



CT-6382T

Wireless ADSL2/2+VoIP IAD

User's Manual

Version A1.1, June 26, 2007



261078-003

Preface

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

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

This document is subject to change without notice.



Warning

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

Copyright

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

Technical support

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

INT-support@comtrend.com

Table of Contents

CHAPTER 1	INTRODUCTION	5
1.1	FEATURES.....	5
1.2	APPLICATION.....	6
1.3	FRONT PANEL LED INDICATORS.....	7
CHAPTER 2	INSTALLATION	9
2.1	HARDWARE INSTALLATION.....	9
CHAPTER 3	LOGIN VIA THE WEB BROWSER.....	11
3.1	IP ADDRESS.....	11
3.2	LOGIN PROCEDURE	13
3.3	DEFAULT SETTINGS	14
CHAPTER 4	DEVICE INFORMATION	15
4.1	WAN.....	17
4.2	STATISTICS	18
4.2.1	<i>LAN Statistics.....</i>	<i>19</i>
4.2.2	<i>WAN Statistics.....</i>	<i>20</i>
4.2.3	<i>ATM statistics</i>	<i>21</i>
4.2.4	<i>ADSL Statistics</i>	<i>23</i>
4.2.5	<i>Route.....</i>	<i>26</i>
4.2.6	<i>ARP.....</i>	<i>27</i>
4.2.7	<i>DHCP.....</i>	<i>28</i>
CHAPTER 5	QUICK SETUP.....	29
5.1	AUTO QUICK SETUP	30
5.2	MANUAL QUICK SETUP	31
5.2.1	<i>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....</i>	<i>33</i>
5.2.2	<i>MAC Encapsulation Routing (MER)</i>	<i>38</i>
5.2.3	<i>IP Over ATM.....</i>	<i>43</i>
5.2.4	<i>Bridging.....</i>	<i>47</i>
CHAPTER 6	ADVANCED SETUP	49
6.1	WAN.....	51
6.2	LAN.....	52
6.3	NAT	54

6.3.1	<i>Virtual Servers</i>	54
6.3.2	<i>Port Triggering</i>	56
6.3.3	<i>DMZ Host</i>	58
6.4	SECURITY	59
6.4.1	<i>MAC Filtering</i>	59
6.4.2	<i>Parental Control</i>	61
6.4.3	<i>IP Filtering</i>	63
6.5	QUALITY OF SERVICE	66
6.6	ROUTING	70
6.6.1	<i>Default Gateway</i>	70
6.6.2	<i>Static Route</i>	71
6.6.3	<i>RIP</i>	72
6.7	DNS.....	73
6.7.1	<i>DNS Server</i>	73
6.7.2	<i>Dynamic DNS</i>	74
6.8	DSL	76
6.9	PRINT SERVER	77
6.10	PORT MAPPING.....	78
6.11	CERTIFICATE.....	81
6.11.1	<i>Local</i>	81
6.11.2	<i>Trusted CA</i>	84
CHAPTER 7	WIRELESS	85
7.1	WIRELESS BASIC SCREEN.....	85
7.1.1	<i>Security</i>	87
7.1.2	<i>MAC Filter</i>	90
7.1.3	<i>Wireless Bridge</i>	92
7.1.4	<i>Advanced</i>	93
7.1.5	<i>Quality of Service</i>	97
7.1.6	<i>Station Info</i>	98
CHAPTER 8	VOICE.....	99
8.1	MGCP.....	100
CHAPTER 9	DIAGNOSTICS	102
CHAPTER 10	MANAGEMENT	104
10.1	SETTINGS	104
10.1.1	<i>Configuration Backup</i>	105
10.1.2	<i>Configuration Restoration</i>	106

10.1.3	Restore Default	107
10.2	SYSTEM LOG	109
10.3	SNMP AGENT	112
10.4	TR-069 CLIENT	113
10.5	INTERNET TIME	115
10.6	ACCESS CONTROL	116
10.6.1	Services	117
10.6.2	Access IP Addresses	118
10.6.3	Passwords	119
10.7	UPDATE SOFTWARE	120
10.8	SAVE AND REBOOT	121
APPENDIX A: PRINTER SERVER CONFIGURATION		122
APPENDIX B: FIREWALL		128
APPENDIX C: PIN ASSIGNMENTS		134
APPENDIX D: SPECIFICATIONS		135
APPENDIX E: SSH CLIENT		137

Chapter 1 Introduction

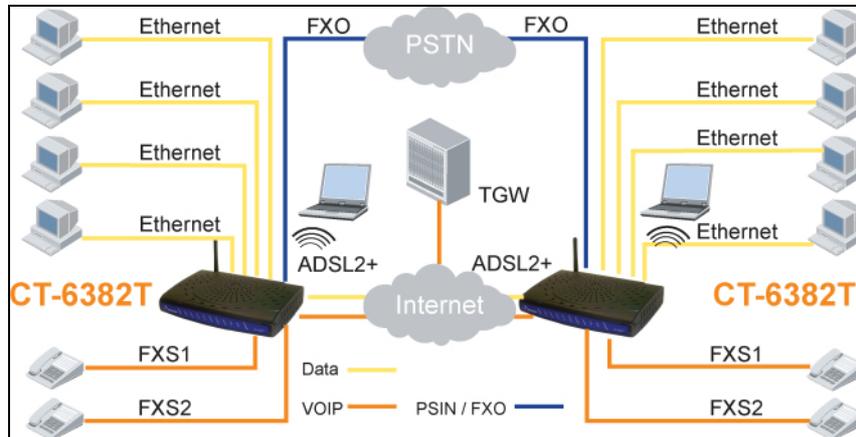
Comtrend's CT-6382T is a powerful WLAN VoIP IAD (Integrated Access Device), providing predictable, real-time, toll-quality voice over the Internet. Developed with ADSL2/2+ broadband technology over PSTN, the CT-6382T offers residential and business users easy access to the Internet via WLAN or Ethernet, also providing VoIP via standard analog telephones.

1.1 Features

- **Supports TR-069**
- **ADSL2/2+**
- **VoIP and Router integrated**
- **Integrated 802.11g AP, backward compatible with 802.11b**
- **Supports life line: PSTN alive when power off**
- **Supports emergency call**
- **Supports QoS (Quality of Service) for voice**
- **Supports caller ID display and restriction**
- **Supports call hold**
- **Supports call waiting**
- **Supports call forwarding**
- **Supports call transfer**
- **Supports 3-way conference**
- **Supports direct number dialing**
- **Supports remote administration, automatic firmware upgrade and configuration**
- **Supports VPN Pass-through**
- **Supports Day-time parental control**

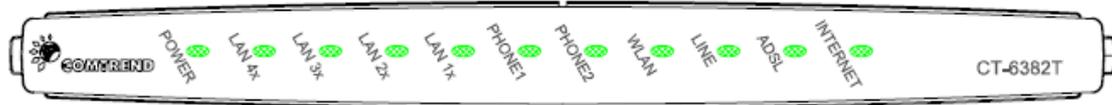
1.2 Application

The following diagram depicts the application of the CT-6382T.



1.3 Front Panel LED Indicators

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



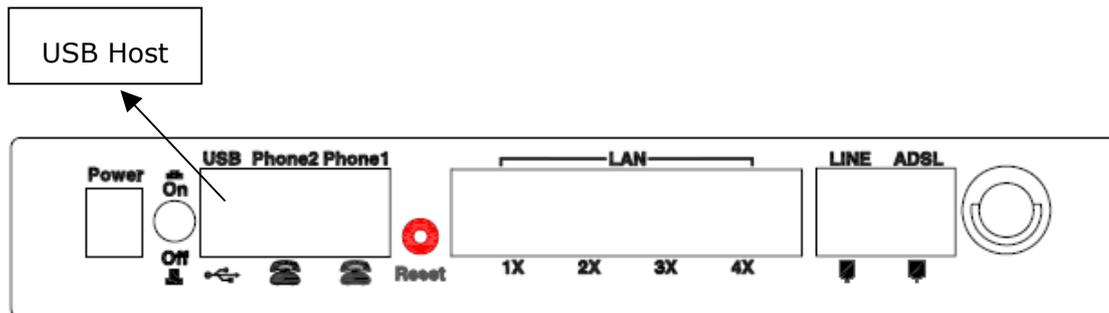
LED	Color	Mode	Function
POWER	Green	On	The VoIP IAD is powered up.
		Off	The VoIP IAD is powered down.
LAN 4x~1x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
PHONE1	Green	On	The FXS phone 1 is off hook.
		Off	The FXS phone 1 is on hook.
PHONE2	Green	On	The FXS phone 2 is off hook.
		Off	The FXS phone 2 is on hook.
WLAN	Green	On	The wireless module is ready.
		Off	The wireless module is not installed or WLAN is disabled.
		Blink	Data transmitting or receiving over WLAN.
LINE	Green	On	An FXO line is off hook.
		Off	An FXO line is on hook.
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	The ADSL link is training.

INTERNET	Red	On	<p>Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)</p> <p>For bridged mode, the indicator light MUST be off.</p> <p>If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.</p>
		Off	<p>Modem power off, modem in bridged mode or ADSL connection not present.</p>
	Green	Blinking	<p>IP connected and IP Traffic is passing thru the device (either direction)</p>

Chapter 2 Installation

2.1 Hardware Installation

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for at least 5 seconds. If held down for more than 12 seconds, the VoIP IAD will go into firmware update state and the user can update the VoIP IAD from web-interface @192.168.1.1 without ID/Password.



Follow the instructions below to complete the hardware connections.

Connection to ADSL port

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

Connection to LINE port

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

Connection to LAN port

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

Connect the telephone set to the RJ11 **Phone1/ Phone2 port** for VoIP service.

Connection to USB host port

The CT-6382T can be equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as printers and a hard disc to the CT-6382T. For this software release, printer server is supported.

Connection to Power

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

After all connections have been made, push the power-switch in to the on position. After power on, the VoIP IAD performs a self-test. Wait for a few seconds until the test is finished, then the VoIP IAD will be ready to operate.

Note: Restore the default parameters of the VoIP IAD by holding down the device's Reset button until the LED's start blinking simultaneously (about 5 seconds). After the device has rebooted successfully, and if the connection is established, the LAN LED, ADSL LED will display in green, depending on the connection type.

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

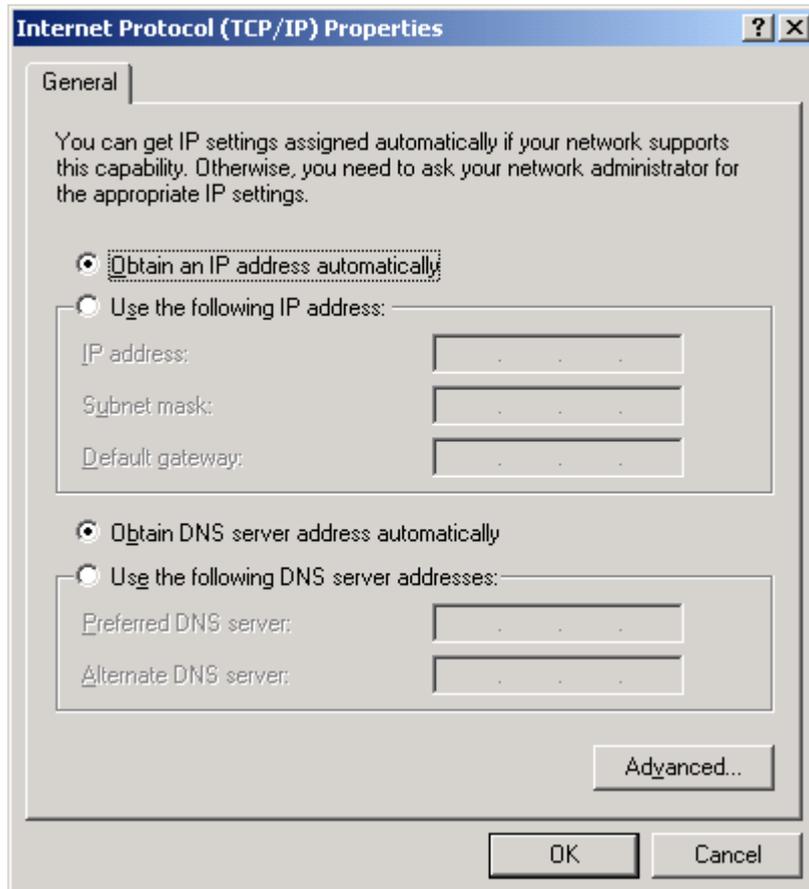
Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

Chapter 3 Login via the Web Browser

This section describes how to manage the VoIP IAD via a Web browser via the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. (The Web page is best viewed with Microsoft Internet Explorer 5.0 and later): A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

3.1 IP Address

Note: When the CT-6382T is switched on, the DHCP server will start automatically. The default address for the CT-6382T is 192.168.1.1 and DHCP is enabled as default for the PC. You can automatically obtain an IP by selecting Obtain an IP address automatically, as shown here:

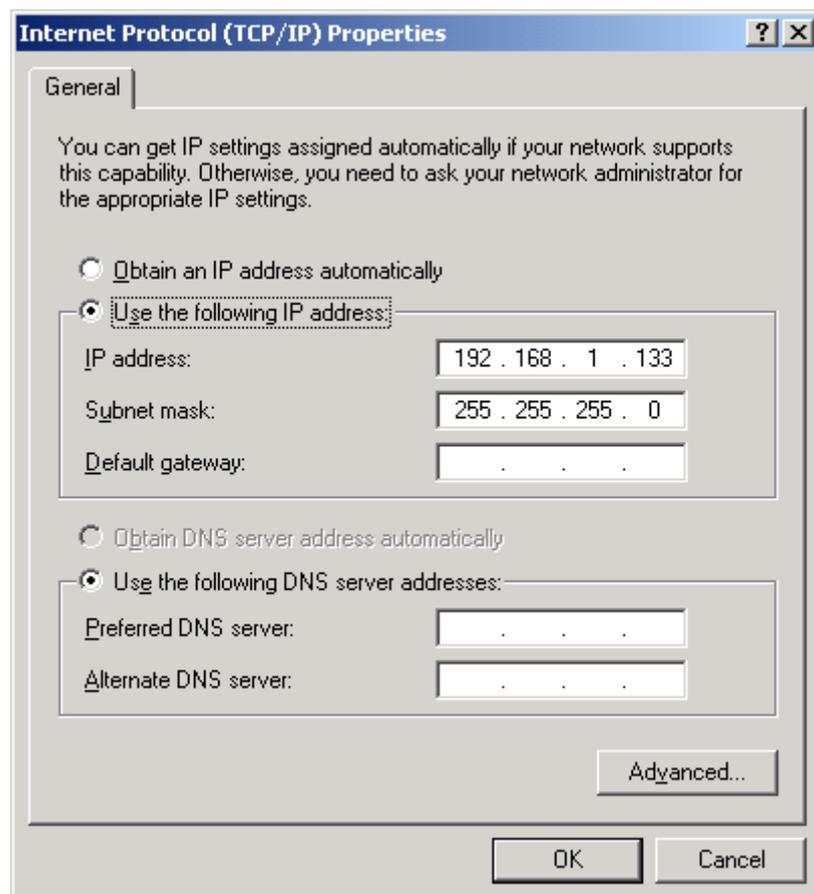


Shown below for your reference is the manual method.

The default IP address of the CT-6382T (LAN port) is 192.168.1.1. To configure the CT-6382T for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

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

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



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

STEP 4: Start your Internet browser with the default IP address 192.168.1.1.

3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-6382T. To log on to the system from the Web browser, follow the steps below:

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

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



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm: DSL Router

User Name: root

Password: *****

Save this password in your password list

OK Cancel

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



COMTREND ADSL Router

Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management

Quick Setup

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

ATM PVC Configuration

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

DSL Auto-connect

3.3 Default Settings

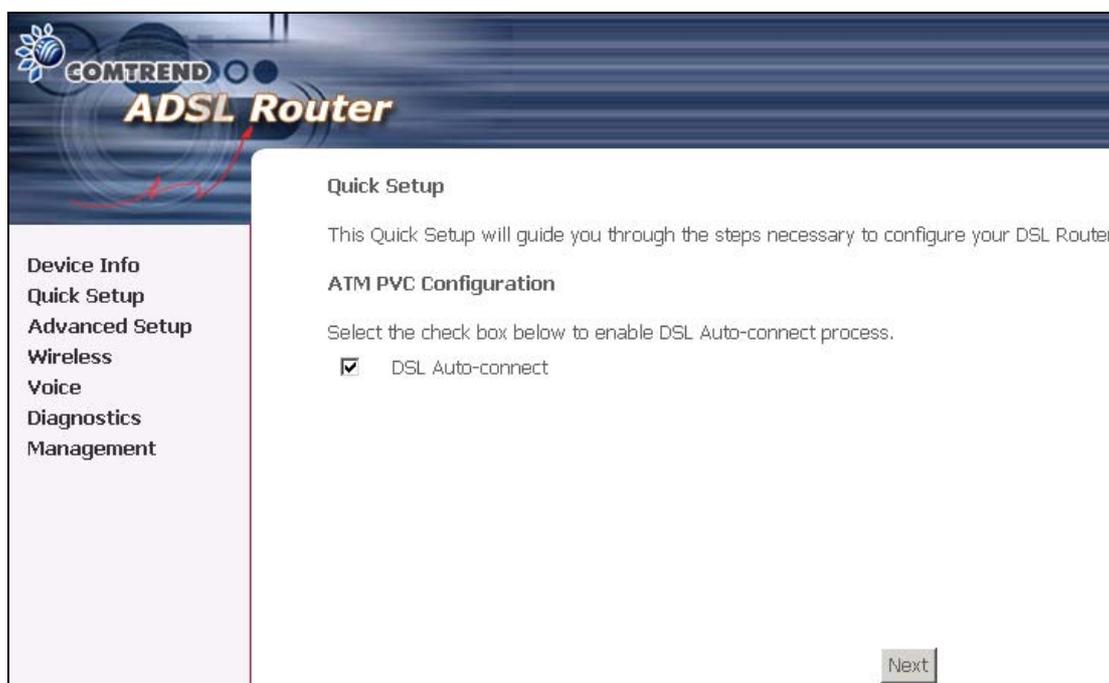
During power on initialization, the CT-6382T initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section on the flash memory. The default attributes are overridden when identical attributes with different values are configured. The configuration profile in Permanent Storage can be created via the Web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking, or by clicking the Restore Default Configuration option in the Restore Settings screen.

The following default settings are present when setting up the VoIP IAD for the first time. The PC running the browser can be attached to the Ethernet.

- LAN port IP address: 192.168.1.1
- Local administrator account name: root
- Local administrator account password: 12345
- Remote WAN access: disabled
- NAT and firewall: enabled
- DHCP server on LAN interface: enabled
- WAN IP address: none

Chapter 4 Device Information

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



Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

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

Shown on the next page for your reference, the **Device Info** screen.



Device Info

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- Quick Setup
- Advanced Setup
- Wireless
- Voice
- Diagnostics
- Management

Device Info

Board ID:	CT6382T-1
Software Version:	E111-S306CTL-C03_R01
Bootloader (CFE) Version:	1.0.37-6.8
Wireless Driver Version:	3.131.35.0.cpe2.3
ADSL Version:	A2pB022c.d20c

This information reflects the current status of your DSL connection.

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

This information reflects the current status of your VoIP connection.

Phone 1 Current Status:	Direct Mode
Phone 2 Current Status:	Direct Mode

4.1 WAN

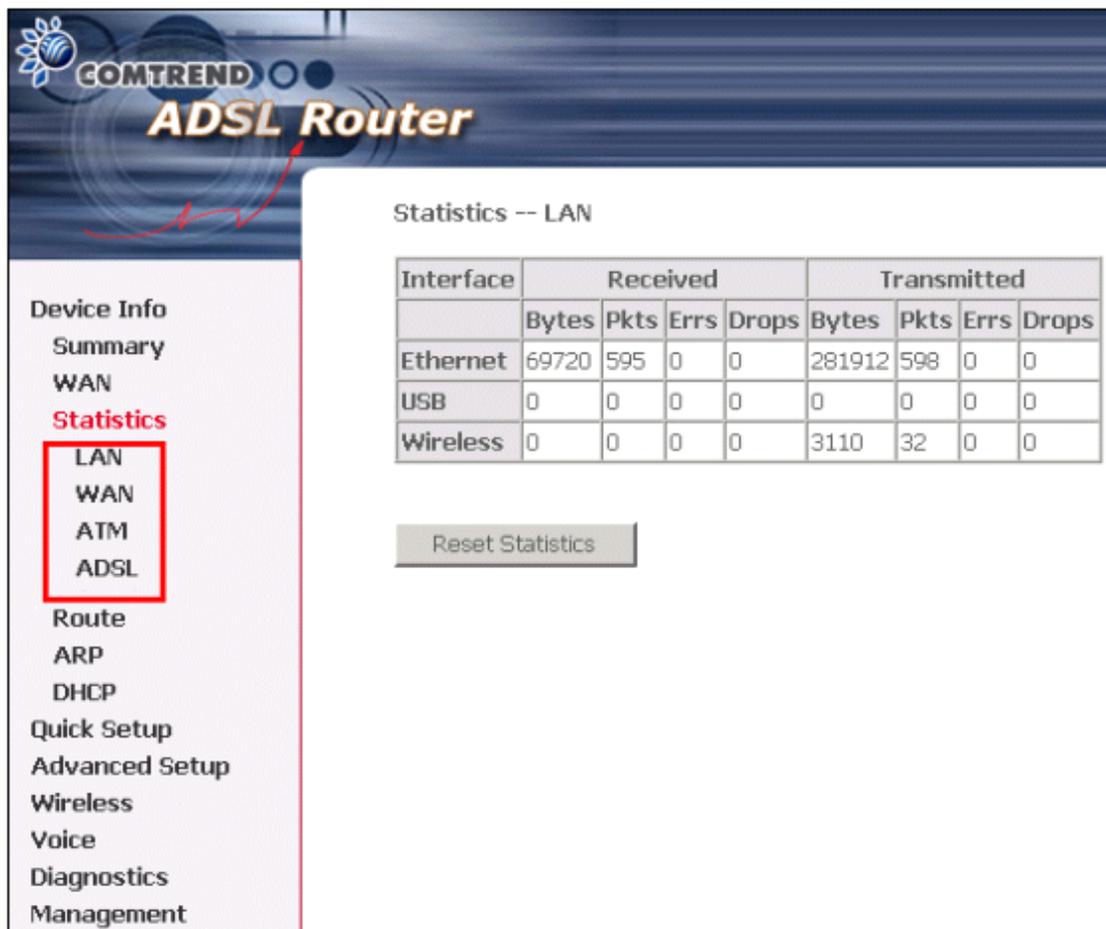
Click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Igmp	Shows the status of the IGMP Proxy function
QoS	Shows if IP QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link and Wan status (ex: PPP up/Down or Authentication Failure)
IP Address	Shows IP address for WAN interface

4.2 Statistics

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



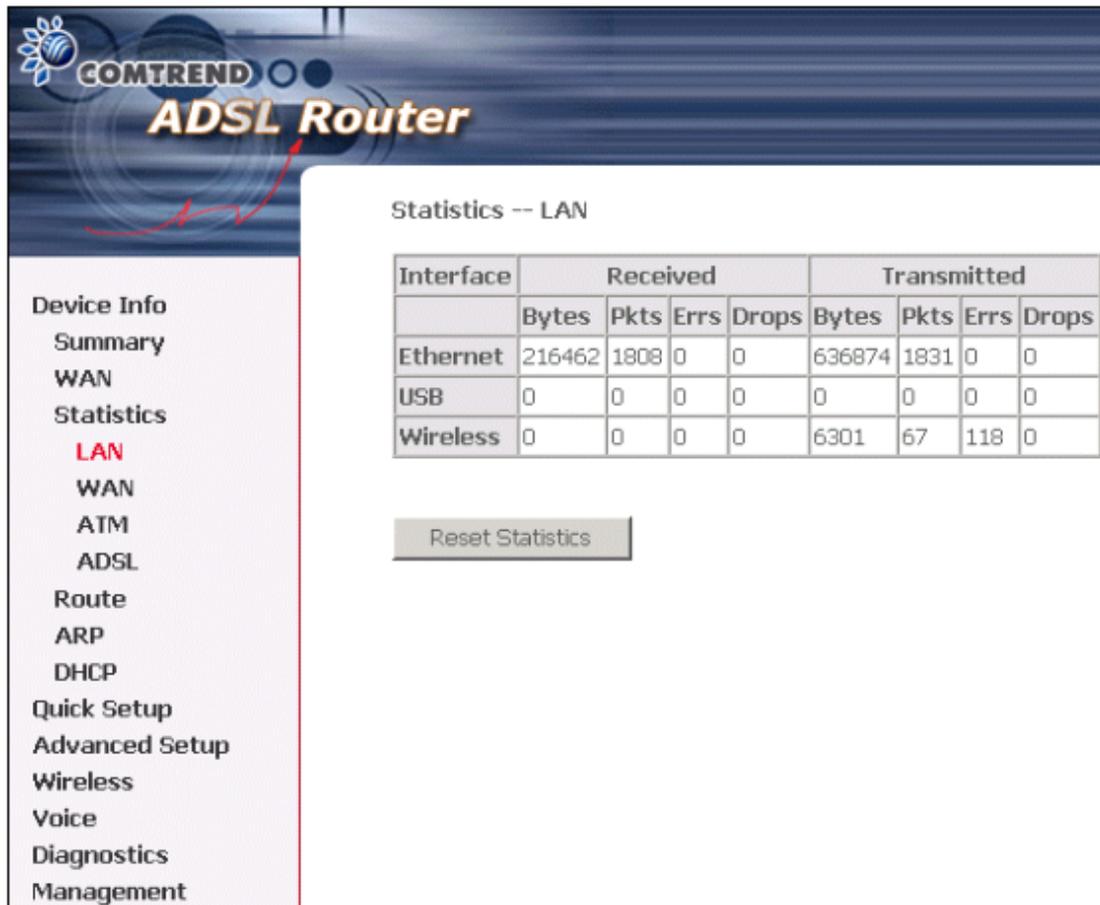
The screenshot displays the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". The left sidebar contains a navigation menu with the following items: Device Info, Summary, WAN, Statistics, LAN, WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The "LAN" item is highlighted with a red box. The main content area is titled "Statistics -- LAN" and contains a table with the following data:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	69720	595	0	0	281912	598	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	3110	32	0	0

Below the table is a "Reset Statistics" button.

4.2.1 LAN Statistics

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



COMTREND
ADSL Router

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

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	216462	1808	0	0	636874	1831	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	6301	67	118	0

Reset Statistics

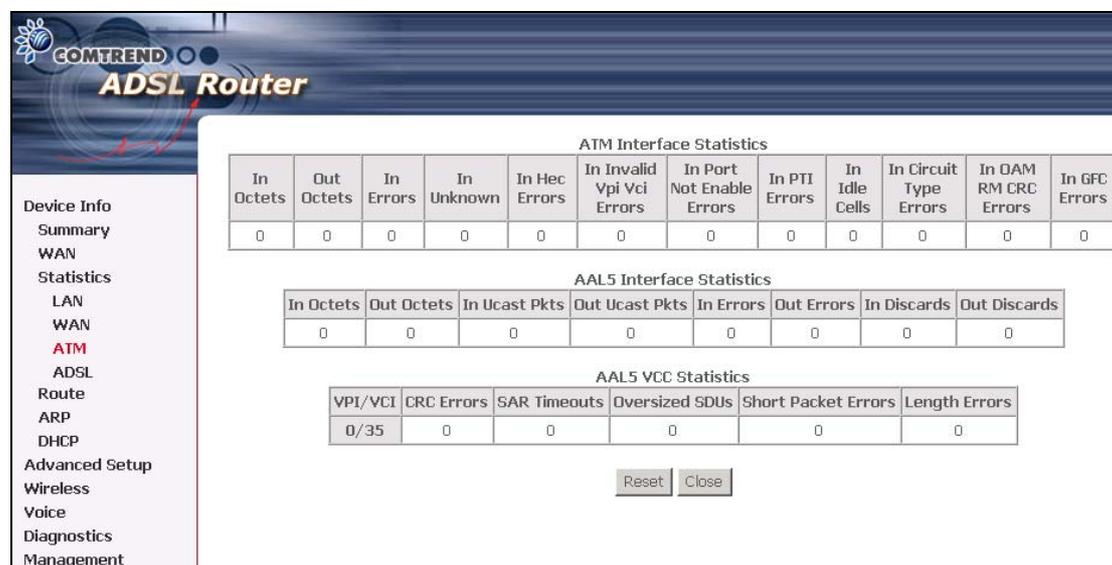
4.2.2 WAN Statistics

The screenshot shows the Comtrend ADSL Router web interface. The main content area is titled "Statistics -- WAN" and contains a table with the following columns: Service, VPI/VCI, Protocol, Interface, Received (Bytes, Pkts, Errs, Drops), and Transmitted (Bytes, Pkts, Errs, Drops). Below the table is a "Reset Statistics" button. The left navigation menu includes options like Device Info, Summary, WAN, Statistics, LAN, WAN (highlighted), ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management.

Service	Shows the service type, as configured by the administrator
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.
Received/Transmitted	<ul style="list-style-type: none"> - Bytes Rx/TX (receive/transmit) packet in Byte - Pkts Rx/TX (receive/transmit) packets - Errs Rx/TX (receive/transmit) the packets which are errors, - Drops Rx/TX (receive/transmit) the packets which are dropped

4.2.3 ATM statistics

The following figure shows the ATM statistics screen.



ATM Interface Statistics

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

ATM AAL5 Layer Statistics over ADSL interface

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

ATM AAL5 LAYER STATISTICS FOR EACH VCC OVER ADSL INTERFACE

Field	Descriptions
CRC Errors	Number of PDUs received with CRC-32 errors
SAR TimeOuts	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packets Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

4.2.4 ADSL Statistics

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

COMTREND ADSL Router

Statistics -- ADSL

Mode:

Type:

Line Coding:

Status: Link Down

Link Power State: LO

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

ADSL BER Test Reset Statistics

Field	Description
Mode	Modulation protocol T1.413, G.lite, G.DMT, ADSL2 or ADSL2+
Type	Channel type Interleave or Fast
Line Coding	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, Annex L and Annex M
Status	Lists the status of the DSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

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

COMTREND ADSL Router

Statistics -- ADSL

Mode:	ADSL2+	
Line Coding:	Trellis On	
Status:	No Defect	
Link Power State:	LO	
	Downstream	Upstream
SNR Margin (dB):	7.4	6.0
Attenuation (dB):	2.5	1.6
Output Power (dBm):	12.7	12.4
Attainable Rate (Kbps):	25896	1
Rate (Kbps):	24040	1203
MSGc (number of bytes in overhead channel message):	57	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):	0.3390	1.9802
L (number of bits in PMD Data Frame):	6018	303
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	3757	3689
Super Frame Errors:	0	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
DCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	3433715	0
Data Cells:	56	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	68	0

ADSL BER Test Reset Statistics

The extra items are explained here.

MSGc (number of bytes in overhead channel message)	65	14
B (number of bytes in Mux Data Frame)	254	13
M (number of Mux Data Frames in FEC Data Frame)	1	16
T (Max Data Frames over sync bytes)	3	9
R (number of check bytes in FEC Data Frame)	0	8
S (ratio of FEC over PMD Data Frame length)	0.3047	5.9678
L (number of bits in PMD Data Frame)	6695	311
D interleaver depth):	1	8
Delay (msec):	0	11

4.2.5 Route

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

Device Info -- Route

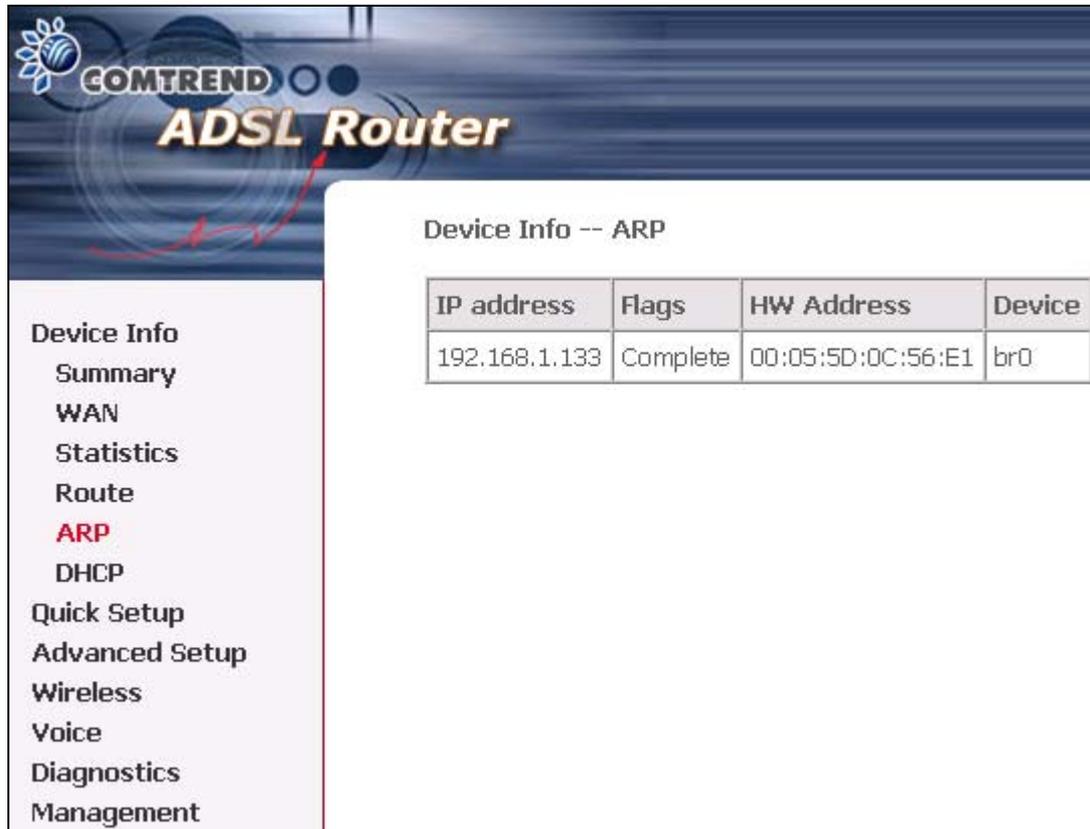
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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

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 name for WAN connection
Interface	Shows connection interfaces

4.2.6 ARP

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

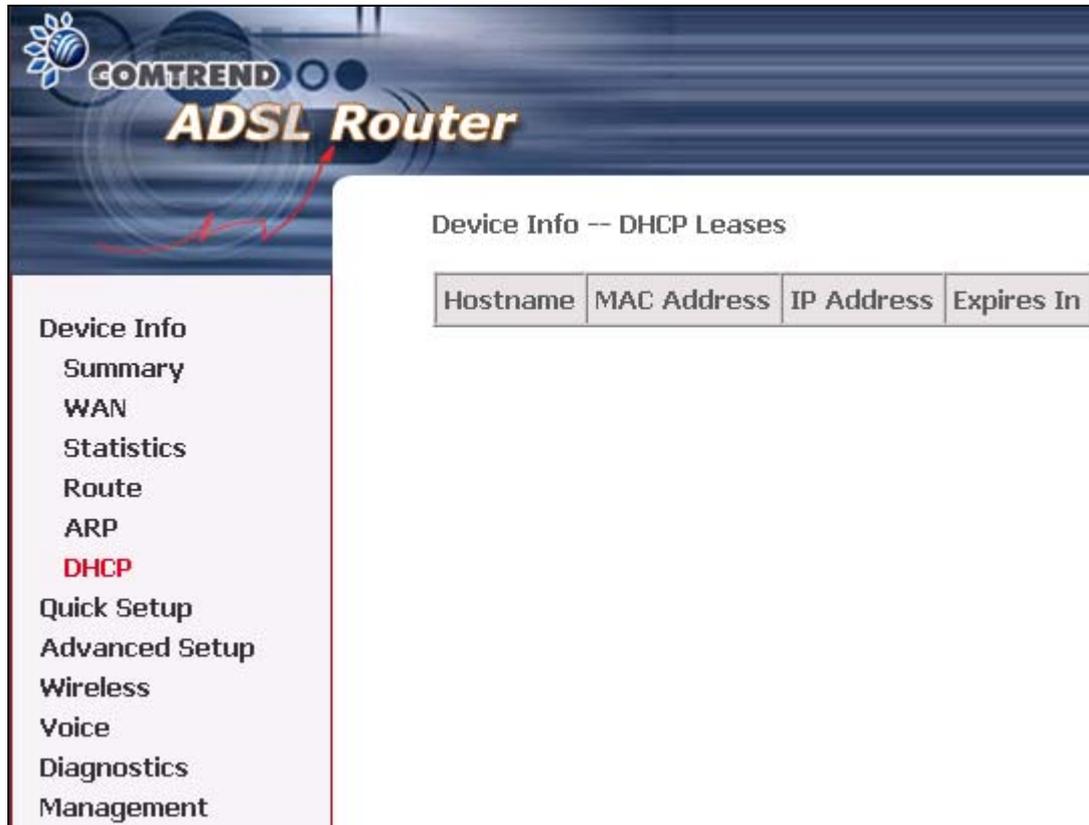


The screenshot displays the web management interface of a Comtrend ADSL Router. The top banner features the Comtrend logo and the text "ADSL Router". On the left side, there is a vertical navigation menu with the following items: Device Info, Summary, WAN, Statistics, Route, **ARP** (highlighted in red),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

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

4.2.7 DHCP

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



The screenshot displays the Comtrend ADSL Router web interface. The header features the Comtrend logo and the text "ADSL Router". A left-hand navigation menu lists various settings: Device Info, Summary, WAN, Statistics, Route, ARP, **DHCP** (highlighted in red), Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Device Info -- DHCP Leases" and contains a table with the following headers: Hostname, MAC Address, IP Address, and Expires In.

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

Chapter 5 Quick Setup

The Quick Setup option will not be displayed in the menu bar if a WAN is configured. The Quick Setup allows the user to configure the ADSL VoIP IAD for DSL connectivity and Internet access. It also guides the user through the WAN network setup first and then the LAN interface setup. You can either manually customize the VoIP IAD or follow the online instruction to set up the VoIP IAD.

The CT-6382T ADSL VoIP IAD supports the following five network operating modes over an ATM PVC WAN interface.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-6382T is to run the PPPoE client. The CT-6382T can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge. In PPPoE mode, CT-6382T also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client and non-PPPoE LAN devices.
- NAPT and firewall are always enabled when PPPoE /PPPoA mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAPT and firewall are always disabled when Bridge mode is selected.

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

5.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL VoIP IAD will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

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



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

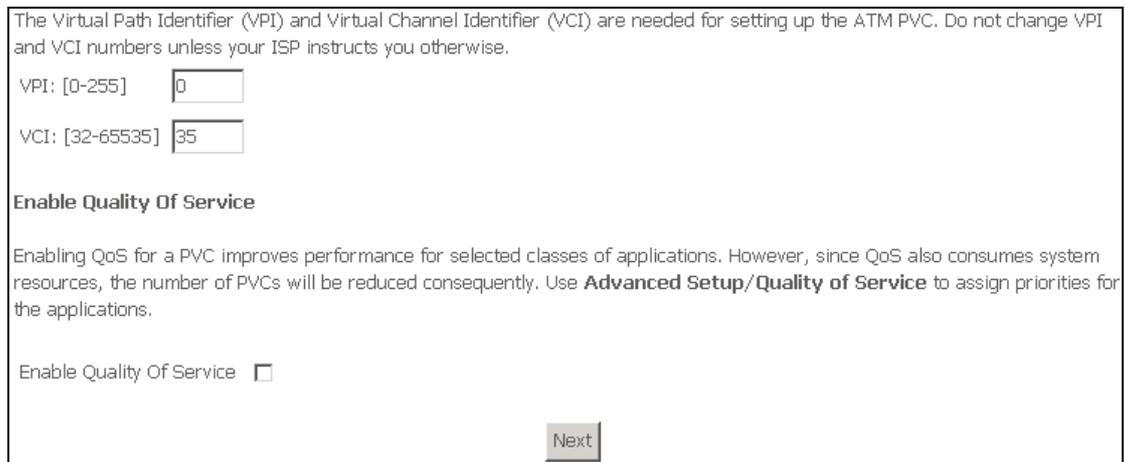
5.2 Manual Quick Setup

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



The screenshot shows the 'Quick Setup' page for a Comtrend ADSL Router. On the left is a navigation menu with 'Quick Setup' highlighted. The main content area is titled 'Quick Setup' and contains instructions. Under 'ATM PVC Configuration', there is a checkbox labeled 'DSL Auto-connect' which is currently checked. A red circle highlights this checkbox, and an arrow points from a yellow callout box below to it.

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



This screenshot shows the configuration screen for VPI and VCI. It includes a text block explaining that these values are needed for ATM PVC setup and should not be changed unless instructed by the ISP. Below this, there are two input fields: 'VPI: [0-255]' with the value '0' and 'VCI: [32-65535]' with the value '35'. A section titled 'Enable Quality Of Service' contains a paragraph explaining that enabling QoS improves performance but reduces the number of PVCs. At the bottom of this section, the 'Enable Quality Of Service' checkbox is unchecked. A 'Next' button is located at the bottom right of the page.

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

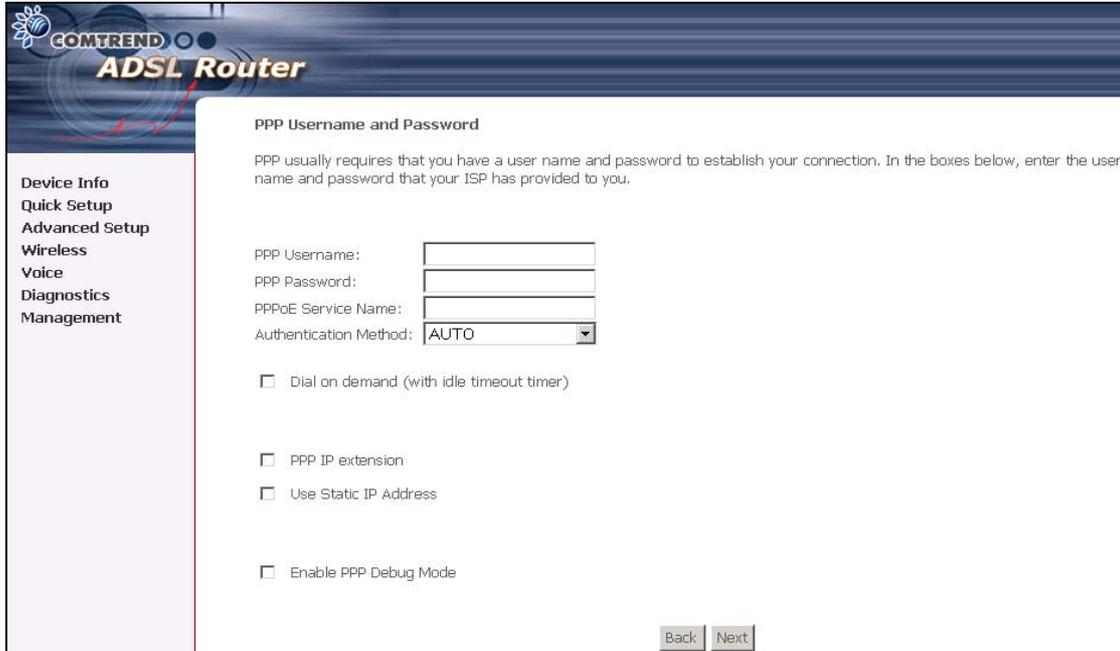
STEP 3: Then, choose the Encapsulation mode. Select **Enable 802.1q** (by ticking the box) if required, and input a number for the VLAN ID. Click Next.

The screenshot shows the Comtrend ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'Connection Type' and includes a note: 'Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.' There are five radio button options: 'PPP over ATM (PPPoA)', 'PPP over Ethernet (PPPoE)', 'MAC Encapsulation Routing (MER)', 'IP over ATM (IPoA)', and 'Bridging' (which is selected). Below this is the 'Encapsulation Mode' dropdown menu, currently set to 'LLC/SNAP-BRIDGING'. At the bottom, there is a checkbox for 'Enable 802.1q' which is currently unchecked. A red arrow points from this checkbox to a zoomed-in view of the checkbox and the 'VLAN ID[0-4095]:' input field below it. The zoomed-in view shows the 'Enable 802.1q' checkbox checked and the 'VLAN ID' field empty. Both screenshots have 'Back' and 'Next' buttons at the bottom right.

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

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

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



The screenshot shows the configuration page for a COMTREND ADSL Router. The page title is "COMTREND ADSL Router". On the left side, there is a navigation menu with the following items: "Device Info", "Quick Setup", "Advanced Setup", "Wireless", "Voice", "Diagnostics", and "Management". The main content area is titled "PPP Username and Password". It contains the following text: "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." Below this text are four input fields: "PPP Username:", "PPP Password:", "PPPoE Service Name:", and "Authentication Method:" (with a dropdown menu showing "AUTO"). There are also four checkboxes: "Dial on demand (with idle timeout timer)", "PPP IP extension", "Use Static IP Address", and "Enable PPP Debug Mode". At the bottom right of the page, there are "Back" and "Next" buttons.

PPP Username/PPP Password

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

PPPoE service name

For PPPoE service, PADI requests contain a service name-tag. Some PPPoE servers (or BRAS) of ISP check this service name-tag for connection.

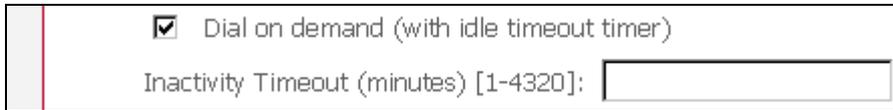
Encapsulation Mode

Choosing different connection types provides different encapsulation modes.

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

Disconnect if no activity

The CT-6382T can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



The screenshot shows a configuration window with a checked checkbox labeled "Dial on demand (with idle timeout timer)". Below it is a text input field labeled "Inactivity Timeout (minutes) [1-4320]:".

PPP IP Extension

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

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL VoIP IAD has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL VoIP IAD becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL VoIP IAD extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL VoIP IAD bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the VoIP IAD's LAN IP address.

Use Static IP Address

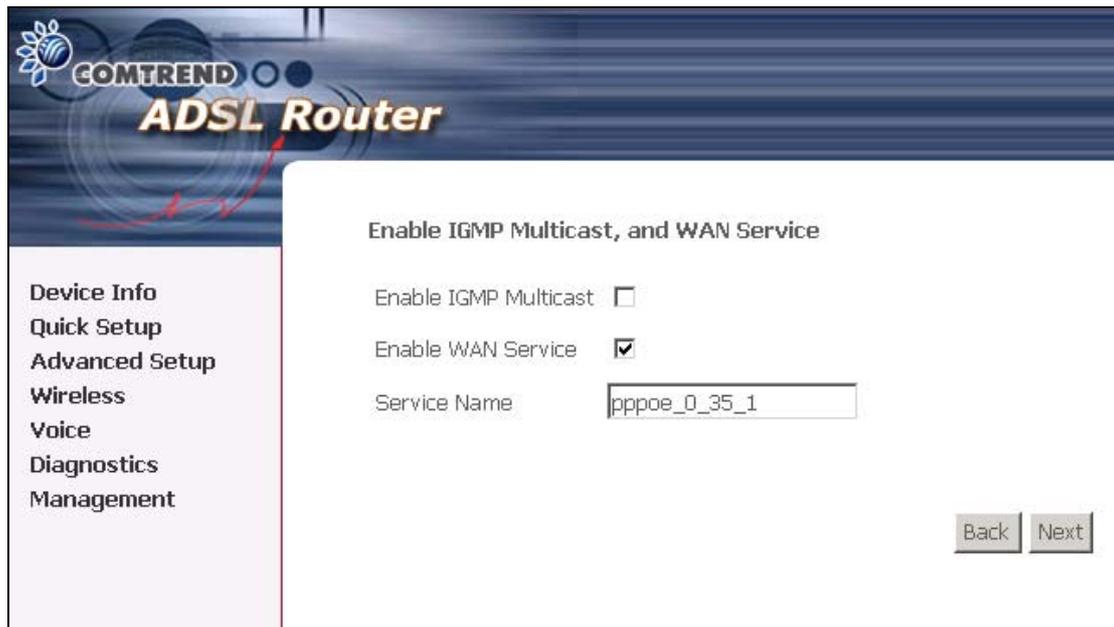
Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

Enable PPP Debug Mode

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

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



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

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

Service Name: This is user-defined.

3. After entering your settings, select **Next**.

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

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

COMTREND
ADSL Router

Device Setup

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

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

Back Next

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

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

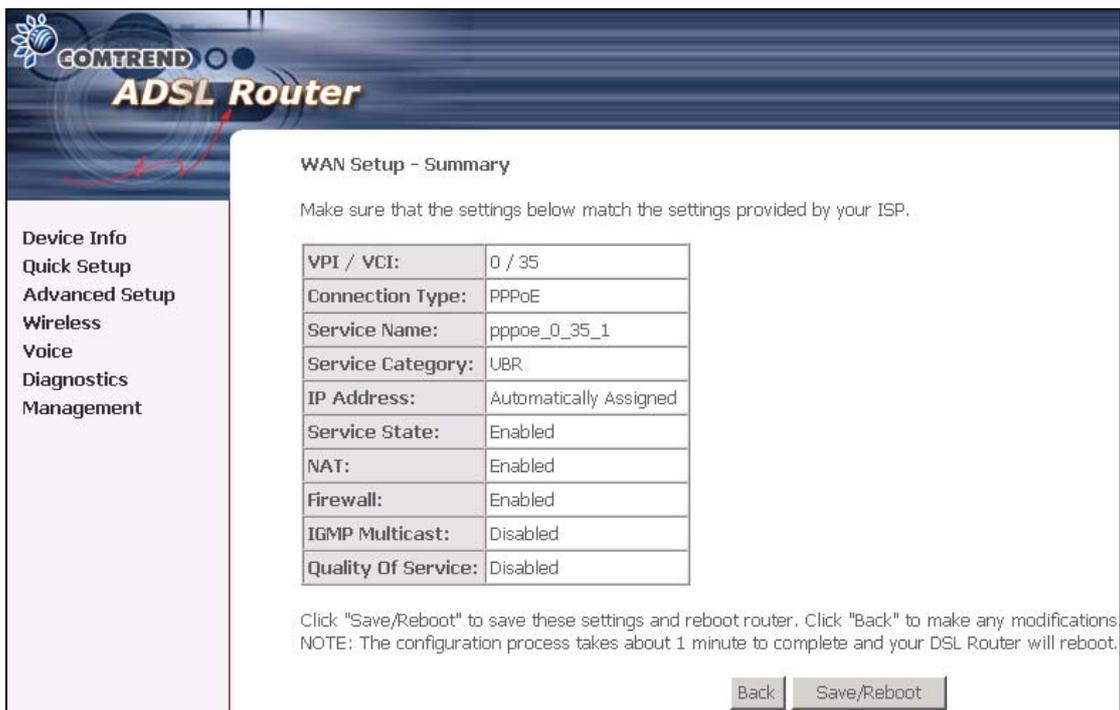
Subnet Mask:

4. Click Next and the screen below will be displayed.

5. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.



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

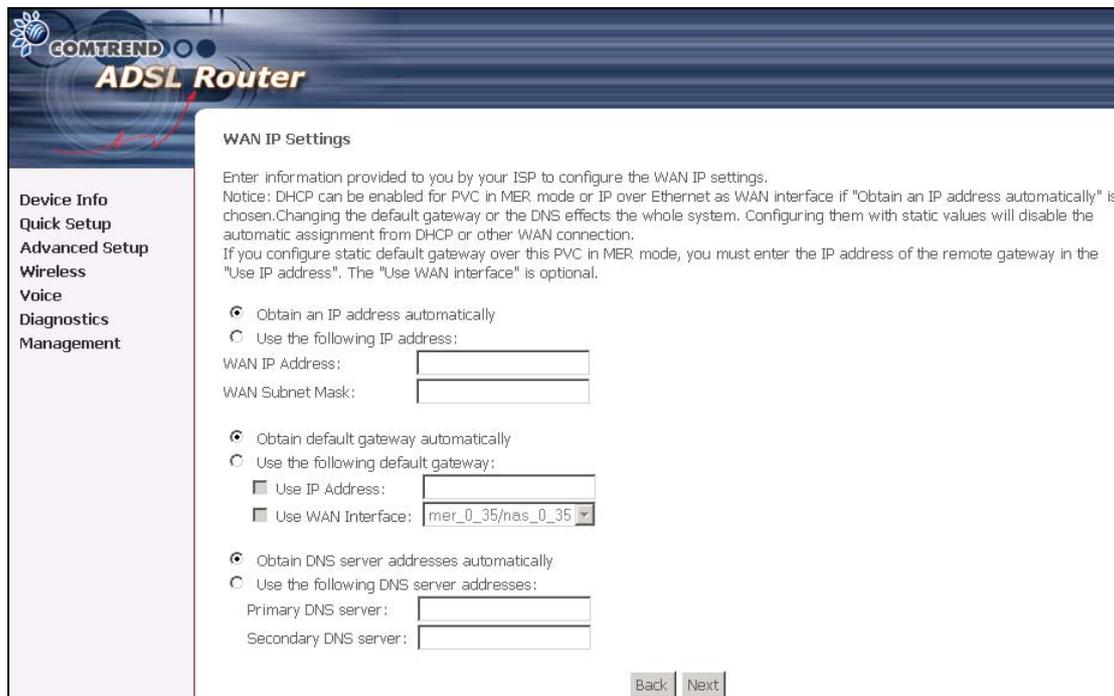


7. After clicking **Save/Reboot**, the VoIP IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382T is ready for operation and the LEDs display as described in the LED description tables.

5.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

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



The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a dark blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'WAN IP Settings' and contains the following text: 'Enter information provided to you by your ISP to configure the WAN IP settings. 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.'

The configuration options are:

- Obtain an IP address automatically
- Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
- Obtain default gateway automatically
- Use the following default gateway:
 - Use IP Address:
 - Use WAN Interface: mer_0_35/nas_0_35
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

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

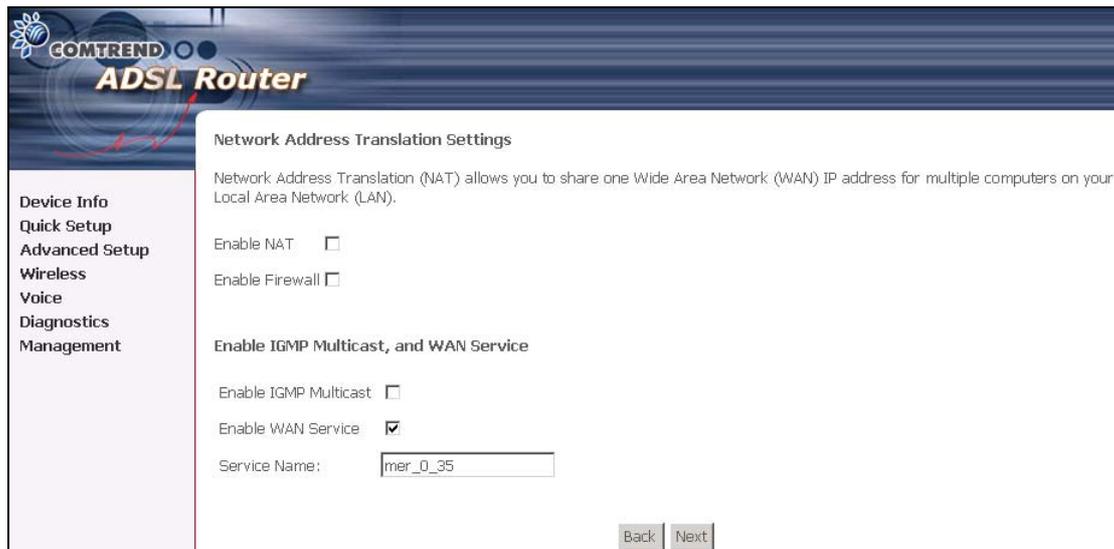
Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

The ISP should provide the values that must be entered in the entry fields.

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



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

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

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

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

Service Name: This is User-defined.

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

COMTREND
ADSL Router

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

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Enable DHCP Server Relay

DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

Back Next

Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management

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

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

Note: The Ethernet interface (and the wireless LAN interface on the CT-6382T) share the same subnet since they are bridged within the IAD.

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

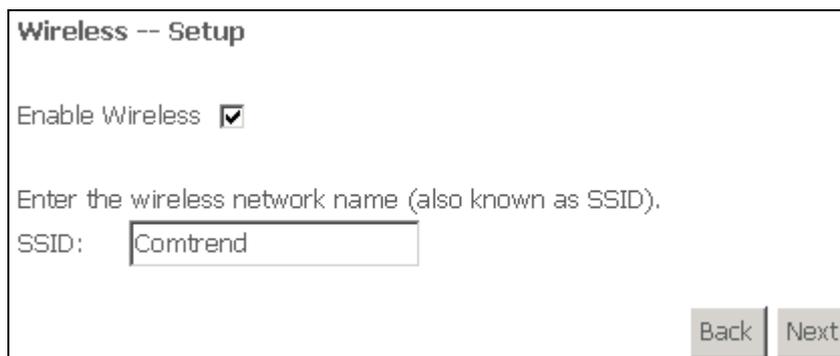
To configure a secondary IP address for the LAN port, click the box as shown below.



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

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

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



Wireless -- Setup

Enable Wireless

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

The following screen will be displayed.

COMTREND
ADSL Router

WAN Setup - Summary

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

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

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

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

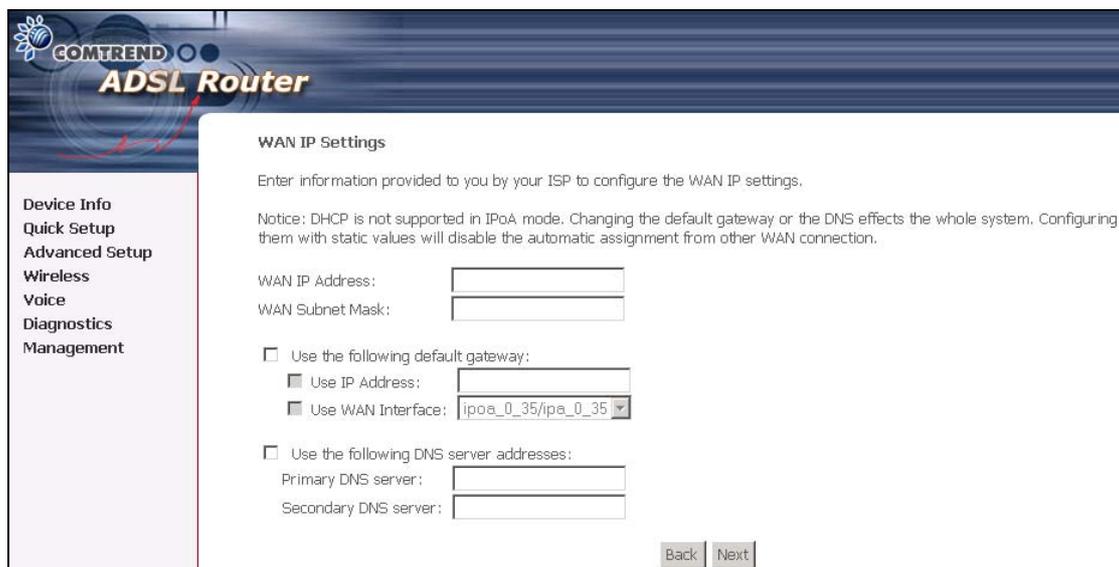
Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management

8. After clicking **Save/Reboot**, the IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382T is ready for operation and the LEDs display as described in the LED description tables.

5.2.3 IP Over ATM

To configure IP Over ATM,

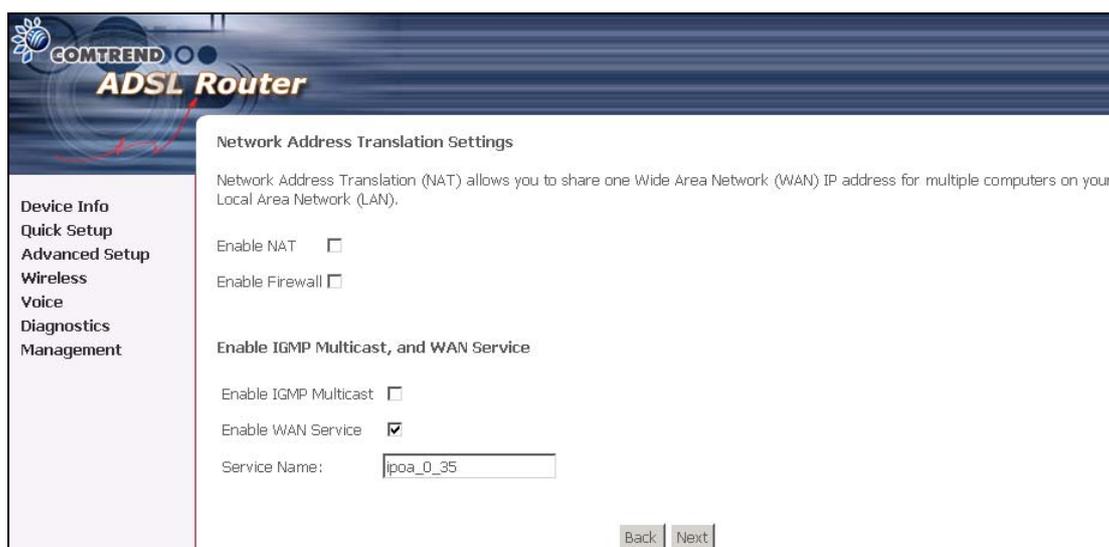
1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**. The following screen appears.



The screenshot shows the WAN IP Settings configuration page for a Comtrend ADSL Router. The page has a dark blue header with the Comtrend logo and 'ADSL Router' text. On the left, there is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'WAN IP Settings' and contains the following text: 'Enter information provided to you by your ISP to configure the WAN IP settings.' Below this is a notice: 'Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.' The form includes several input fields: 'WAN IP Address', 'WAN Subnet Mask', 'Use IP Address' (checkbox), 'Use WAN Interface' (checkbox with a dropdown menu showing 'ipoa_0_35/ipa_0_35'), 'Use the following DNS server addresses' (checkbox), 'Primary DNS server', and 'Secondary DNS server'. At the bottom right, there are 'Back' and 'Next' buttons.

Notice that **Obtain an IP address automatically** (DHCP client) is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup, and the DNS server addresses provided by the ISP.

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



Enable NAT checkbox

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

Enable Firewall checkbox

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

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

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

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

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

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

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

Wireless -- Setup

Enable Wireless

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

SSID:

Back Next

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

COMTREND ADSL Router

WAN Setup - Summary

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

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

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

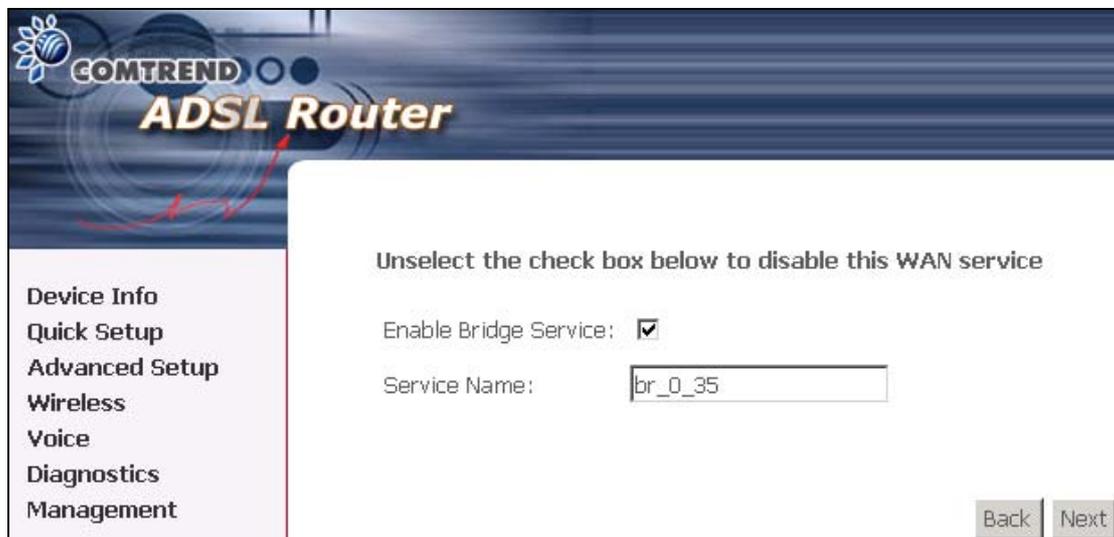
Back Save/Reboot

9. After clicking **Save/Reboot**, the IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382T is ready for operation and the LEDs display as described in the LED description tables.

5.2.4 Bridging

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

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

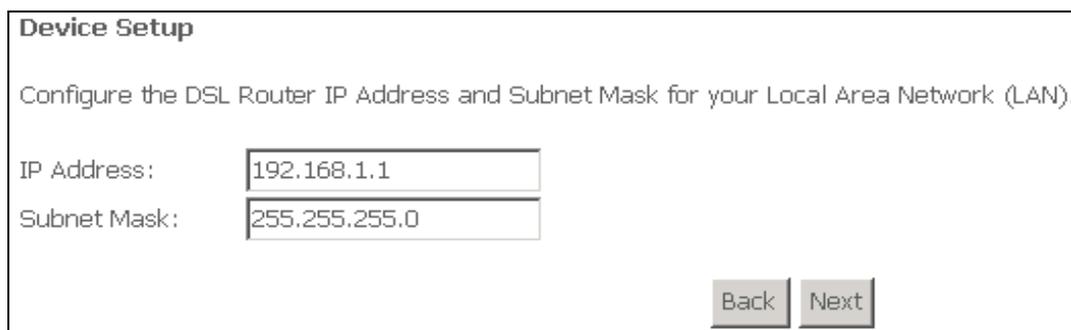


The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main area displays the following configuration options:

- Unselect the check box below to disable this WAN service
- Enable Bridge Service:
- Service Name:

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

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



The screenshot shows the 'Device Setup' configuration screen. The title is 'Device Setup'. Below the title, it says 'Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN)'. The configuration options are:

- IP Address:
- Subnet Mask:

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

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

Wireless -- Setup

Enable Wireless

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

SSID:

The following screen will be displayed.

COMTREND ADSL Router

WAN Setup - Summary

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

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

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

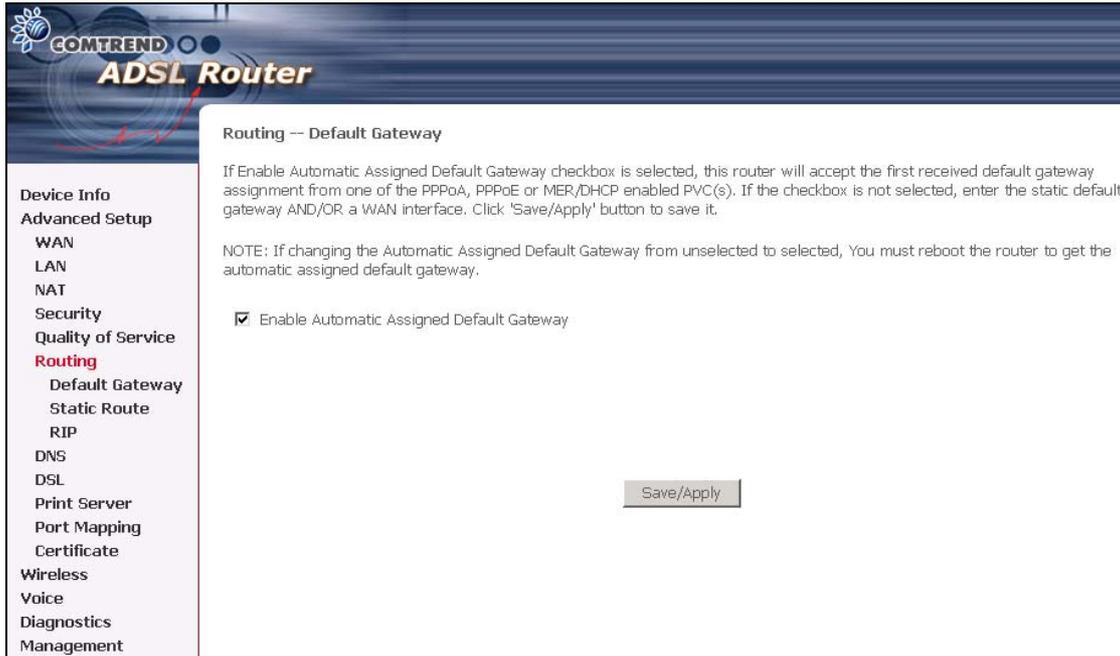
Device Info
Quick Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management

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

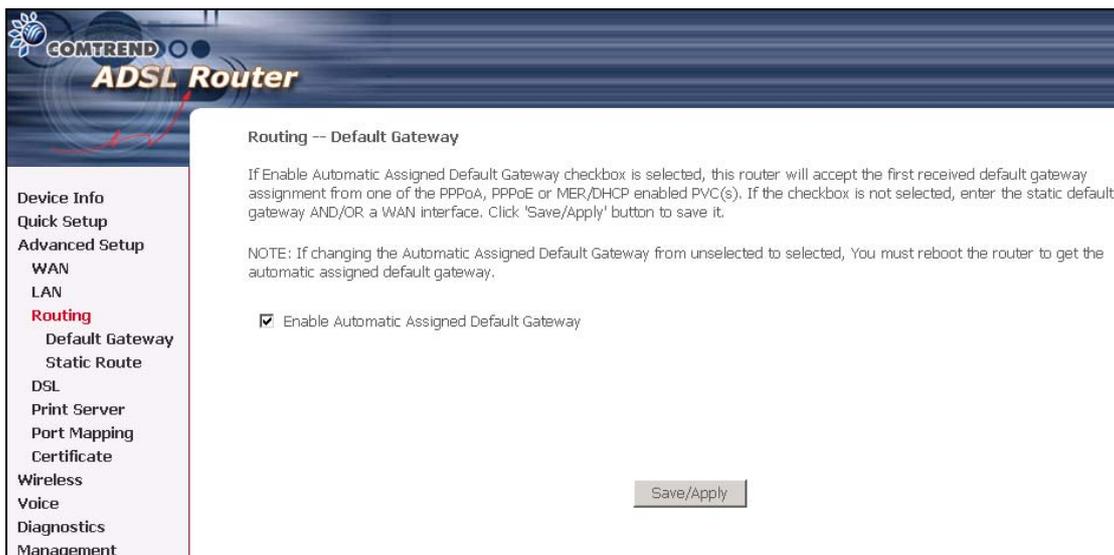
Chapter 6 Advanced Setup

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

Note: Shown below for your reference are the available menu options for each different configuration.



This screenshot is for Mer and IPoA encapsulations.



This screenshot is for PPPoE and PPPoA encapsulations.

COMTREND
ADSL Router

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

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

Choose Add or Remove to configure MAC filtering rules.

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

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

This screenshot is for Bridged encapsulation.

6.1 WAN

Wide Area Network (WAN) Setup

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

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Save/Reboot"/>											

VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR...
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows bridge or router mode
Igmp	Shows enable or disable IGMP proxy
QoS	Shows enable or disable QoS
State	Shows enable or disable WAN connection
VlanId	VLAN ID is the identification of the VLAN, which is basically used by the IEEE - 802.1Q

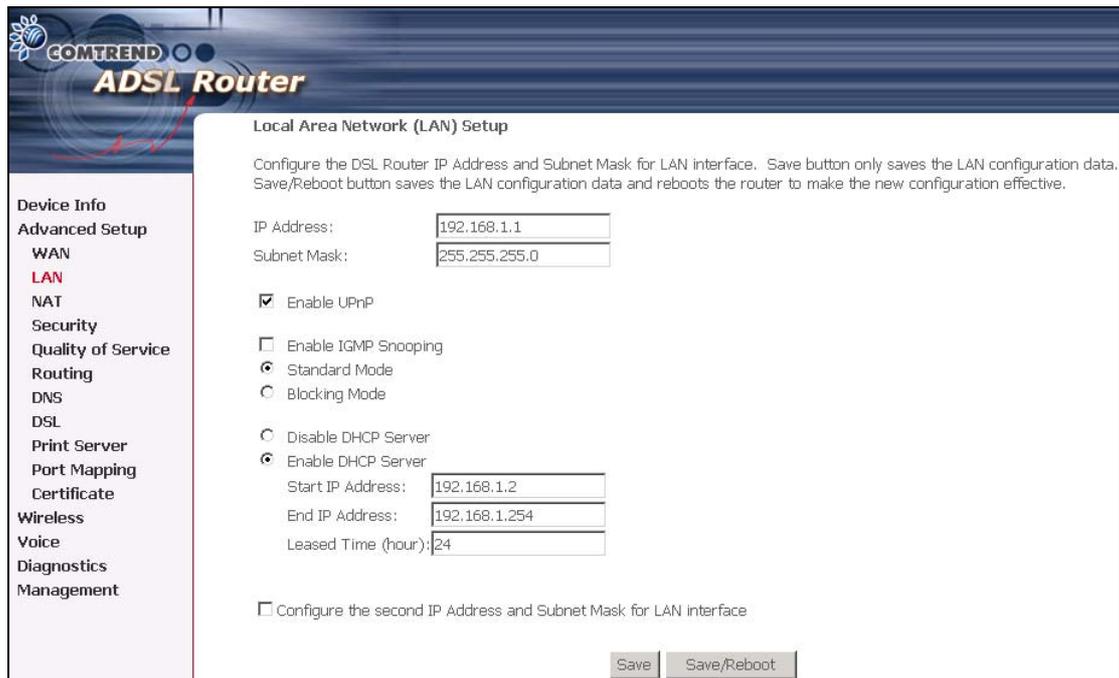
For further information on WAN please reference section: 4.1, Page 17.

6.2 LAN

Configure the VoIP IAD 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 IAD to make the new configuration effective.

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

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



The screenshot shows the 'Local Area Network (LAN) Setup' configuration page for a GOMTREND ADSL Router. The page includes a navigation menu on the left with options like Device Info, Advanced Setup, WAN, LAN (highlighted), NAT, Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area contains the following configuration options:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Enable UPnP
- Enable IGMP Snooping
- Standard Mode
- Blocking Mode
- Disable DHCP Server
- Enable DHCP Server
- Start IP Address: 192.168.1.2
- End IP Address: 192.168.1.254
- Leased Time (hour): 24
- Configure the second IP Address and Subnet Mask for LAN interface

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

Enable UPnP: Tick the box to enable.

Note: This option will not display in Bridge mode or if no PVC is configured.

Enable IGMP Snooping: Enable IGMP Snooping function by ticking the box.

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

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there is no client subscription to any multicast group. To configure a secondary IP address for the LAN port, click the box as shown below.

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

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

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

6.3 NAT

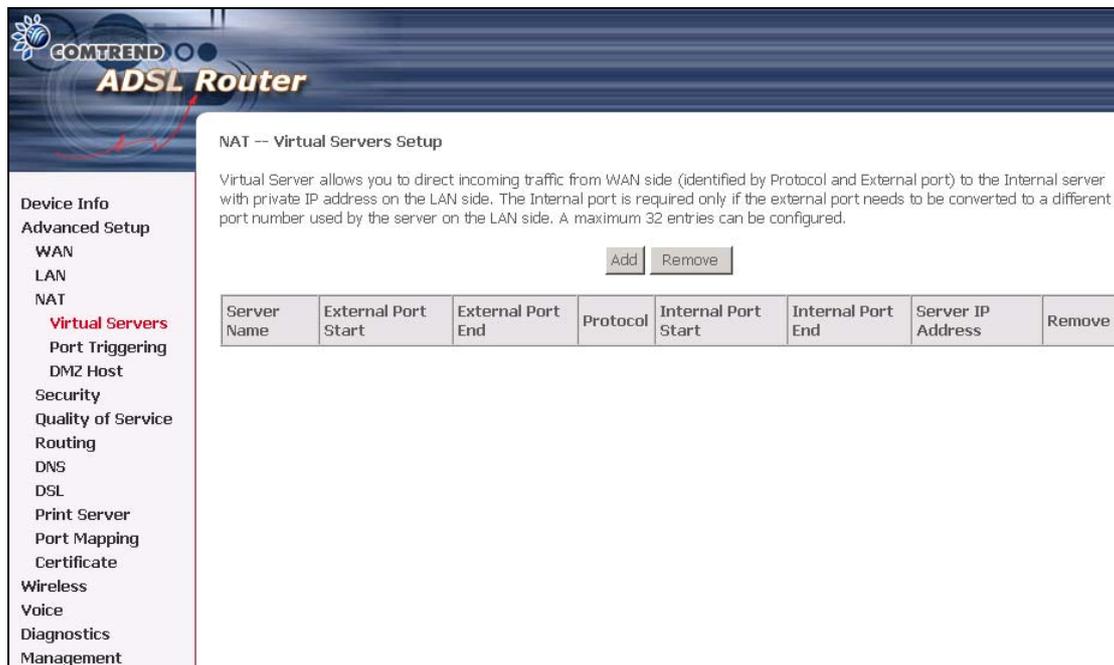
Note: This option is not available for bridge mode.

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

6.3.1 Virtual Servers

Note: This option is not available for Bridge mode.

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.



COMTREND ADSL Router

NAT -- Virtual Servers Setup

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

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

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

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

6.3.2 Port Triggering

Note: This option is not available for Bridge mode.

Some applications require that specific ports in the IAD'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 IAD 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.

COMTREND ADSL Router

NAT -- Port Triggering Setup

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

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

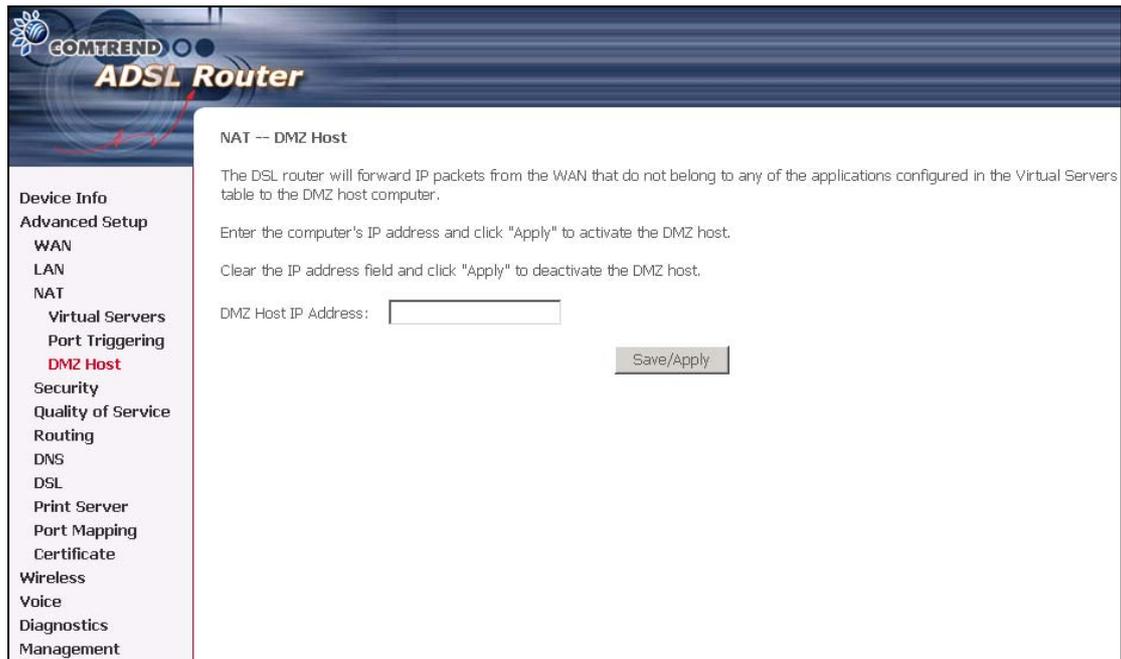
To add a Trigger Port, simply click the Add button. The following will be displayed.

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

6.3.3 DMZ Host

Note: This option is not available for Bridge mode.

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



The screenshot shows the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Virtual Servers, Port Triggering, DMZ Host (highlighted in red), Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled "NAT -- DMZ Host" and contains the following text: "The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer." Below this, there are two instructions: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." A text input field labeled "DMZ Host IP Address:" is present, followed by a "Save/Apply" button.

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

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

6.4 Security

6.4.1 MAC Filtering

Mac Filtering is only available for Bridged mode.

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

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

COMTREND
ADSL Router

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

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

[Change Policy](#)

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

Choose Add or Remove to configure MAC filtering rules.

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

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

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

COMTREND ADSL Router

Add MAC Filter

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Select All

br_0_35/nas_0_35

Option	Description
Protocol type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Define the destination MAC address
Source MAC Address	Define the source MAC address
Frame Direction	Select the incoming/outgoing packet interface

6.4.2 Parental Control

Daytime Parental Control

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

COMTREND ADSL Router

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

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

Add Remove

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

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

COMTREND ADSL Router

Time of Day Restriction

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

User Name

Browser's MAC Address: 00:05:5D:0C:56:E1
 Other MAC Address:
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>						

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Save/Apply

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

Click Save/Apply to enforce the settings.

User Name: Name of the Filter.

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

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

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

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

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

6.4.3 IP Filtering

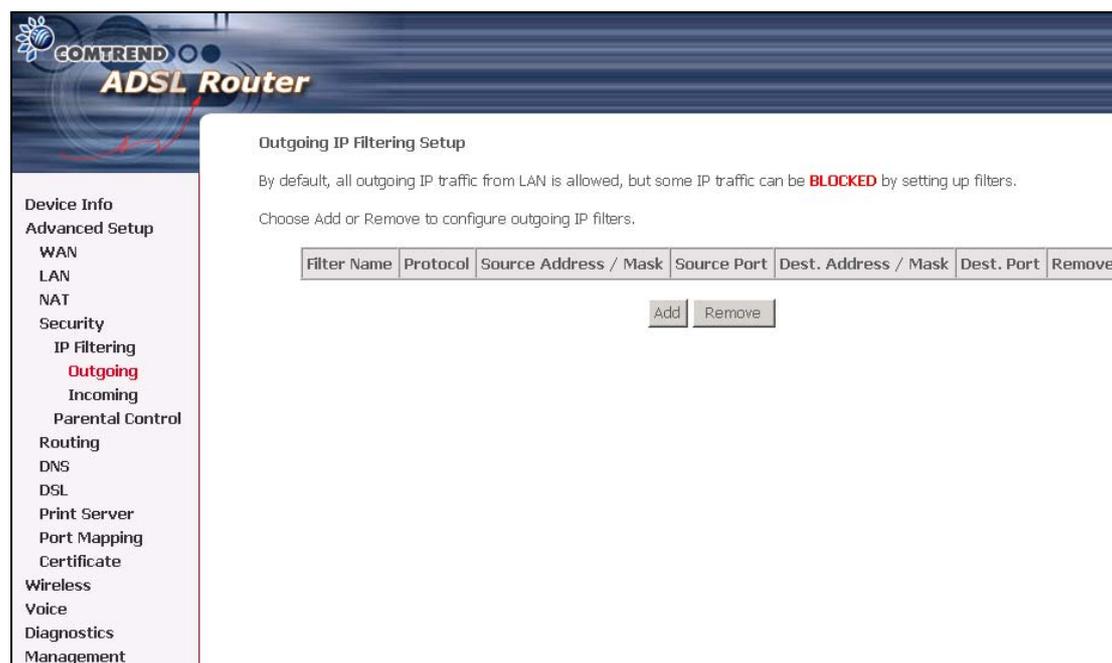
This option is not available for bridge mode.

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

Note: After you enable the "Firewall", you can set the "IP filter". If firewall is disabled, you cannot set the IP filter.

Outgoing

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



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

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

COMTREND ADSL Router

Add IP Filter -- Outgoing

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Device Info
Advanced Setup
 WAN
 LAN
 NAT
Security
 IP Filtering
 Outgoing
 Incoming
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 Print Server
 Port Mapping
 Certificate
 Wireless
 Voice
 Diagnostics
 Management

Filter Name	Type a name for the filter rule.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or port 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 port range.

Incoming

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

The screenshot shows the 'Incoming IP Filtering Setup' page. The left sidebar contains a navigation menu with 'Incoming' highlighted. The main content area has a title 'Incoming IP Filtering Setup' and a paragraph explaining that incoming IP traffic is blocked by default but can be accepted by setting up filters. Below this is a table with columns: Filter Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. There are 'Add' and 'Remove' buttons below the table.

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

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

The screenshot shows the 'Add IP Filter -- Incoming' page. The left sidebar is the same as the previous screenshot. The main content area has a title 'Add IP Filter -- Incoming' and a paragraph explaining that the screen allows creating a filter rule by specifying a new filter name and at least one condition. Below this are several input fields: Filter Name, Protocol (dropdown), Source IP address, Source Subnet Mask, Source Port (port or port:port), Destination IP address, Destination Subnet Mask, and Destination Port (port or port:port). There is a section for 'WAN Interfaces (Configured in Routing mode and with firewall enabled only)' with a checkbox for 'Select All' and a checked checkbox for 'pppoe_0_35_1/ppp_0_35_1'. A 'Save/Apply' button is at the bottom right.

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

6.5 Quality of Service

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

COMTRENDS ADSL Router

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

Differentiated Service Configuration

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

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

COMTREND ADSL Router

Add Network Traffic Class Rule

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

Traffic Class Name:

Enable Differentiated Service Configuration

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

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

Assign ATM Transmit Priority:

Mark IP Precedence:

Mark IP Type Of Service:

Mark 802.1p if 802.1q is enabled on WAN:

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

SET-1

Physical LAN Port:

Protocol:

Source IP Address:

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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

SET-2

802.1p Priority:

Traffic Class Name	Enter name for traffic class.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit shows the higher the priority.
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7. The higher the digit shows the higher the priority.
SET-1	
Physical LAN Port	Select between ENET(1-4), USB, Wireless and Wireless_Guest.
Protocol	User can select from: TCP, TCP/UDP, UDP or ICMP.
Source IP Address	Enter the source IP address.

Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number or port 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 port range.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

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

COMTREND ADSL Router

Add Network Traffic Class Rule

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

Traffic Class Name:

Enable Differentiated Service Configuration

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

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

Assign ATM Transmit Priority:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled on WAN:

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

SET-1

Physical LAN Port:

Protocol:

Source IP Address:

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

SET-2

802.1p Priority:

Save/Apply

The additional Items are explained below.

Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.

6.6 Routing

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

Note: This " RIP " option is not available for Bridge mode.

6.6.1 Default Gateway

If '**Enable Automatic Assigned Default Gateway**' checkbox is selected, this IAD 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.

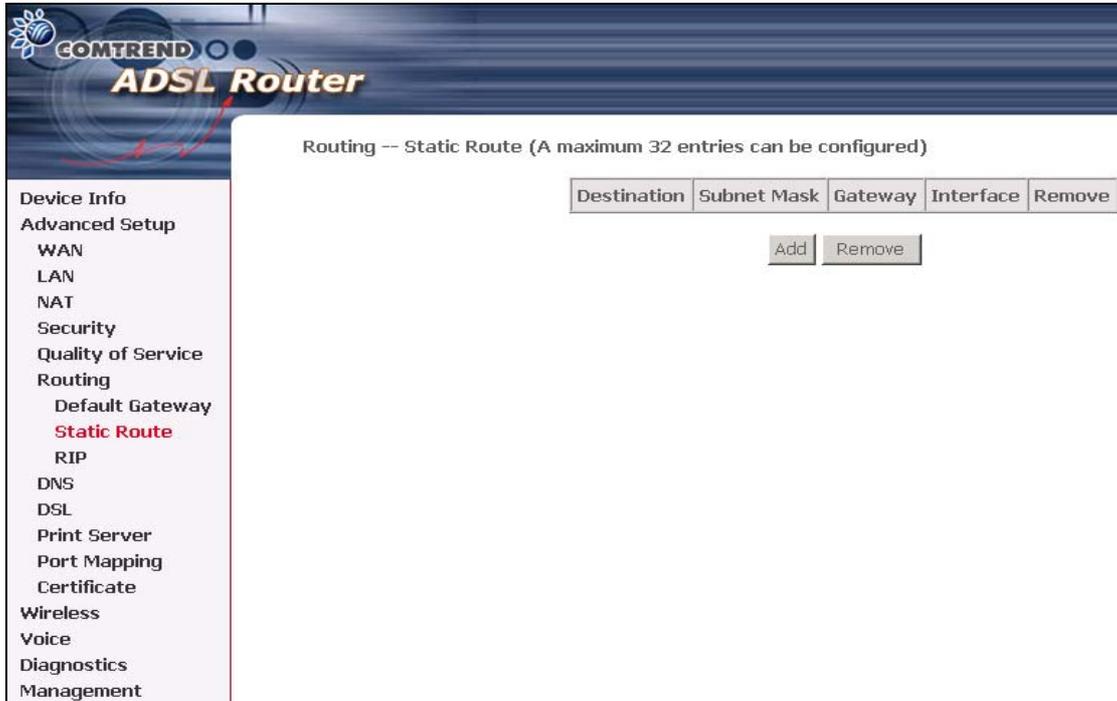
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the IAD to get the automatic assigned default gateway.



Note: This screenshot is based on PPPoE encapsulation.

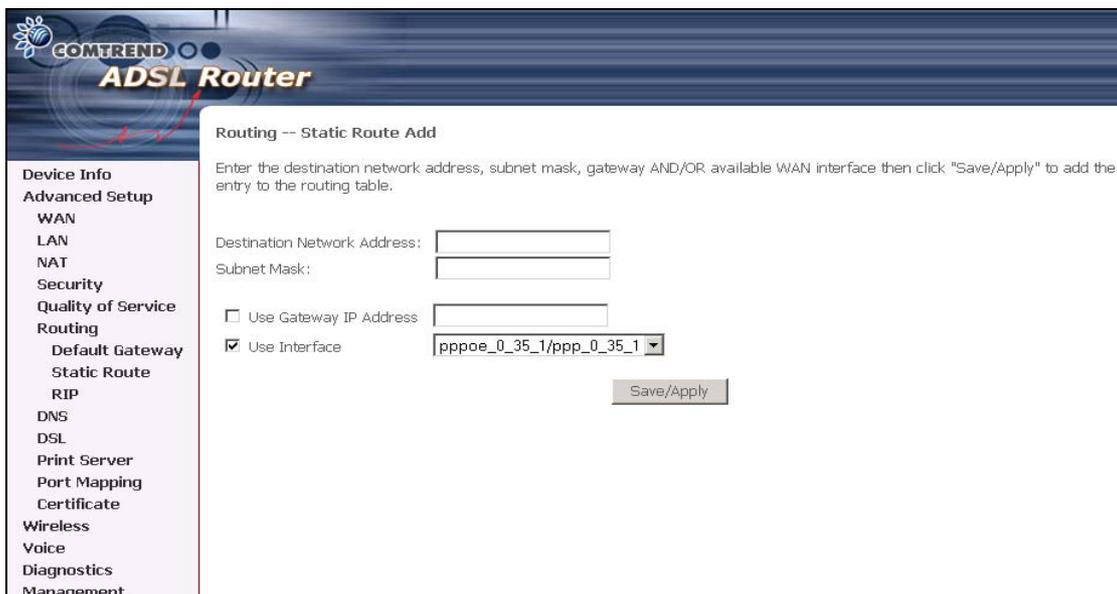
6.6.2 Static Route

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



Note: This screenshot is based on PPPoE encapsulation.

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



6.6.3 RIP

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

Routing -- RIP Configuration

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

Global RIP Mode Disabled Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ppp_0_35_1	0/35	2	Passive	<input type="checkbox"/>

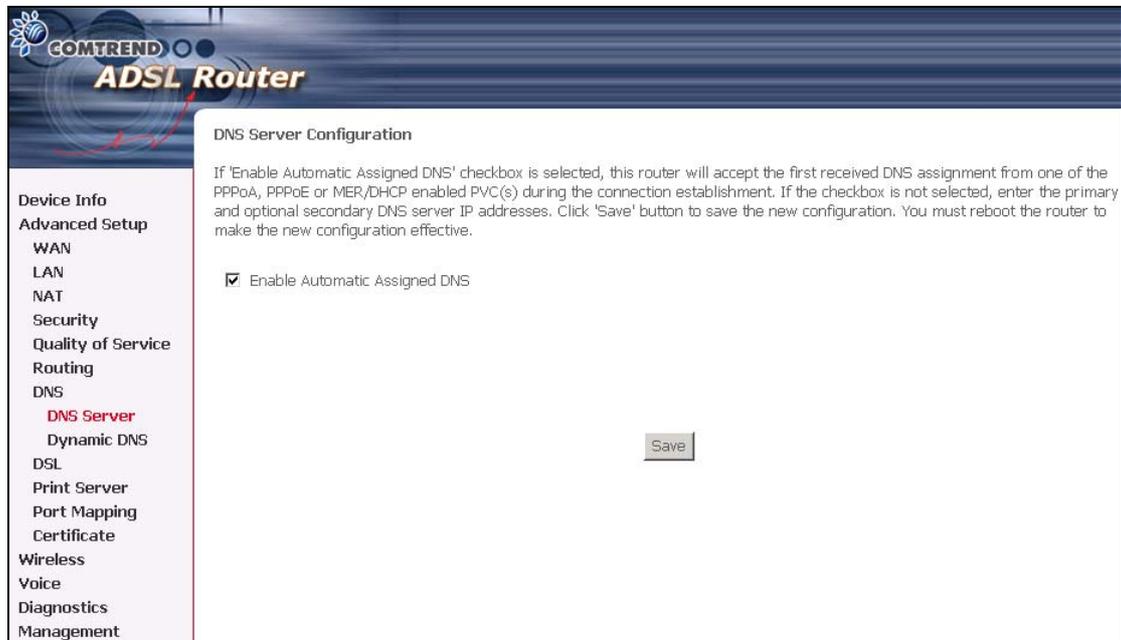
Save/Apply

Note: This screenshot is based on PPPoE encapsulation.

6.7 DNS

6.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this IAD 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 IAD to make the new configuration effective.



The screenshot displays the web management interface for a COMTREND ADSL Router. The page title is "DNS Server Configuration". On the left, a navigation menu lists various settings: Device Info, Advanced Setup (WAN, LAN, NAT), Security, Quality of Service, Routing, DNS (highlighted), DNS Server (highlighted in red), Dynamic DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area contains the following text: "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." Below this text, there is a checked checkbox labeled "Enable Automatic Assigned DNS" and a "Save" button.

6.7.2 Dynamic DNS

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



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

COMTREND
ADSL Router

Add dynamic DDNS

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

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

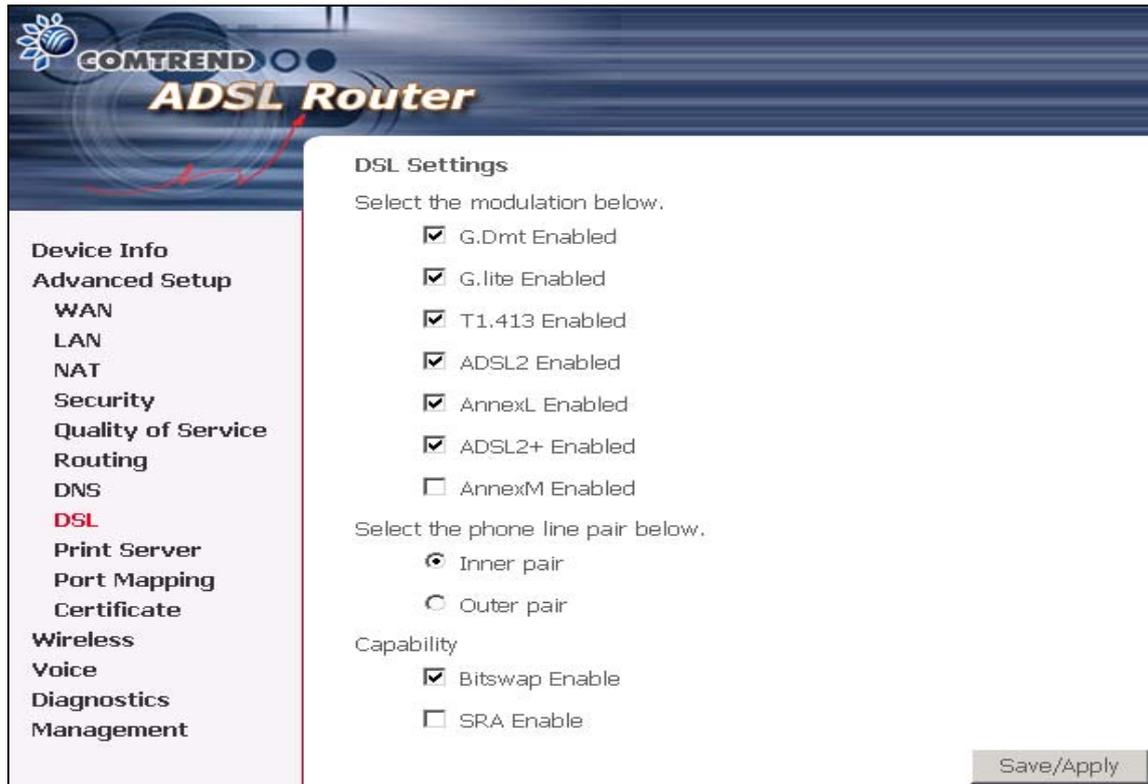
Password:

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

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

6.8 DSL

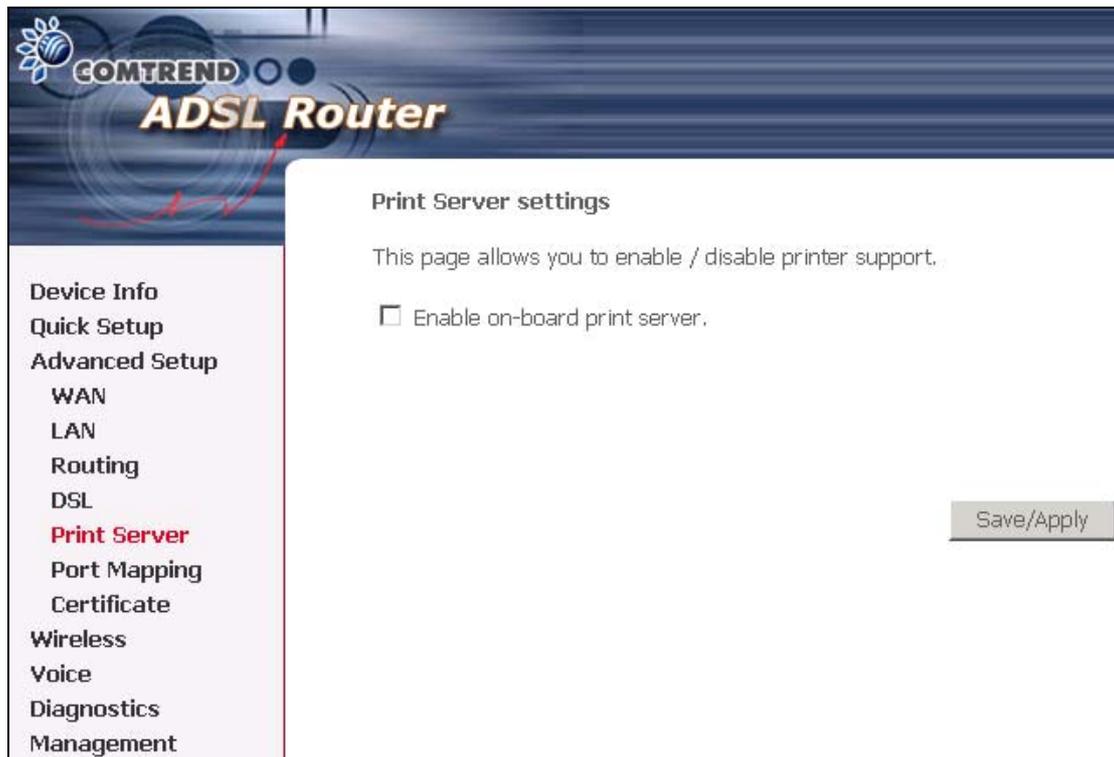
To access the DSL settings, First click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode. Note that this means the IAD uses one of the selected modulation modes to sync with the DSLAM if two more modes are selected.



Option	Description
G.dmt	Sets G.Dmt if you want the system to use only G.Dmt mode
G.lite	Sets G.lite if you want the system to use only G.lite mode
T1.413	Sets the T1.413 if you want the system to use only T1.413 mode
ADSL2 Enabled	The device can support the functions of the ADSL2
AnnexL Enabled	The device can support/enhance the long loop test
ADSL2+ Enabled	The device can support the functions of the ADSL2+
AnnexM Enabled	The device can support/enhance the data rate of both upstream/downstream
Inner Pair	Reserved only
Outer Pair	Reserved only
Bitswap Enable	Allows bitswaping function
SRA Enable	Allows seamless rate adaptation

6.9 Print Server

The CT-6382T is equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as a printer and hard disc to the CT-6382T. For this software release, printer server is supported.

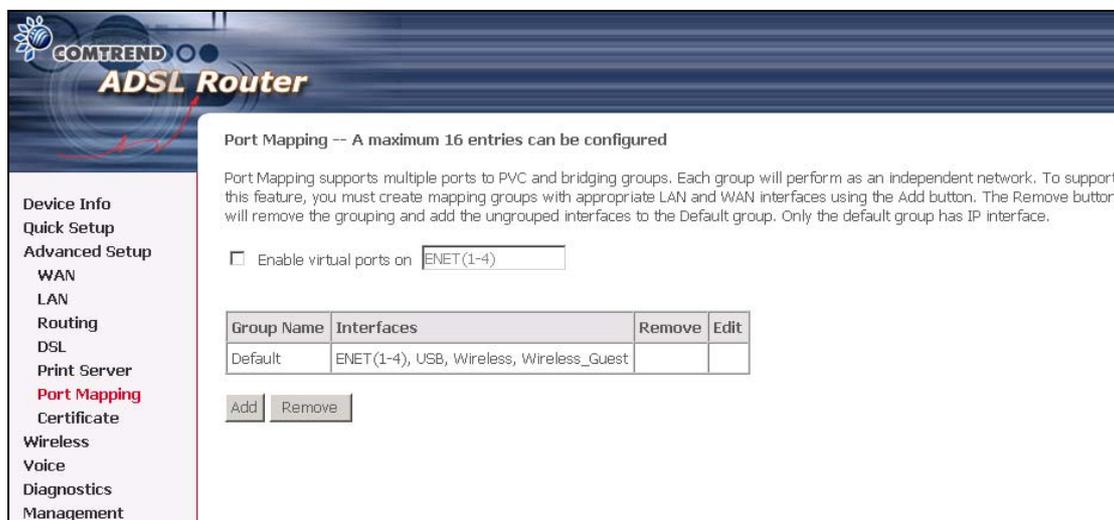


Please refer to Appendix A for an Example.

6.10 Port Mapping

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

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



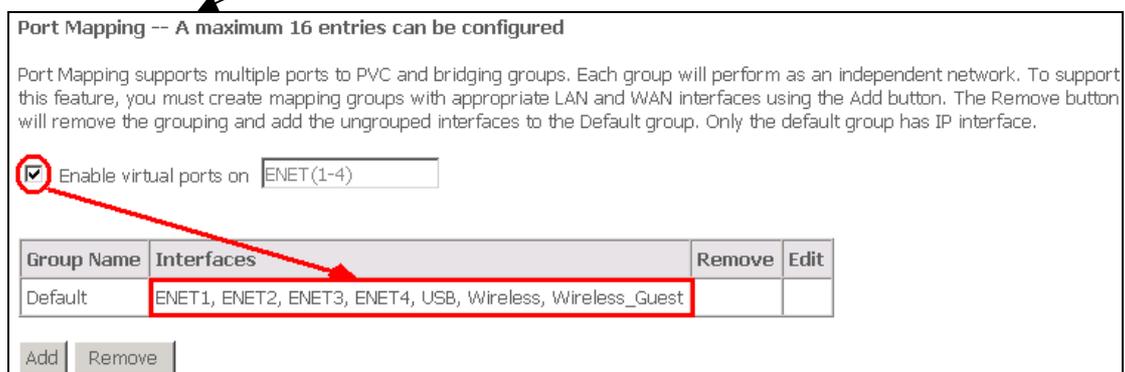
COMTREND ADSL Router

Port Mapping -- A maximum 16 entries can be configured

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

Enable virtual ports on

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



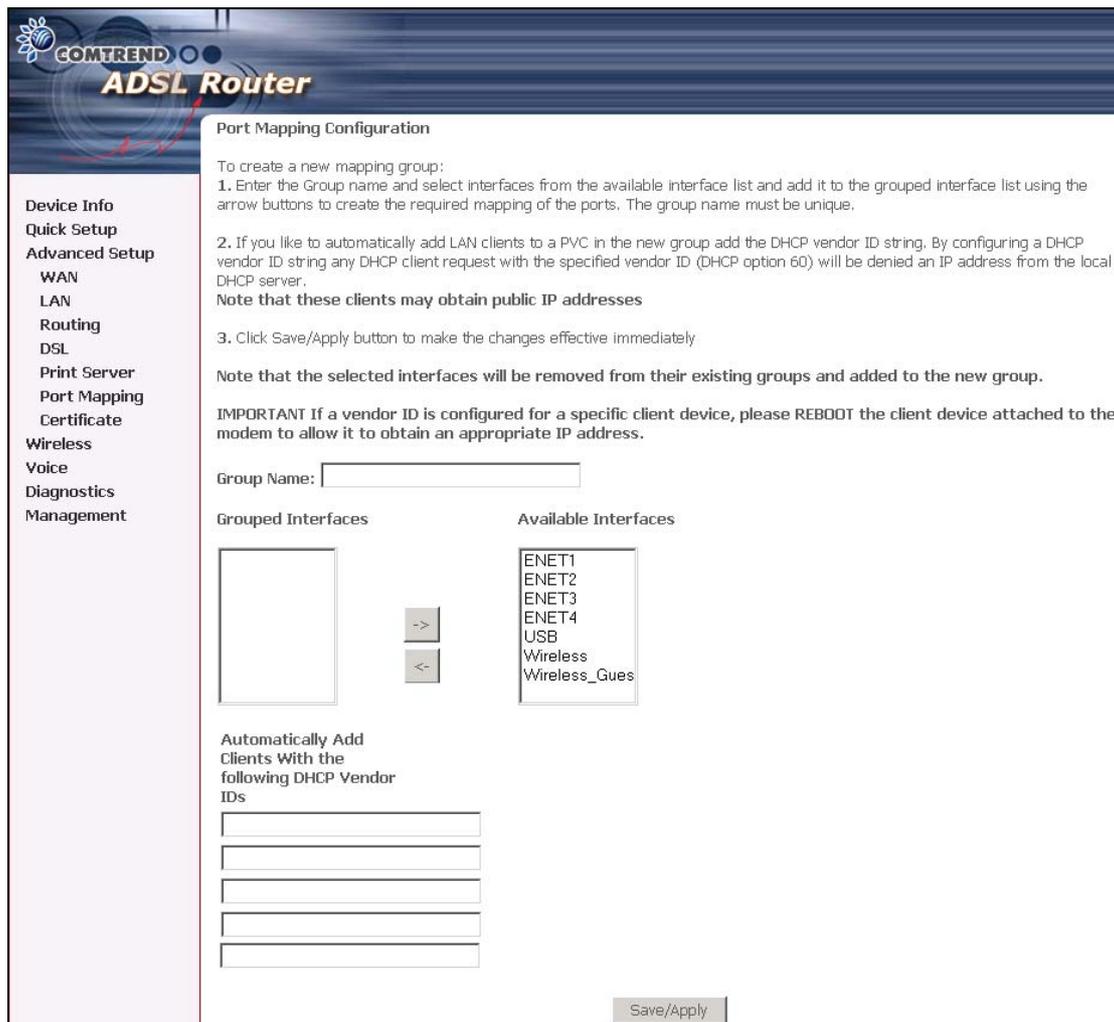
Port Mapping -- A maximum 16 entries can be configured

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

Enable virtual ports on

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

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



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

Automatically Add Clients With the Following DHCP Vendor IDs:

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

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video).

The LAN interfaces are ETH1, ETH2, ETH3, ETH4, Wireless and USB.

Port mapping configuration are:

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

The CPE's dhcp server is running on "Default". And ISP's dhcp server is running on PVC 0/36. It is for setup-box use only.

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

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

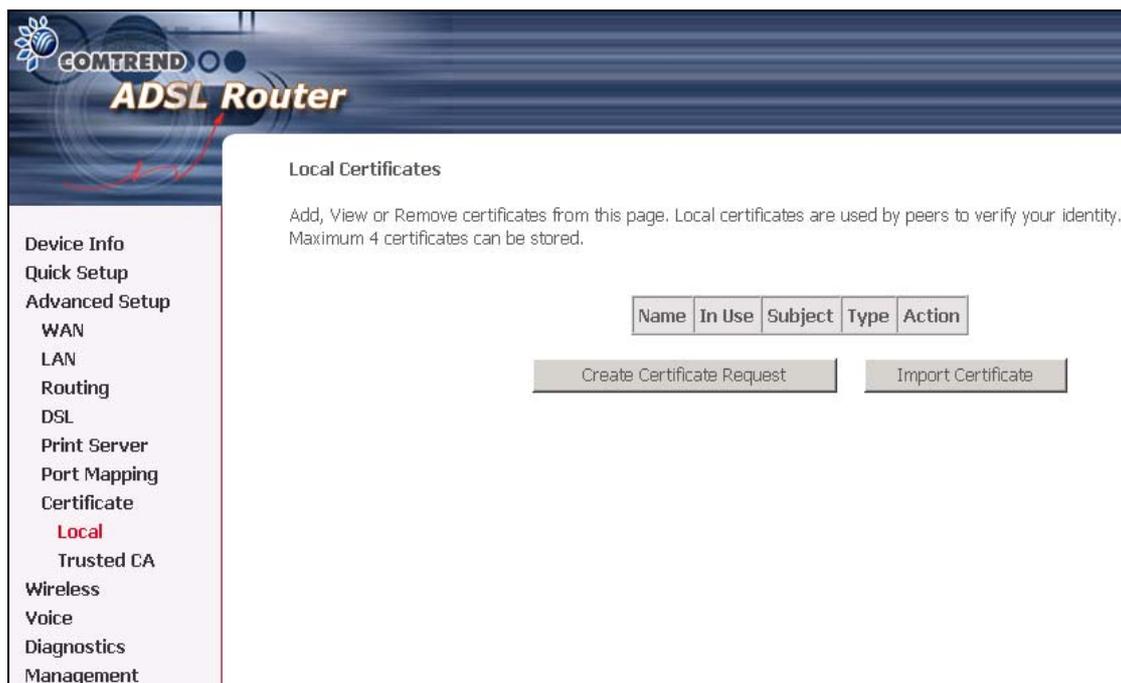
And CPE will change the portmapping configuration automatically. The portmapping configuration will become:

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

6.11 Certificate

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

6.11.1 Local



The screenshot shows the web interface of a COMTREND ADSL Router. The main heading is "Local Certificates". Below the heading, there is a text box that reads: "Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored." Below this text, there is a table with five columns: "Name", "In Use", "Subject", "Type", and "Action". Below the table, there are two buttons: "Create Certificate Request" and "Import Certificate". On the left side of the interface, there is a navigation menu with the following items: "Device Info", "Quick Setup", "Advanced Setup", "WAN", "LAN", "Routing", "DSL", "Print Server", "Port Mapping", "Certificate", "Local" (highlighted in red), "Trusted CA", "Wireless", "Voice", "Diagnostics", and "Management".

Click **Create Certificate Request** to generate a certificate signing request. The certificate signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate signing request. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.

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

The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with categories like Device Info, Advanced Setup, Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'Create new certificate request' and contains the following text: '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.' Below this text are five input fields: 'Certificate Name:', 'Common Name:', 'Organization Name:', 'State/Province Name:', and 'Country/Region Name:'. The 'Country/Region Name' field is a dropdown menu currently showing 'US (United States)'. An 'Apply' button is located at the bottom right of the form area.

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

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

COMTREND
ADSL Router

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-----
```

Apply

Device Info
Quick Setup
Advanced Setup
WAN
LAN
Routing
DSL
Print Server
Port Mapping
Certificate
 Local
 Trusted CA
Wireless
Voice
Diagnostics
Management

6.11.2 Trusted CA

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

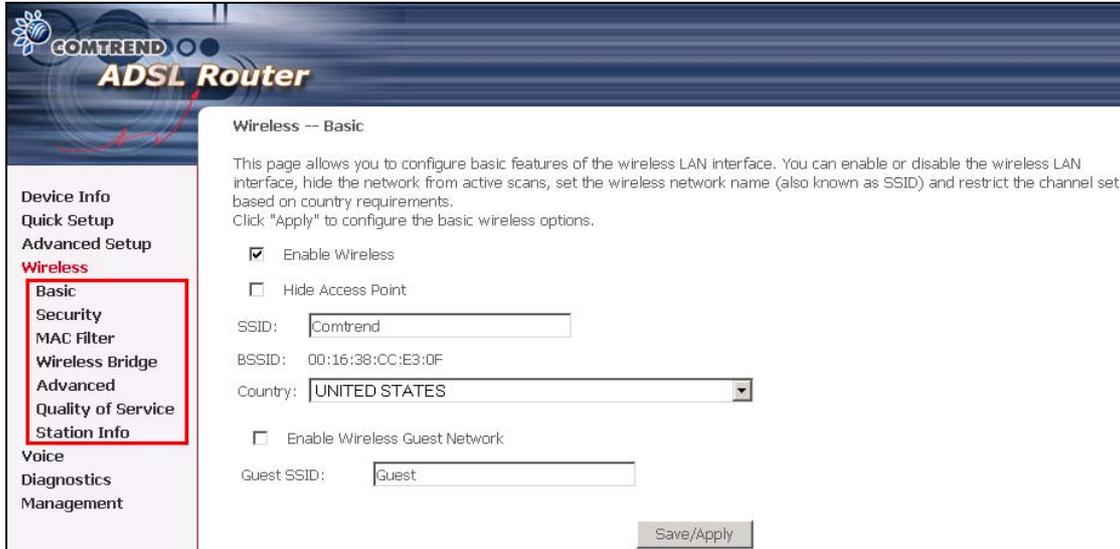


Click **Import Certificate** to paste the certificate content of your trusted CA. Generally speaking, the certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Chapter 7 Wireless

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



7.1 Wireless Basic Screen

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

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



Option	Description
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	<p>Select Hide Access Point to protect VoIP IAD access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected.</p> <p>The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration.</p> <p>In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.</p>
SSID	<p>Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.</p> <p>The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.</p>
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	<p>A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range:</p> <ul style="list-style-type: none"> ● US= worldwide ● Japan=1-14 ● Jordan= 10-13 ● Israel= TBD

7.1.1 Security

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

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

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

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



The screenshot shows the configuration interface for a Comtrend ADSL Router. The page title is "Wireless -- Security". On the left, there is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Basic, Security (highlighted in red), MAC Filter, Wireless Bridge, Advanced, Quality of Service, Station Info, Voice, Diagnostics, and Management. The main content area contains the following text and form fields:

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

Select SSID:

Network Authentication:

WEP Encryption:

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

Option	Description
Network Authentication	<p data-bbox="443 394 1565 618">It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications.</p> <p data-bbox="443 680 1321 714">Different authentication type pops up different settings requests.</p> <p data-bbox="443 777 1565 857">Choosing 802.1X, enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key.</p> <p data-bbox="443 920 1265 954">Also, enable WEP Encryption and select Encryption Strength.</p> <div data-bbox="443 1016 1565 1809" style="border: 1px solid black; padding: 10px;"> <p data-bbox="448 1055 916 1088">Select SSID: <input type="text" value="Comtrend"/></p> <p data-bbox="448 1122 1067 1155">Network Authentication: <input type="text" value="802.1X"/></p> <p data-bbox="448 1196 1023 1229">RADIUS Server IP Address: <input type="text" value="0.0.0.0"/></p> <p data-bbox="448 1245 1023 1279">RADIUS Port: <input type="text" value="1812"/></p> <p data-bbox="448 1294 1023 1328">RADIUS Key: <input type="text"/></p> <p data-bbox="448 1339 903 1373">WEP Encryption: <input type="text" value="Enabled"/></p> <p data-bbox="448 1384 884 1417">Encryption Strength: <input type="text" value="128-bit"/></p> <p data-bbox="448 1429 826 1462">Current Network Key: <input type="text" value="2"/></p> <p data-bbox="448 1473 1129 1507">Network Key 1: <input type="text"/></p> <p data-bbox="448 1518 1129 1552">Network Key 2: <input type="text"/></p> <p data-bbox="448 1563 1129 1597">Network Key 3: <input type="text"/></p> <p data-bbox="448 1608 1129 1641">Network Key 4: <input type="text"/></p> <p data-bbox="767 1641 1560 1697">Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys</p> <p data-bbox="1034 1765 1201 1798" style="text-align: right;"><input type="button" value="Save/Apply"/></p> </div> <p data-bbox="443 1832 1560 1955">Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.</p>

	<p>Choosing WPA, you must enter WPA Group Rekey Interval.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Select SSID: <input type="text" value="Comtrend"/></p> <p>Network Authentication: <input type="text" value="WPA"/></p> <p>WPA Group Rekey Interval: <input type="text" value="0"/></p> <p>RADIUS Server IP Address: <input type="text" value="0.0.0.0"/></p> <p>RADIUS Port: <input type="text" value="1812"/></p> <p>RADIUS Key: <input type="text"/></p> <p>WPA Encryption: <input type="text" value="TKIP"/></p> <p>WEP Encryption: <input type="text" value="Disabled"/></p> <p style="text-align: right;"><input type="button" value="Save/Apply"/></p> </div> <p>Choosing WPA-PSK, you must enter WPA Pre-Shared Key and Group Rekey Interval.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Select SSID: <input type="text" value="Comtrend"/></p> <p>Network Authentication: <input type="text" value="WPA-PSK"/></p> <p>WPA Pre-Shared Key: <input type="text"/> Click here to display</p> <p>WPA Group Rekey Interval: <input type="text" value="0"/></p> <p>WPA Encryption: <input type="text" value="TKIP"/></p> <p>WEP Encryption: <input type="text" value="Disabled"/></p> <p style="text-align: right;"><input type="button" value="Save/Apply"/></p> </div>
<p>WEP Encryption</p>	<p>It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.</p>
<p>Encryption strength</p>	<p>A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-character or 10-character hexadecimal or 128 8-bit (13-character or 10-character) key. If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key. The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.</p>

7.1.2 MAC Filter

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

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

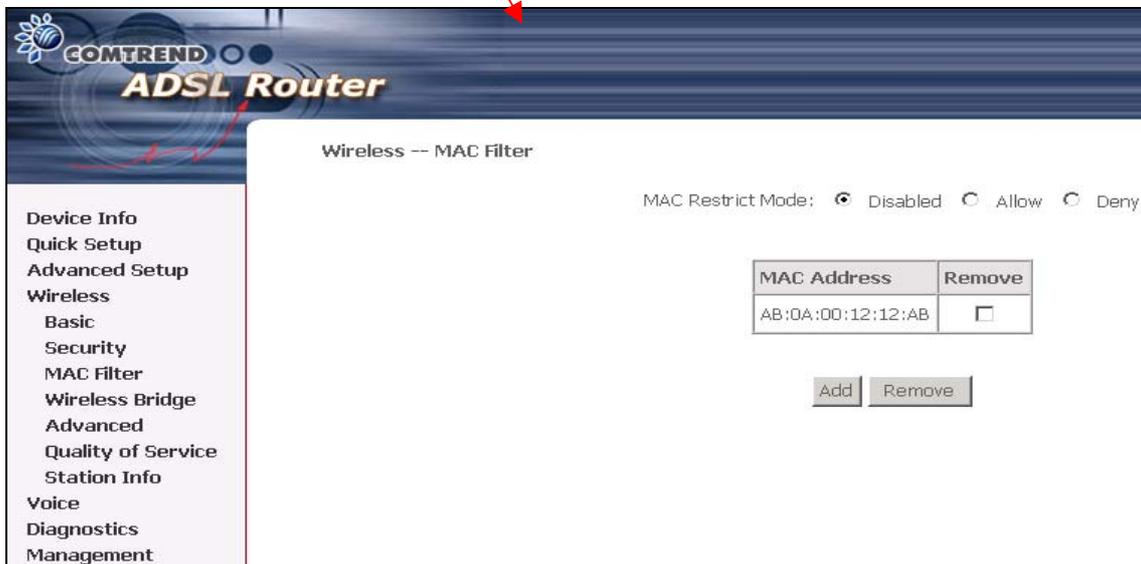
MAC Restrict mode: **Off** - disables MAC filtering; **Allow** – permits **access** for the specified MAC address; **Deny**; reject access of the specified MAC address, then click the **SET** button.

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

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



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



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

7.1.3 Wireless Bridge

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



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

7.1.4 Advanced

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

Wireless -- Advanced

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

AP Isolation:

Band:

Channel:

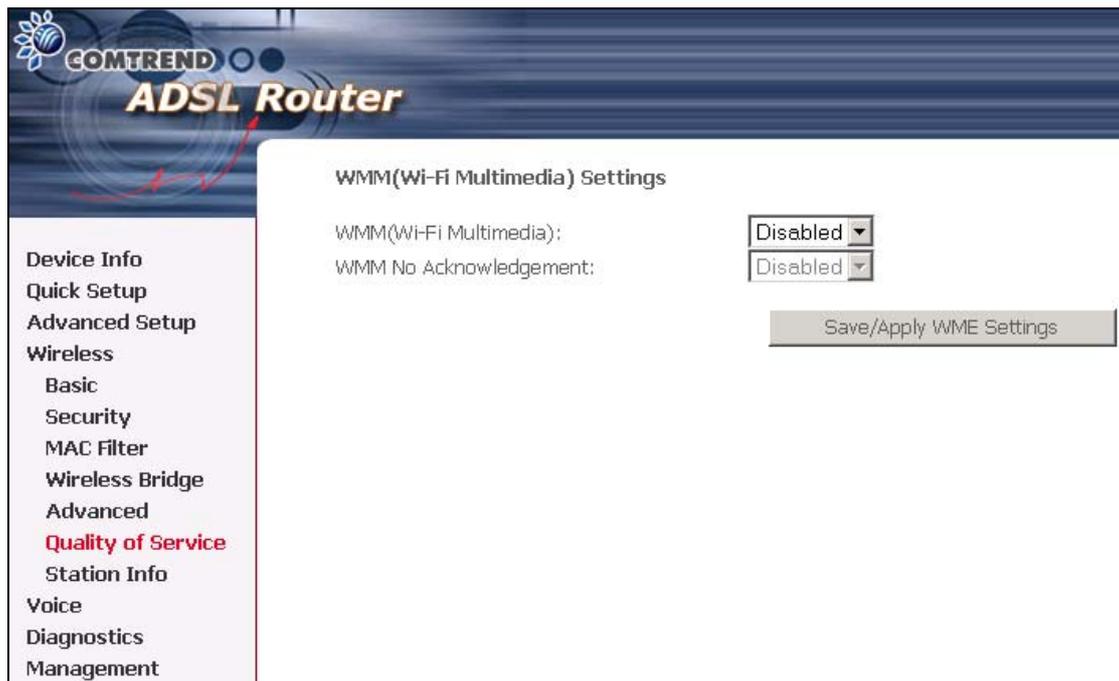
Channel	Drop-down menu that allows selection of specific channel
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g™ Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary.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

DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Xpress™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
54g™ Mode	Select the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the IAD will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.

Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.

7.1.5 Quality of Service

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



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

7.1.6 Station Info

This page shows authenticated wireless stations and their status.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

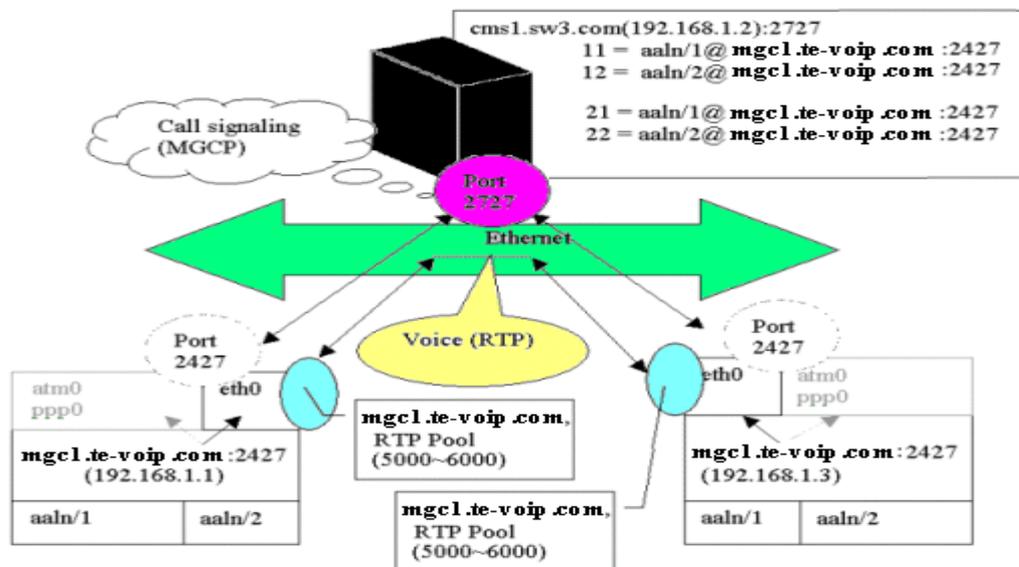
BSSID	Associated	Authorized
00:12:F0:B5:C9:9C		

Refresh

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

Chapter 8 Voice

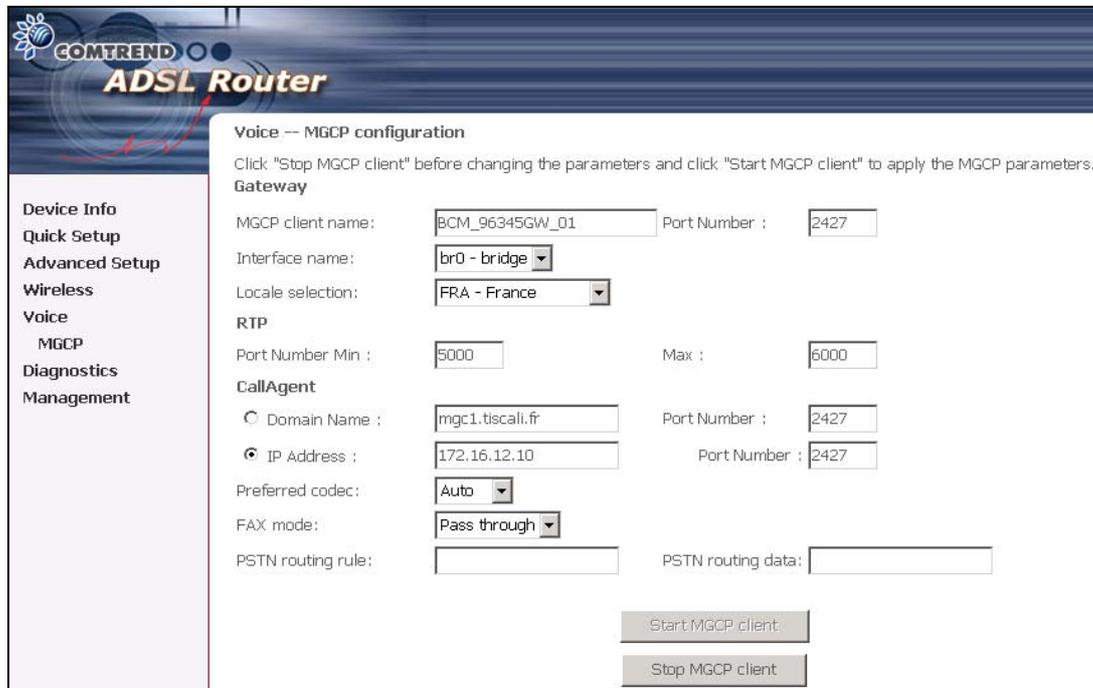
The MGCP option is used to verify the MGCP application configured by you. We will use the scenario illustrated in the following diagram to explain the Web configuration:



To access MGCP, Simply click on the Voice->**MGCP** from main menu.

8.1 MGCP

STEP 1: Select **MGCP** on the menu; the current configuration of the Media Gateway will be displayed.



COMTREND ADSL Router

Voice -- MGCP configuration

Click "Stop MGCP client" before changing the parameters and click "Start MGCP client" to apply the MGCP parameters.

Gateway

MGCP client name: Port Number:

Interface name:

Locale selection:

RTP

Port Number Min: Max:

CallAgent

Domain Name: Port Number:

IP Address: Port Number:

Preferred codec:

FAX mode:

PSTN routing rule: PSTN routing data:

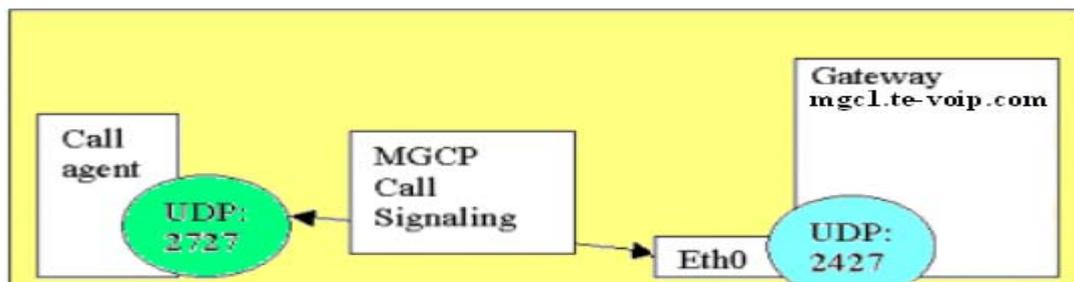
STEP 2: Enter the MGCP Gateway and Call Agent information for your Service provider. The fields are explained below.

- **Gateway**

MGCP Client name: Enter the MGCP client name.

Interface Name: Select the LAN interface or WAN interface. Gateway Binding interface for MGCP Call Signaling control, e.g. "ppp0" for PPPoE or PPPoA, "atm0" for RFC1483 routed, and "mer0" for MER encapsulation.

Locale Selection: Sets tone, ring type and physical characteristics for each specific country.



Port Number: The gateway port number for MGCP Call Signaling control, e.g. "2427".

- **RTP**

Port Number (Min): The RTP-pool lower range

Port Number (Max): The RTP-pool upper range

- **CallAgent**

Domain Name/Port Number: The Call agent domain name type and port number

IP Address/Port Number: The Call agent IP address type and port number

Preferred codec: The preferred codec of this user. The default is Auto first.

FAX mode: Use G711u (Pass-through) or T.38 when sending a fax.

PSTN routing rule: If PSTN route rule is "auto", when a PSTN call coming will ring the idle phone(phone1 idle ring phone1,phone1 busy ring phone2)

PSTN routing data: If PSTN route rule is "fix", when a PSTN call coming will ring the phone that the user selects from PSTN route data (phone1 OR phone2)

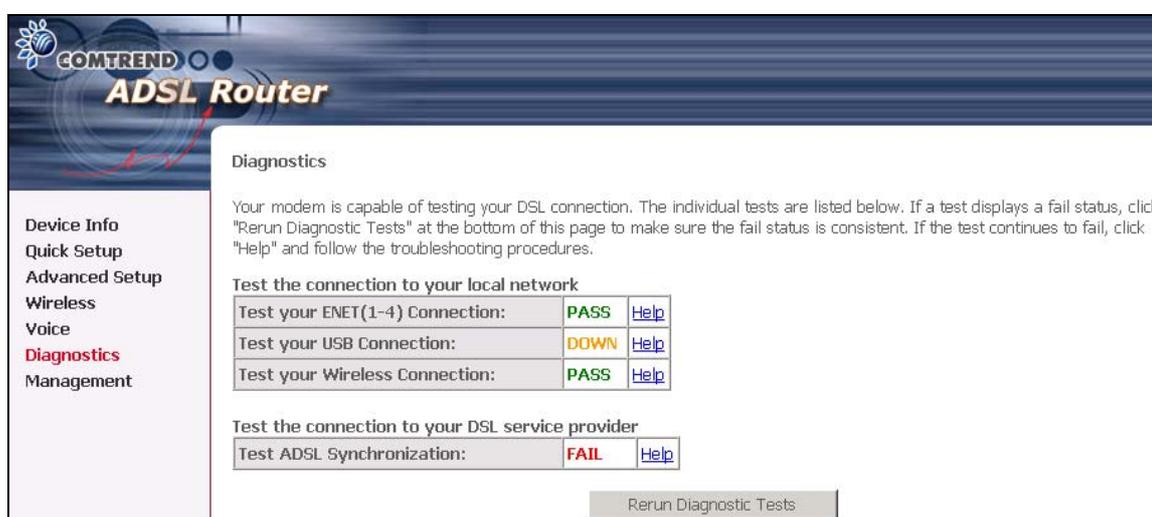
Saving Configuration: To save a new configuration, first click Stop MGCP client. Then, click Start MGCP client. The configuration will be saved. We recommend that you save and reboot the unit to enable the new configuration.

Note 1: You can assign the call agent as IP address type or Domain Name type. If you choose IP address type, every time you restart the machine, the gateway will send a RSIP to this IP address. If you choose Domain Name type, every time you restart the machine, the gateway will do a DNS lookup until it receives a valid IP address translation from the DNS server, and then it will send RSIP to this IP address.

Note 2: If you choose Domain Name type, the IP address field will display the DNS lookup result automatically.

Chapter 9 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-6382T and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Test	Description
Ethernet Connection	<p>Pass: indicates that the Ethernet interface from your computer is connected to the LAN port of your VoIP IAD. A flashing or solid green LAN LED on the IAD also signifies that an Ethernet connection is present and that this test is successful.</p> <p>Fail: Indicates that the VoIP IAD does not detect the Ethernet interface on your computer.</p>
USB connection (Note: this device does not support a USB connection)	<p>Pass: Indicates that the USB interface from your computer is connected to the LAN port of your VoIP IAD.</p> <p>Down: Indicates that the VoIP IAD does not detect the USB interface on your computer.</p>

Wireless connection	<p>Pass: Indicates that the Wireless interface from your computer is connected to the wireless network.</p> <p>Down: Indicates that the VoIP IAD does not detect the wireless network.</p>
ADSL Synchronization	<p>Pass: Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid ADSL LED on the IAD also indicates the detection of a DSL signal from the telephone company.</p> <p>Fail: indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The ADSL LED will turn off.</p>

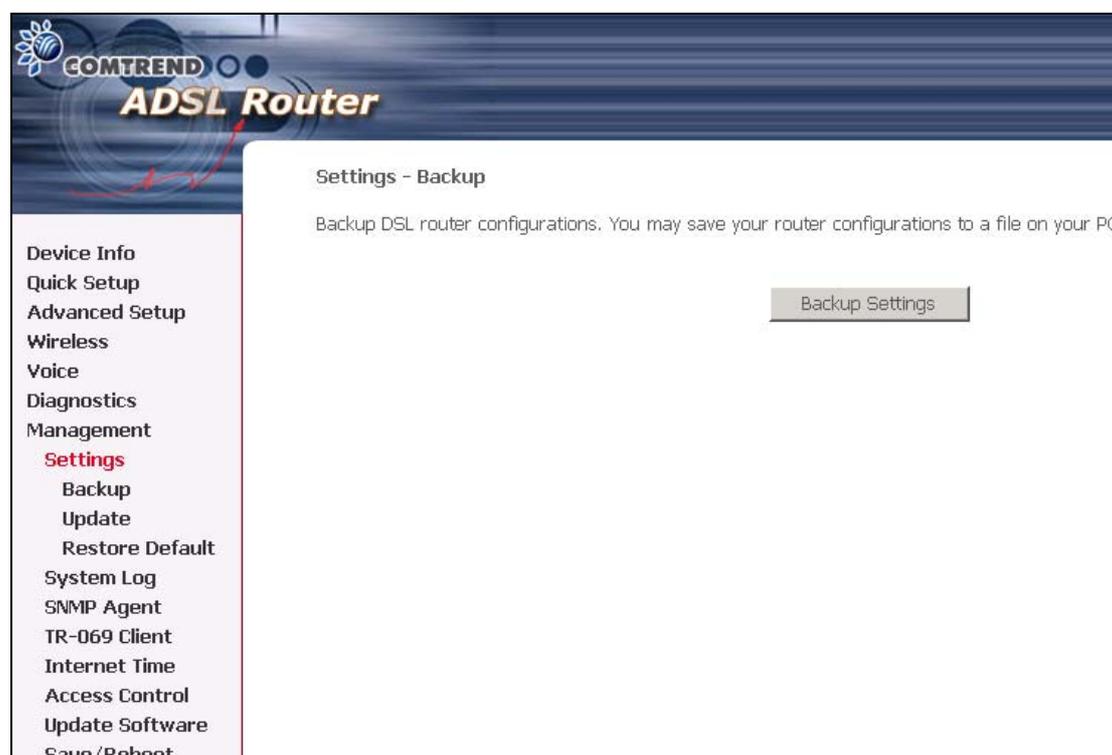
Chapter 10 Management

The Management section of the CT-6382T supports the following maintenance functions and processes:

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

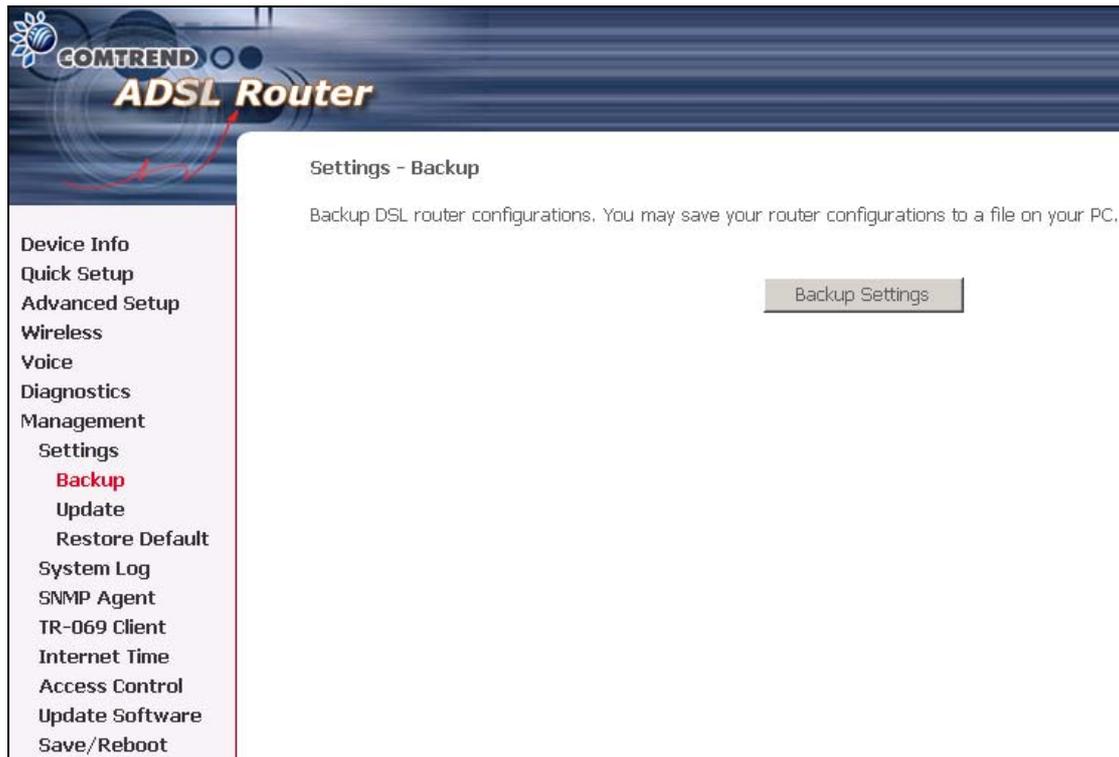
10.1 Settings

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



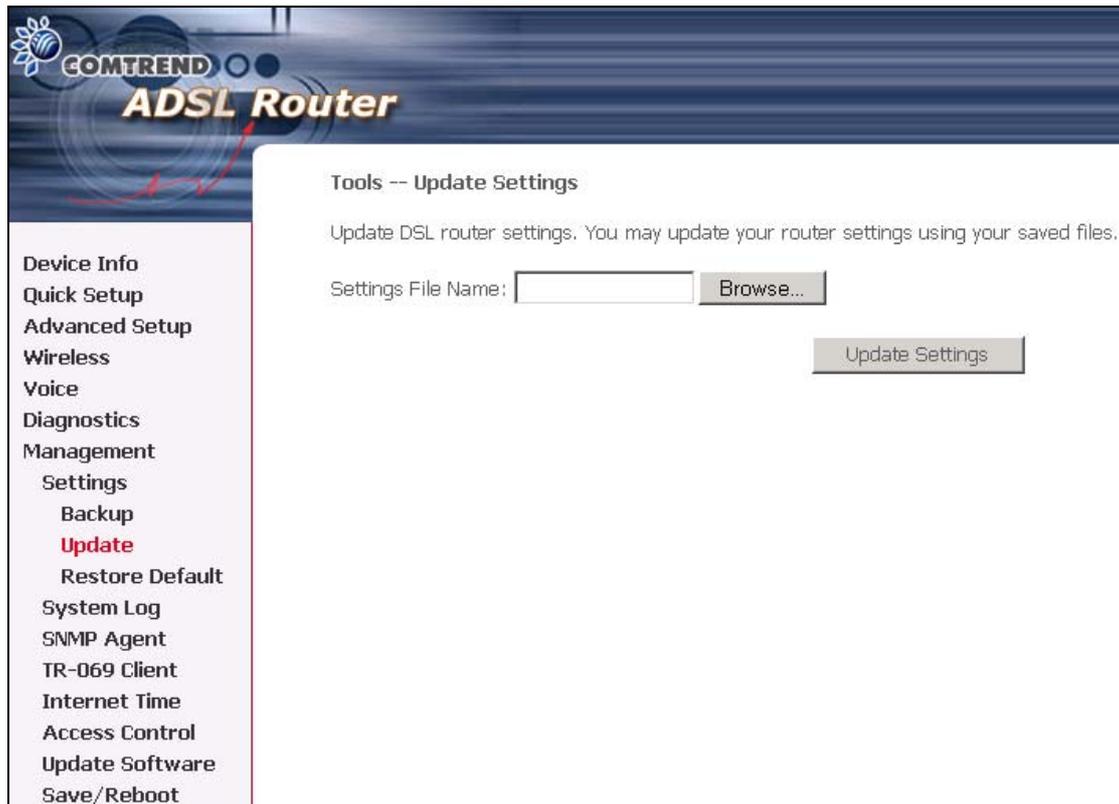
10.1.1 Configuration Backup

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



10.1.2 Configuration Restoration

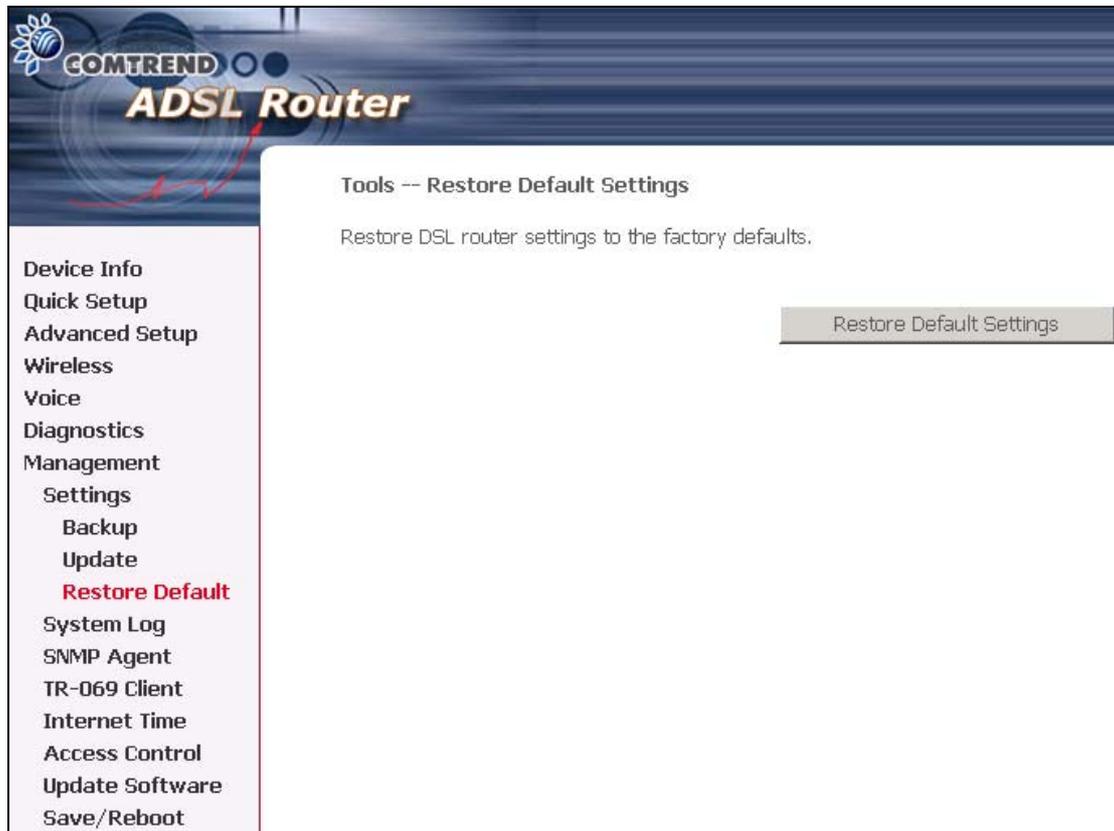
The Update option under Management>Settings update your IAD settings using your saved files.



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

10.1.3 Restore Default

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



NOTE: This entry has the same effect as the hardware reset-to-default button. The CT-6382T board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration settings saved on the flash memory.

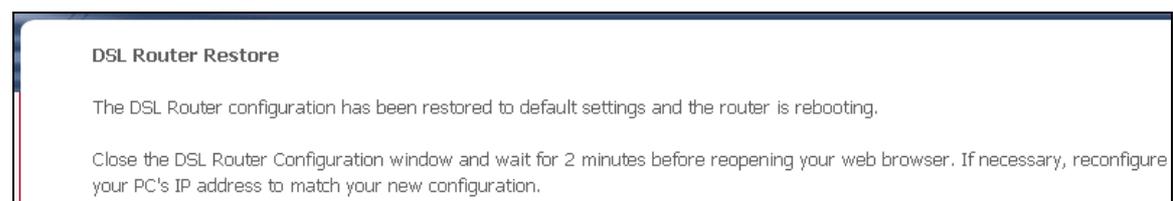
NOTE: Restoring system settings require a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-6382T.

Default settings

The CT-6382T default settings are

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

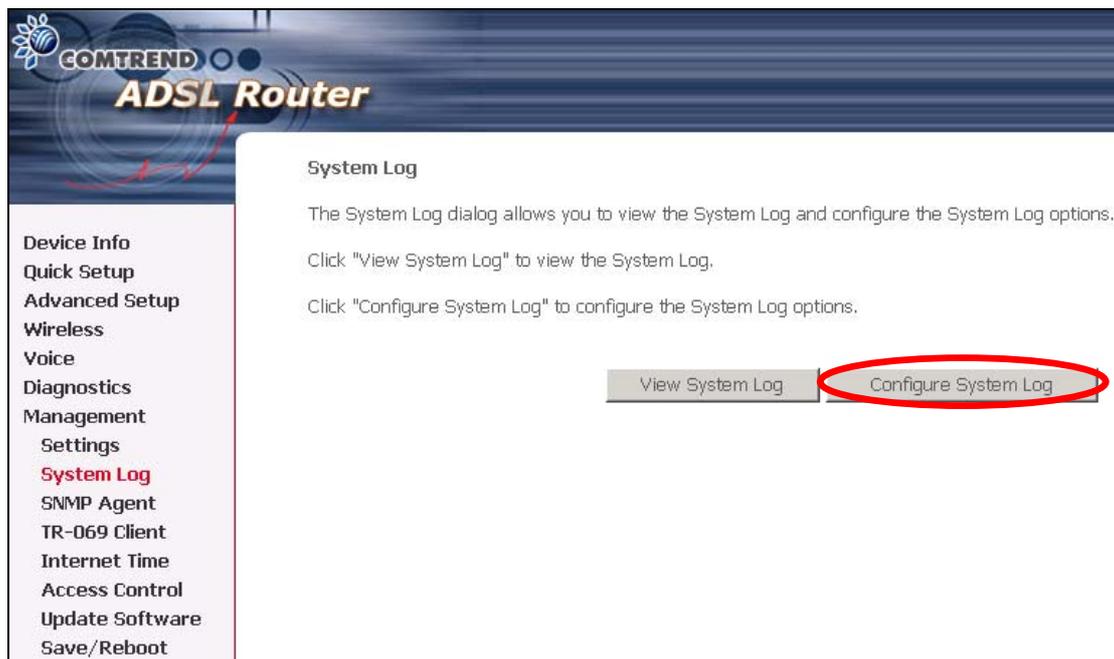
After the Restore Default Configuration button is selected, the following screen appears. Close the VoIP IAD Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



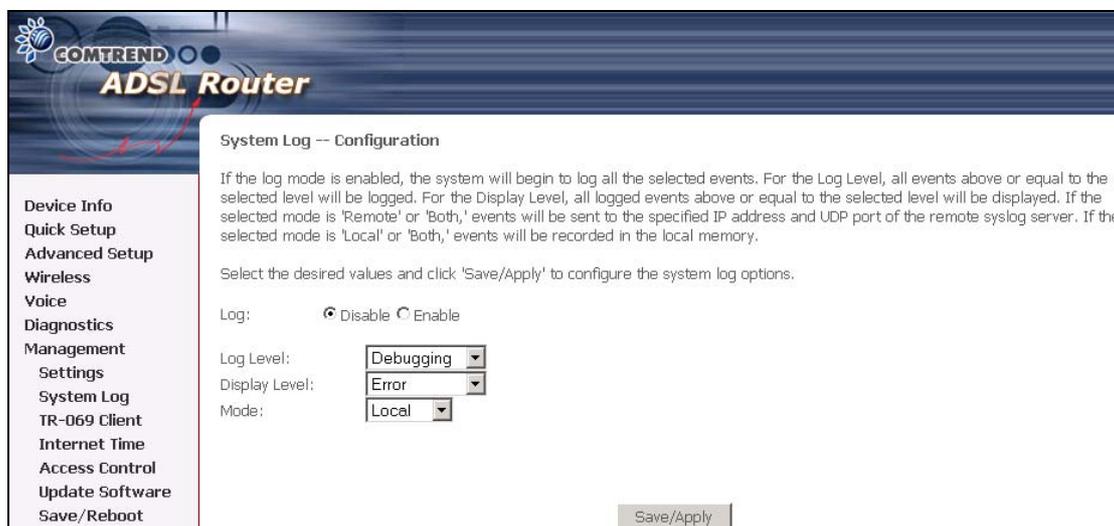
10.2 System Log

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

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



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



Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, click Enable and then Apply button.
Log level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-6382T SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are</p> <ul style="list-style-type: none"> ● Emergency = system is unstable ● Alert = action must be taken immediately ● Critical = critical conditions ● Error = Error conditions ● Warning = normal but significant condition ● Notice ● Informational ● Debugging = debug-level messages <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p>
Display Level	Allows the user to select the logged events and displays on the View System Log page for events of this level and above to the highest Emergency level.
Mode	<p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously.</p> <p>If remote mode is selected, view system log will not be able to display events saved in the remote syslog server.</p> <p>When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>

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

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	kern	crit	kernel: eth0 Link UP.

Refresh

Close

10.3 SNMP Agent

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

Select or enter the desired values and click **Save/Apply** to configure the SNMP options.



The screenshot shows the configuration page for the SNMP Agent on a Comtrend ADSL Router. The page has a dark blue header with the Comtrend logo and 'ADSL Router' text. On the left is a navigation menu with options like 'Device Info', 'Quick Setup', 'Advanced Setup', 'Wireless', 'Voice', 'Diagnostics', 'Management', 'Settings', 'System Log', 'SNMP Agent' (highlighted in red), 'TR-069 Client', 'Internet Time', 'Access Control', 'Update Software', and 'Save/Reboot'. The main content area is titled 'SNMP - Configuration' and contains the following text and form fields:

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:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="Comtrend"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

At the bottom right of the configuration area is a 'Save/Apply' button.

10.4 TR-069 Client

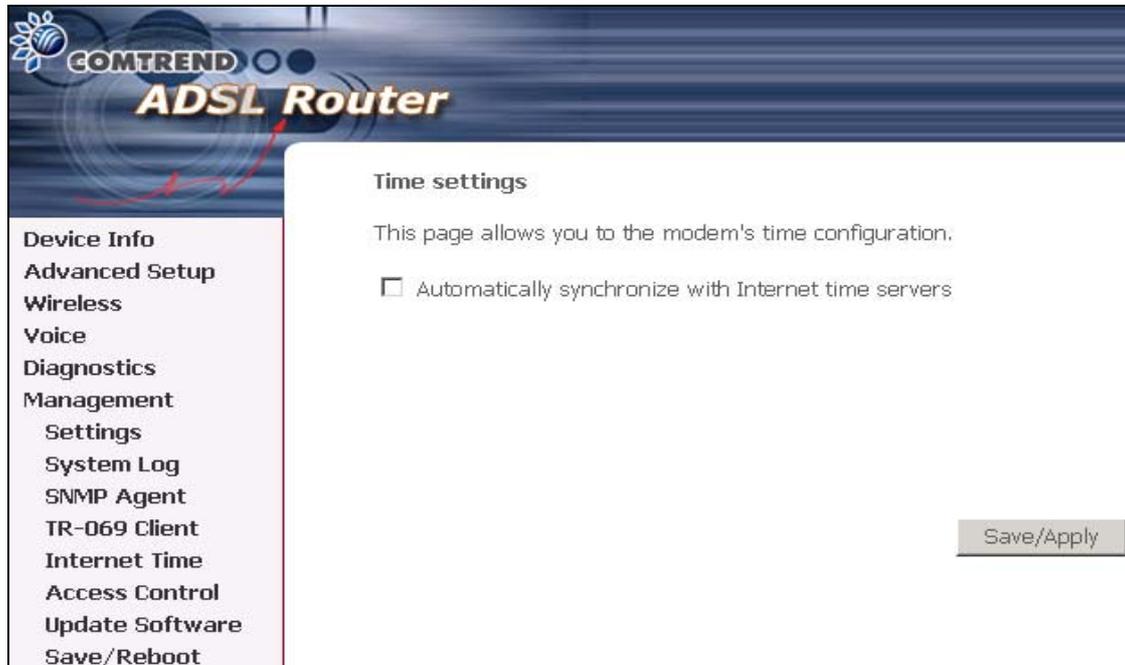
WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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

Connection Request User Name	Username used to authenticate an ACS making a Connection. Request to the CPE.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE.
Get RPC Methods	This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to immediately establish a connection to the ACS.

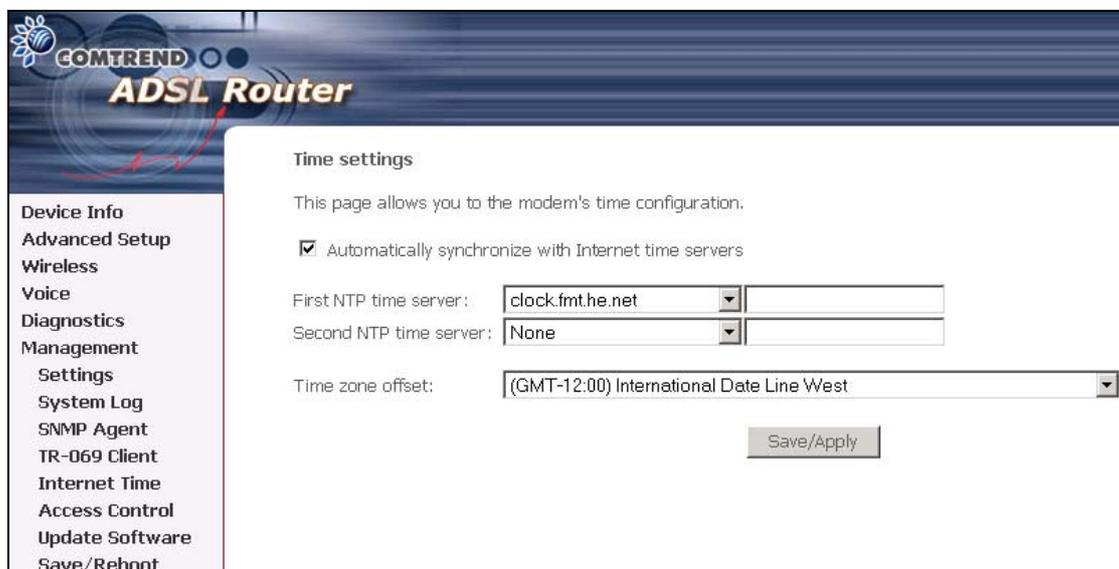
10.5 Internet Time

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



The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled "Time settings" and contains the text "This page allows you to the modem's time configuration." Below this text is a checkbox labeled "Automatically synchronize with Internet time servers", which is currently unchecked. A "Save/Apply" button is located at the bottom right of the main content area.

If you want to use Parental control function, user must set Internet time on IAD first.



The screenshot shows the COMTREND ADSL Router web interface with the "Internet Time" menu item selected in the navigation bar. The "Time settings" page is displayed with the "Automatically synchronize with Internet time servers" checkbox checked. Below this, there are two fields for NTP time servers: "First NTP time server" is set to "clock.fmt.he.net" and "Second NTP time server" is set to "None". The "Time zone offset" is set to "(GMT-12:00) International Date Line West". A "Save/Apply" button is visible at the bottom right.

First NTP time server: Select your required server.

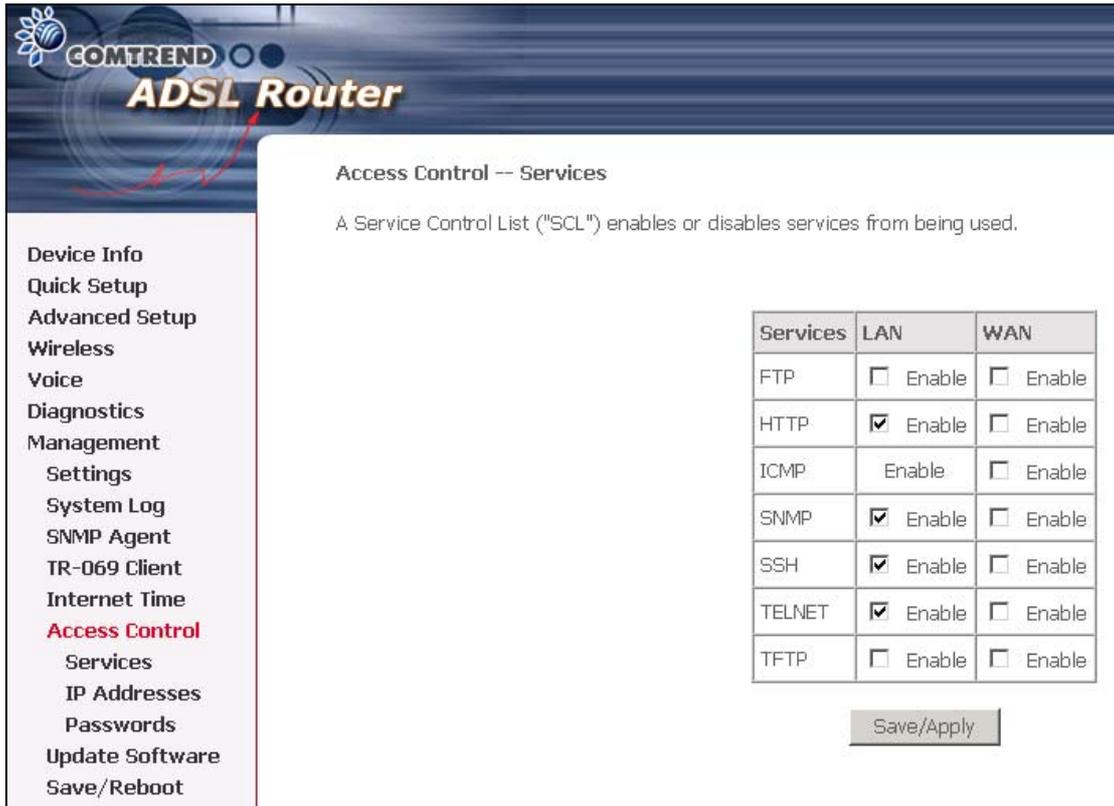
Second NTP time server: Select second time server if required.

Time zone offset: Select your local time zone.

Click **Save/Apply** to apply settings.

10.6 Access Control

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



The screenshot shows the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". On the left is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management (highlighted), Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control (highlighted), Services (highlighted), IP Addresses, Passwords, Update Software, and Save/Reboot. The main content area is titled "Access Control -- Services" and includes a descriptive paragraph: "A Service Control List ('SCL') enables or disables services from being used." Below this is a table with three columns: Services, LAN, and WAN. The table lists eight services with checkboxes for enabling them on either LAN or WAN. A "Save/Apply" button is located at the bottom right of the table.

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

Save/Apply

10.6.1 Services

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

GOMTREND ADSL Router

Access Control -- Services

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

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

Save/Apply

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

10.6.2 Access IP Addresses

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



The screenshot displays the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". A left-hand navigation menu lists various settings categories, with "IP Addresses" highlighted in red. The main content area is titled "Access Control -- IP Address" and contains a descriptive paragraph about the IP Address Access Control mode. Below the text, there are radio buttons for "Access Control Mode" set to "Disable". Two rows of buttons are present: the first row has "IP Address" and "Remove" buttons, and the second row has "Add" and "Remove" buttons.

COMTREND
ADSL Router

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

Access Control -- IP Address

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

Access Control Mode: Disable Enable

IP Address Remove

Add Remove

10.6.3 Passwords

The Passwords option configures the access passwords for the IAD. Access to your VoIP IAD is controlled through three user accounts: admin, support, and user.

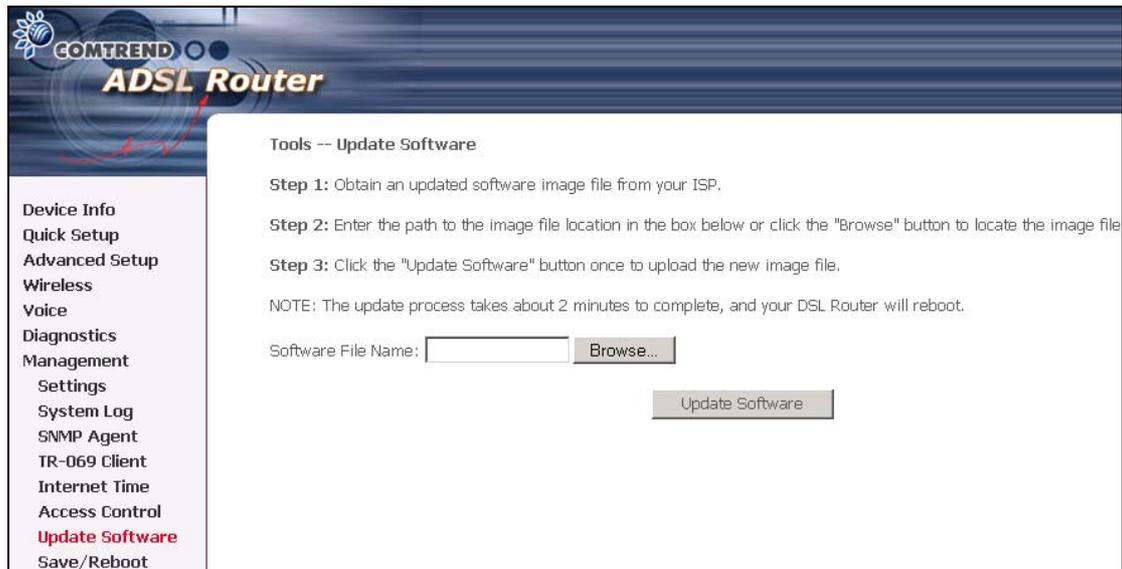
- "root" has unrestricted access to change and view configuration of your VoIP IAD.
- "support" is used to allow an ISP technician to access your VoIP IAD for maintenance and to run diagnostics.
- "user" can access the IAD, view configuration settings and statistics, as well as, update the IAD's software.

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

The screenshot shows the web interface for a COMTREND ADSL Router. The page title is "Access Control -- Passwords". The main content area explains that access is controlled through three user accounts: root, support, and user. It provides details for each user: "root" has unrestricted access, "support" is for ISP technicians, and "user" is for general access and software updates. Below this, there are instructions to use the form fields to enter up to 16 characters and click "Apply". The form includes a dropdown menu for "Username", and text input fields for "Old Password", "New Password", and "Confirm Password". A "Save/Apply" button is located at the bottom right of the form area. On the left side, there is a navigation menu with options like "Device Info", "Quick Setup", "Advanced Setup", "Wireless", "Voice", "Diagnostics", "Management", "Settings", "System Log", "SNMP Agent", "TR-069 Client", "Internet Time", "Access Control", "Services", "IP Addresses", "Passwords", "Update Software", and "Save/Reboot". The "Passwords" option is highlighted in red.

10.7 Update software

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



The screenshot shows the 'Update Software' tool in the COMTREND ADSL Router web interface. The left sidebar contains a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics Management, Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Update Software (highlighted in red), and Save/Reboot. The main content area is titled 'Tools -- Update Software' and contains the following instructions:

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

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

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

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

Software File Name:

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

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

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

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

10.8 Save and Reboot

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



Appendix A: Printer Server Configuration

1. Introduction

This application notes explain the steps of enabling the Printer Server function in CT-6382T reference platforms.

2. How to enable on-board Printer Server function

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

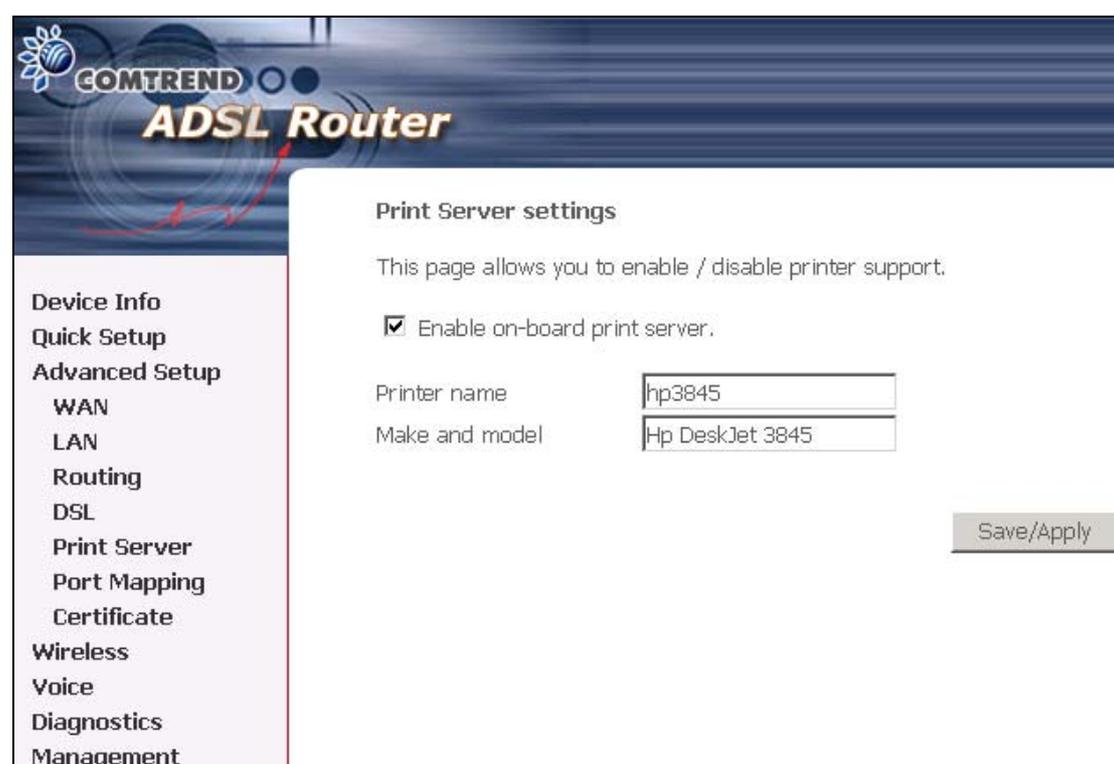
Step1: Enable Print Server from Modem Web GUI.

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

Note:

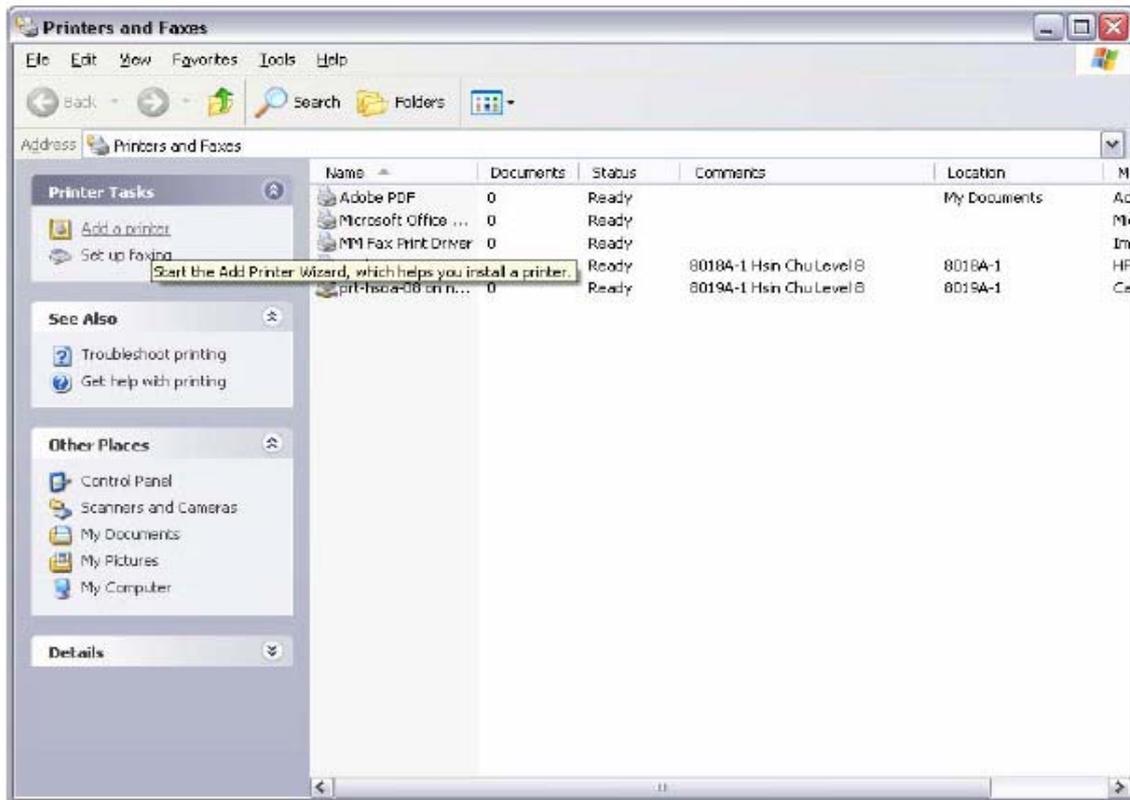
The **"Printer name"** can be any text string up to **40** characters.

The **"Make and model"** can be any text string up to **128** characters.



The screenshot displays the Comtrend ADSL Router Web GUI. The main header features the Comtrend logo and the text "ADSL Router". On the left side, there is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, WAN, LAN, Routing, DSL, Print Server (highlighted), Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Print Server settings" and contains the following text: "This page allows you to enable / disable printer support." Below this text is a checked checkbox labeled "Enable on-board print server." There are two input fields: "Printer name" with the value "hp3845" and "Make and model" with the value "Hp DeskJet 3845". A "Save/Apply" button is located at the bottom right of the settings area.

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



Step3: Select Network Printer and click "Next".



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

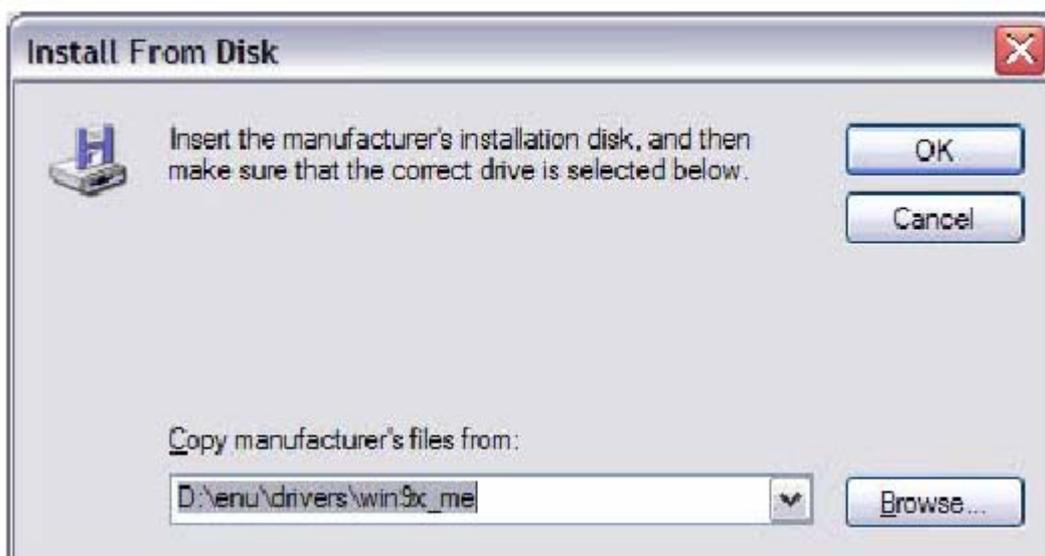
The printer name "hp3845" must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.



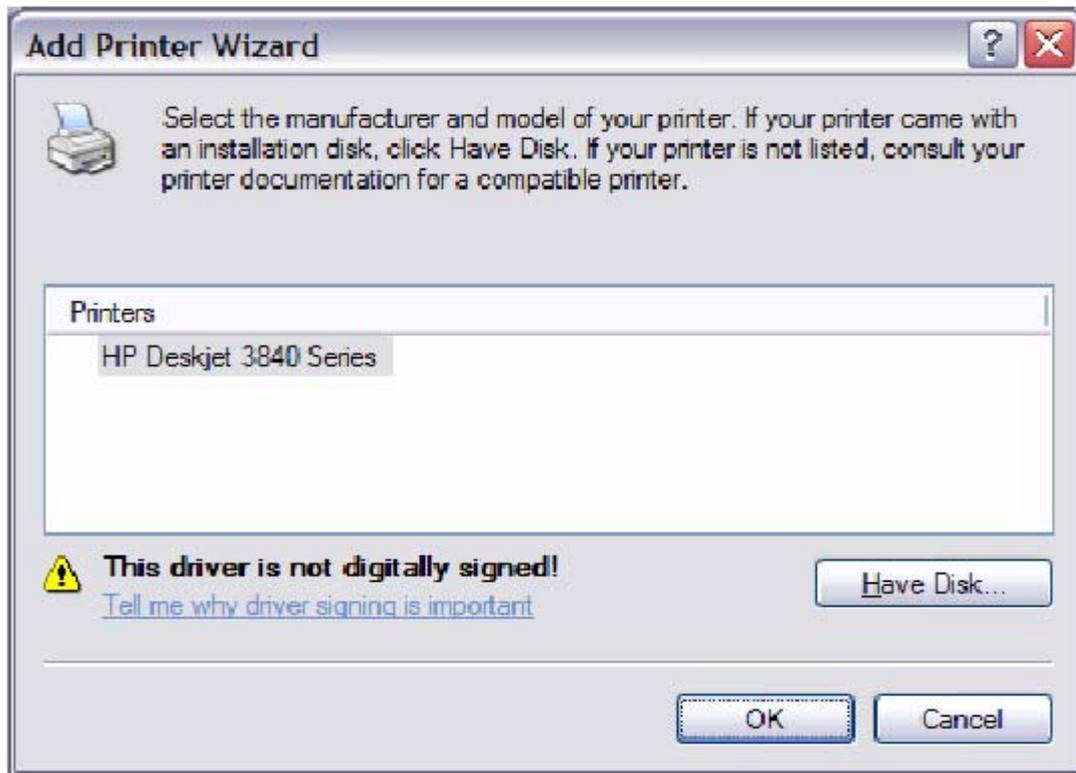
Step 5: Click "Have Disk", insert printer driver CD.



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



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



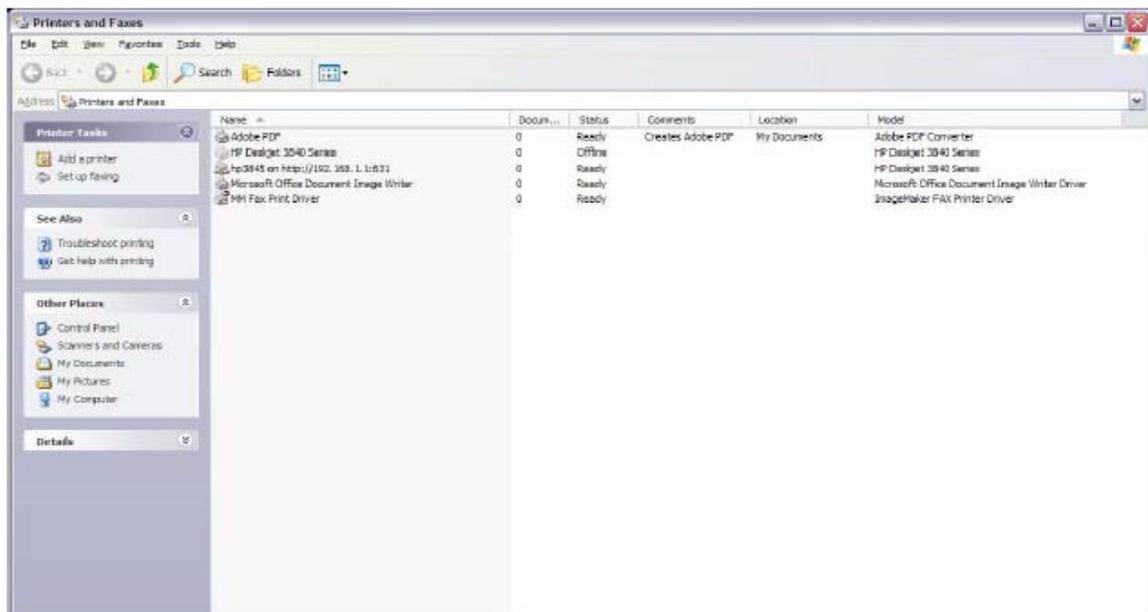
Step 8: Choose "Yes" or "No" for default printer setting and click "Next".



Step 9: Click "Finish".



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



Appendix B: Firewall

Stateful Packet Inspection

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

Denial of Service attack

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

TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3. When a Routing interface is created "Enable Firewall" must be checked. Navigate to Advanced Setup -> Security -> IP Filtering, web page.

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

Filter Name: User defined Filter Name.

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

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

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

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

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

Examples:

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

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

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

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

Incoming IP Filtering:

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

Filter Name: User defined Filter Name.

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

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

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

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

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

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

Examples:

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

Selected WAN interface: mer_0_35/nas_0_35

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

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

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

MAC Layer Filtering:

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

Global Policy:

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

To setup a rule:

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

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

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

Frame Direction:

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

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

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

Examples:

1.

Global Policy: Forwarded

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: NA

Frame Direction: LAN => WAN

WAN Interface Selected: br_0_34/nas_0_34

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

2.

Global Policy: Blocked

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: 00:34:12:78:90:56

Frame Direction: WAN => LAN

WAN Interface Selected: br_0_34/nas_0_34

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

Daytime Parental Control

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

User Name: Name of the Filter.

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

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

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

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

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

Example:

User Name: FilterJohn

Browser's MAC Address: 00:25:46:78:63:21

Days of the Week: Mon, Wed, Fri

Start Blocking Time: 14:00

End Blocking Time: 18:00

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

Appendix C: Pin Assignments

Line port (RJ11)

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

Pin Assignments of the RJ11 Port

LAN Port (RJ45)

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

Pin assignments of the LAN Port

Appendix D: Specifications

WAN Interface

ADSL Standard

ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ITU-T G.992.2, ANSI T1.413 Issue 2
G.992.3(ADSL2) Downstream: Up to 12 Mbps Upstream: 1.3 Mbps
G.992.5(ADSL2+) Downstream: Up to 24 Mbps Upstream: 1.3 Mbps

LAN Interface

Ethernet x 4

Optional USB Interface

USB2.0 host

WLAN

Standard IEEE802.11g, backward compatible with 802.11b

Encryption 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption

Channels 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)

Data Rate Up to 54Mbps

MAC Address Filtering, WPA, IEEE 802.1x

10, 25, 50, 100mW @ 22MHz channel bandwidth Output power level can be selected according to the environment

Analog Interface

FXS x 2, FXO x 1

ATM Attributes

RFC 2364, RFC 2684 (RFC 1483) Bridge; RFC 2684 (RFC 1483) Route; RFC 2516; RFC 1577

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

Management

TR069, SNMP, ILMI 4.0, Telnet, Web-based management, Configuration backup and restoration

Software upgrade via TFTP client or FTP server

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
IGMP Proxy	Yes
IGMP Snooping	Yes

Routing Functions

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

Security Functions

Authentication protocols	PAP, CHAP
VPN	PPTP/L2TP/IpSec pass-through
Stateful Packet Inspection, Packet filtering, Denial Of Service protection, Traffic Conditioning, WFQ-based Bandwidth Management, HTTP proxy	

QoS

L3 policy-based QoS, IP QoS, ToS

Voice Functions

MGCP	RFC 3435
Codec	G.711, G.723.1, G.729ab
RTP	RFC 1889
SDP	RFC 2327
Caller ID	ETSI based
Life line/Emergency call	Yes
Echo cancellation	G.168
Silence suppression	Yes

Power External power adapter

Input: AC100-240V,
Output: DC15V/ 1.6A

Environmental Conditions

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

Dimensions

205 mm (W) x 47 mm (H) x 145 mm (D)

Note: Specifications are subject to change without notice

Appendix E: SSH Client

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one "putty" that you can download.

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

To access the IAD using Linux ssh client:

From LAN: Use the IAD WEB UI to enable SSH access from LAN.

(default is enabled)

type: `ssh -l root 192.168.1.1`

From WAN: In the IAD, use WEB UI to enable SSH access from WAN.

type: `ssh -l support IAD-WAN-ip-address`

To access the IAD using Windows putty ssh client:

From LAN: Use the IAD WEB UI to enable SSH access from LAN

(default is enabled)

type: `putty -ssh -l admin 192.168.1.1`

From WAN: In the IAD, use WEB UI to enable SSH access from WAN.

type: `putty -ssh -l support IAD-WAN-ip-address`