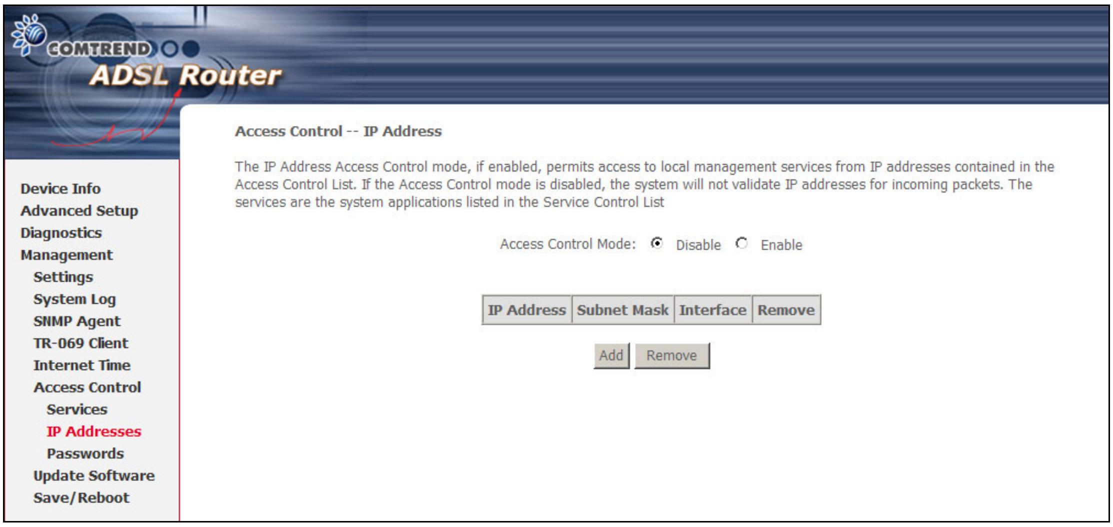
Services	LAN	WAN
FTP	☑ Enable	□ Enable
HTTP	☑ Enable	□ Enable
ICMP	Enable	□ Enable
SNMP	☑ Enable	□ Enable
SSH	☑ Enable	□ Enable
TELNET	☑ Enable	□ Enable
TFTP	☑ Enable	□ Enable

NOTES: The WAN column only appears if a PVC connection is configured.

For a quick introduction to SSH clients consult Appendix D.

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.



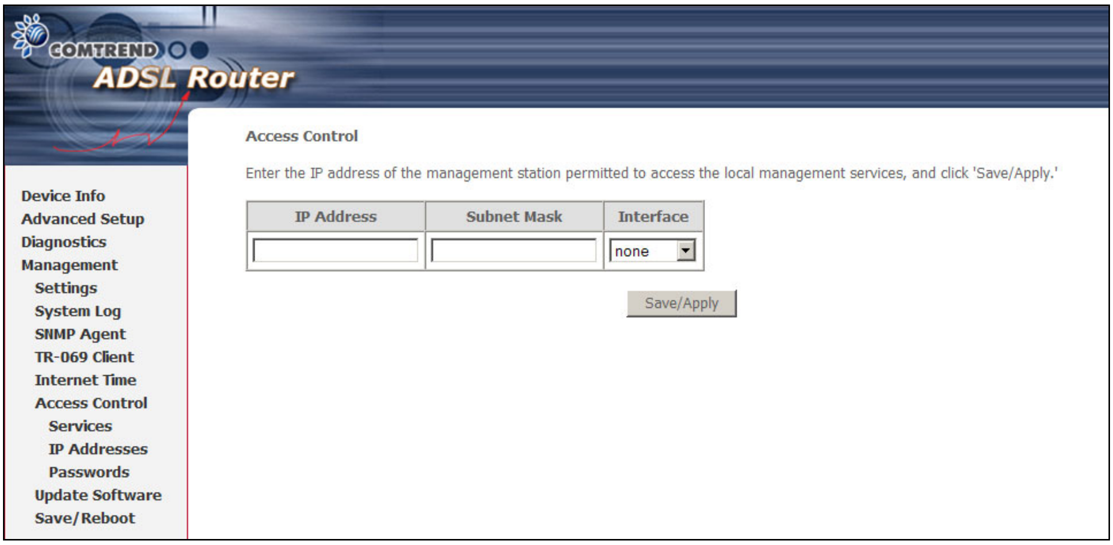
Access Control -- IP Address

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

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.



Access Control

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

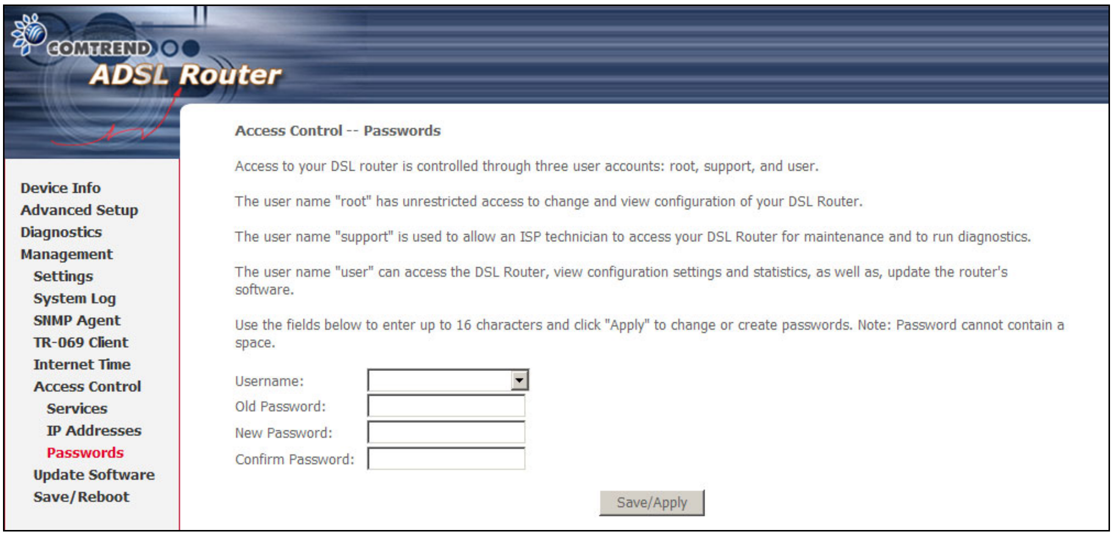
IP Address	Subnet Mask	Interface
		none

8.6.3 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5072T 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.

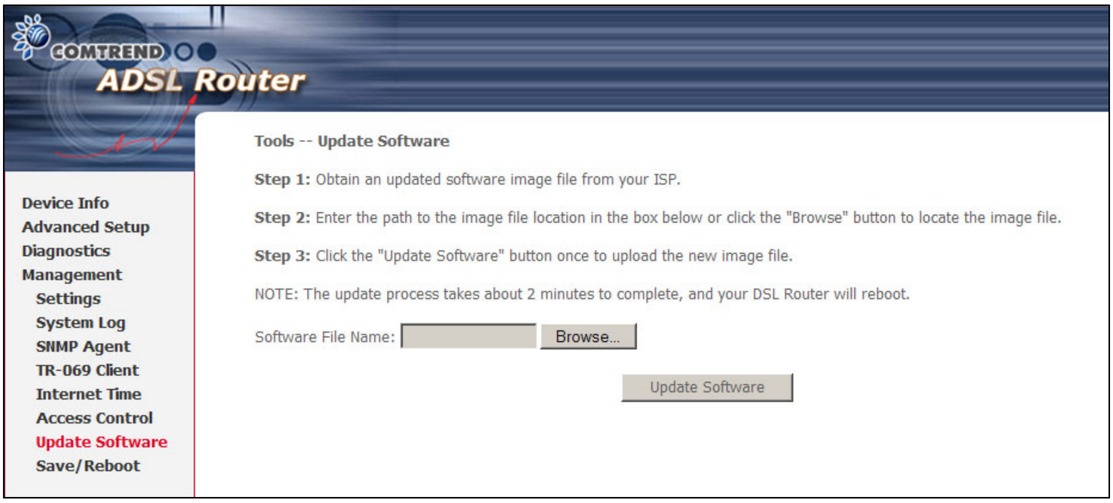
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

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.

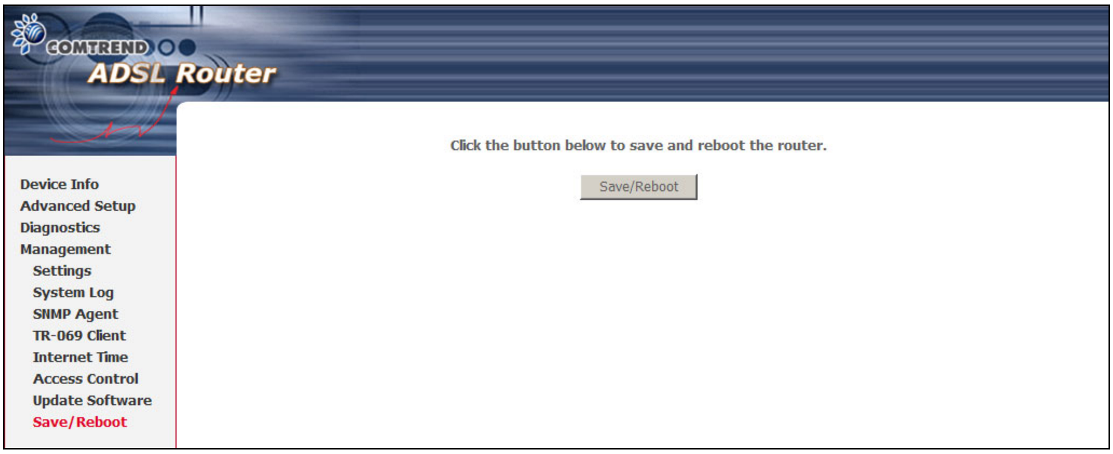
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

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 Information 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**.



Click the button below to save and reboot the router.

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.

<u>**Example 2**</u>**:**

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.

<u>**Example 1**</u>**:**

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-5072T, 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.992.5/G.992.3/G.992.1, ANSI T1.413 Issue 2

G.992.5 (ADSL2+)	Downstream : 24 Mbps	Upstream : 1.3 Mbps
G.992.3 (ADSL2)	Downstream : 12 Mbps	Upstream : 1.3 Mbps
G.DMT	Downstream : 8 Mbps	Upstream : 0.8 Mbps

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, DMZ, DHCP Server/Relay/Client, DNS probe/relay, 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: 100 - 240 Vac
Output: 18 Vdc / 300 mA

Environment Condition

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

Dimensions..................................... 107 mm (W) x 95 mm (H) x 36 mm (D)

Kit Weight

(1*CT-5072T, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 0.33 kg

Certifications .... FCC Part 15 class B, CE

NOTE: Specifications are subject to change without notice

Appendix D – SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

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

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

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

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

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