CT-5364A 802.11n ADSL2+ Router User Manual

Version A2.0, May 17, 2010



261091-007

Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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

A WARNING

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

FCC Compliance

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment has been tested and found to comply with the limits for a Class Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

--Reorient or relocate the receiving antenna.

--Increase the separation between the equipment and receiver.

--Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

--Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval form Comtrend Corporation .Modification could void authority to use this equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. No change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

Copyright

Copyright©2010 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTA ILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE: This document is subject to change without notice.

Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Table of Contents

CHAPTER 1	INTRODUCTION	6
1.1 FEATUR	ES	6
1.2 APPLICA	TION	7
CHAPTER 2	INSTALLATION	8
2.1 HARDW	ARE SETUP	8
2.2 LED INI	DICATORS	. 10
CHAPTER 3	WEB USER INTERFACE	11
3.1 DEFAUL	T SETTINGS	11
3.2 IP CONF	IGURATION	. 12
3.3 LOGIN P	ROCEDURE	. 14
CHAPTER 4		. 10
4.1 AUTO Q	UICK SETUP	. 1/
4.2 IVIANUA	L QUICK SETUP	. 18
4.2.1	PPP Over ATM (PPPOA) and PPP Over Einernei (PPPOE)	. 20 25
4.2.2	MAC Encapsulation Routing (MER)	. 20 20
4.2.3	IP OVER ATIVI	. 29 22
4.2.4	Di luyiliy	. 32
CHAPTER 5	DEVICE INFORMATION	. 35
5.1 WAN		. 36
5.2 Statist	ICS	. 37
5.2.1	LAN Statistics	. 37
5.2.2	WAN Statistics	. 38
5.2.3	ATM Statistics	. 39
5.2.4	xDSL Statistics	. 41
5.3 Route .		. 44
5.4 ARP		. 45
5.5 DHCP		. 45
5.5 DHCP		. 45 46
5.5 DHCP CHAPTER 6 6 1 WAN	ADVANCED SETUP	. 45 . 46 . 46
5.5 DHCP CHAPTER 6 6.1 WAN 6.1 1	ADVANCED SETUP	. 45 . 46 . 46 . 47
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 47 . 49
5.5 DHCP CHAPTER 6 6.1 WAN <i>6.1.1</i> <i>6.1.2</i> 6.21 AN	ADVANCED SETUP VLAN Mux MSP	. 45 . 46 . 46 . 47 . 49 . 52
5.5 DHCP CHAPTER 6 6.1 WAN <i>6.1.1</i> <i>6.1.2</i> 6.2 LAN 6.3 NAT	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 49 . 52 . 55
5.5 DHCP CHAPTER 6 6.1 WAN <i>6.1.1</i> <i>6.1.2</i> 6.2 LAN 6.3 NAT <i>6.3.1</i>	ADVANCED SETUP VLAN Mux MSP Virtual Servers.	. 45 . 46 . 46 . 47 . 49 . 52 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2	ADVANCED SETUP VLAN Mux MSP. Virtual Servers. Port Triagering	. 45 . 46 . 46 . 47 . 49 . 52 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3	ADVANCED SETUP VLAN Mux MSP. Virtual Servers Port Triggering DMZ Host.	. 45 . 46 . 47 . 47 . 52 . 55 . 55 . 56 . 57
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4	ADVANCED SETUP VLAN Mux MSP Virtual Servers Port Triggering DMZ Host. ALG	. 45 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 56 . 57 . 58
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT	ADVANCED SETUP	. 45 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 56 . 57 . 58 . 59
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1	ADVANCED SETUP	. 45 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 56 . 57 . 58 . 59 . 59
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2	ADVANCED SETUP	. 45 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 55 . 57 . 58 . 59 . 59 . 61
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT	ADVANCED SETUP	. 45 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 55 . 57 . 58 . 59 . 59 . 61 . 62
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENTL 6.5.1	ADVANCED SETUP VLAN Mux	. 45 . 46 . 46 . 47 . 49 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENTL 6.5.1 6.5.2	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.1 6.4.2 6.5 PARENT 6.5.1 6.5.2 6.6 QUALIT	ADVANCED SETUP VLAN Mux MSP Virtual Servers Port Triggering DMZ Host ALG Y IP Filtering MAC Filtering AL CONTROL Time of Day Restrictions URL Filter Y OF SERVICE (QOS)	. 45 . 46 . 46 . 47 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT 6.5.1 6.5.2 6.6 QUALIT 6.6.1	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.1 6.5.2 6.6 QUALIT 6.6.1 6.6.2	ADVANCED SETUP VLAN Mux	. 45 . 46 . 47 . 52 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT 6.5.2 6.6 QUALIT 6.6.1 6.6.2 6.6.3	ADVANCED SETUP VLAN Mux MSP Virtual Servers Port Triggering DMZ Host ALG Y IP Filtering MAC Filtering AL CONTROL Time of Day Restrictions URL Filter Y of SERVICE (QOS) Queue Management Configuration QoS Classification	. 45 . 46 . 47 . 52 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT 6.5.2 6.6 QUALIT 6.6.1 6.6.2 6.6.3 6.7 ROUTIN	ADVANCED SETUP VLAN Mux MSP Virtual Servers Port Triggering DMZ Host ALG Y IP Filtering MAC Filtering AL CONTROL Time of Day Restrictions URL Filter Y of SERVICE (QOS) Queue Management Configuration QoS Classification G	. 45 . 46 . 47 . 52 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.2 6.6 QUALIT 6.6.1 6.6.2 6.6.3 6.7 ROUTIN 6.7.1	ADVANCED SETUP VLAN Mux MSP Virtual Servers Port Triggering DMZ Host ALG Y IP Filtering MAC Filtering MAC Filtering Time of Day Restrictions URL Filter Y of SERVICE (QOS) Queue Management Configuration QoS Classification G Default Gateway	. 45 . 46 . 47 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.2 6.6 QUALIT 6.6.1 6.6.2 6.6.3 6.7 ROUTIN 6.7.1 6.7.2	ADVANCED SETUP VLAN Mux MSP Virtual Servers. Port Triggering DMZ Host. ALG. Y. IP Filtering. MAC Filtering. AL CONTROL Time of Day Restrictions. URL Filter. Y OF SERVICE (QOS) Queue Management Configuration. Queue Configuration. Configurati	. 45 . 46 . 47 . 52 . 55 . 55 . 55 . 55 . 55 . 55 . 55
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.2 6.6 QUALIT 6.6.1 6.6.2 6.6.3 6.7 ROUTIN 6.7.1 6.7.2 6.7.3	ADVANCED SETUP VLAN Mux MSP. Virtual Servers Port Triggering DMZ Host ALG Y. IP Filtering MAC Filtering AL CONTROL Time of Day Restrictions URL Filter. Y of SERVICE (QOS) Queue Management Configuration Queue Configuration Queue Configuration QoS Classification G. Default Gateway Static Route RIP	. 45 . 46 . 47 . 55 . 55 . 55 . 55 . 55 . 55 . 55 . 5
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.2 6.6 QUALIT 6.6.2 6.6.3 6.7 ROUTIN 6.7.1 6.7.2 6.7.3 6.8 DNS	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 52 . 55 . 55 . 57 . 58 . 59 . 62 . 65 . 67 . 71 . 71
5.5 DHCP CHAPTER 6 6.1 WAN 6.1.1 6.1.2 6.2 LAN 6.3 NAT 6.3 NAT 6.3.1 6.3.2 6.3.3 6.3.4 6.4 SECURIT 6.4.1 6.4.2 6.5 PARENT, 6.5.2 6.6 QUALIT 6.6.2 6.6.3 6.7 ROUTIN 6.7.1 6.7.2 6.7.3 6.8 DNS 6.8.1	ADVANCED SETUP	. 45 . 46 . 46 . 47 . 52 . 55 . 55 . 57 . 58 . 59 . 62 . 65 . 67 . 71 . 71

6.9 DSL	73
6.10 Print Server	74
6.11 Interface Grouping	75
6.12 IP SEC	77
6.13 Certificate	80
6.13.1 Local	80
6.13.2 Trusted CA	82
CHAPTER 7 WIRELESS	83
7.1 Basic	83
7.2 Security	85
7.2.1 WPS	87
7.3 MAC FILTER	92
7.4 Wireless Bridge	93
7.5 Advanced	94
7.6 Station Info	96
CHAPTER 8 DIAGNOSTICS	98
8.1 Diagnostics	
CHAPTER 9 MANAGEMENT	99
9.1 SETTINGS	99
9.1.1 Backup Settings	99
9.1.2 Update Settings	99
9.1.3 Restore Default	100
9.2 SYSTEM LOG.	101
9.3 SNIMP AGENT	. 103
9.4 TR-069 CLIENT	. 103
9.5 INTERNET I IME	. 105
9.6 ACCESS CONTROL	. 106
9.6.1 Services	106
9.6.2 IP Addresses	107
9.6.3 Passwords	108
9.7 UPDATE SOFTWARE	. 109
9.8 REBOOT	110
APPENDIX A - FIREWALL	111
APPENDIX B - PIN ASSIGNMENTS	114
APPENDIX C - SPECIFICATIONS	115
APPENDIX D - SSH CLIENT	117
APPENDIX E - PRINTER SERVER	118

Chapter 1 Introduction

The CT-5364A 802.11n ADSL2+ Router provides wired and wireless access for high-bandwidth applications in the home or office. It includes one ADSL port and five 10/100 ase-T Fast Ethernet ports, with one Ethernet port assigned to the Ethernet WAN and the other four supporting LAN traffic. An added US host port supports printers. The front and back panels are TR-068 compliant, with colored panels and LED indicators that make for easy setup and use.

An integrated 802.11n (2x2 MIMO) WLAN Access Point supports faster connections (up to 270Mbps) and increased range compared with 802.11b or 802.11g protocols, without sacrificing compatibility with these older standards. A WPS (Wi-Fi Protected Setup) button is included for easy and secure wireless network setup. Security features include 64/128 bit WEP and WPA/WPA2 encryption, firewall and VPN.

1.1 Features

- Printer Server through US host 2x2 MIMO wireless antennas Ethernet WAN or ADSL access 802.11b/g backward-compatible • Auto PVC configuration, up to 16 VCs • Wireless Distribution System (WDS) DHCP Client/Server/Relay Wi-Fi Protected Setup (WPS) • Dynamic IP assignment Strong wireless security encryption • • Static and RIP v1/v2 routing WPA/WPA2 and 802.1x • **DNS Proxy/Relay** Supports remote administration Per-VC packet level QoS TR-069/TR-098/TR-111 protocols • IP/TCP/UDP QoS Configuration backup and restoration NAT/PAT Automatic firmware upgrade • IP/MAC address filtering **FTP/TFTP** server • Parental Control **RADIUS** client • UPnP Web-based management • IGMP Proxy Embedded SNMP agent WMM TR-068 compliant color connectors
- Integrated 802.11n AP

1.2 Application

The following diagram depicts the application of the CT-5364A.



Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



ADSL PORT

Connect the ADSL line to the ADSL port with a RJ-11 (telephone) cable.

LAN PORTS

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

ETH WAN PORT

Use RJ45 straight through or crossover MDI/X cable to connect to Ethernet WAN.

USB HOST PORT

The high-speed US 2.0 host connection connects compatible US devices. This firmware release supports most printers.

• Consult Appendix E for generic printer setup.

POWER ON

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected (see section 2.2 LED Indicators) then the CT-5364A is ready for use.

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

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

SIDE PANEL

The figure below shows the right-side panel of the device.



WPS BUTTON

Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode. When WPS is available the WPS LED will be ON.

Reset Button

Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 LED Indicators for details).

NOTE: If pressed down for more than 20 seconds, the CT-5364A will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

2.2 LED Indicators

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



LED	Color	Mode	Function
	Groop	On	The device is powered up.
	Green	Off	The device is powered down.
POWER	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
		On	An Ethernet Link is established.
LAN 4X-1X	Green	Off	An Ethernet Link is not established.
		link	Data transmitting or receiving over LAN.
		On	WPS enabled.
WPS	Green	Off	WPS disenabled.
		link	The router is searching for WPS clients.
		On	The wireless module is ready. (i.e. installed and enabled).
Wireless	Green	Off	The wireless module is not ready. (i.e. either not installed or disabled).
		link	Data transmitting or receiving over WLAN.
		On	An Ethernet WAN Link is established.
ETH WAN	Green	Off	An Ethernet WAN Link is not established.
		link	Data transmitting or receiving over Ethernet WAN.
		On	The ADSL link is established.
ADSL	Green	Off	The ADSL link is not established.
		link	The ADSL link is training.
		On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
INTERNET	Green	Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		link	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: root , password: 12345)
- User access (username: user, password: user)
- Remote WAN access: enabled
- Remote (WAN) access (username: support, password: support)
- WLAN access: enabled
- Service Set Identifier (SSID): Comtrend_xxxx, where xxxx are the last-four digits of the MAC address of the wireless interface.

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the CT-5364A powers up, the onboard DHCP server will switch on. The DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

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

- **NOTE**: The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.
- **STEP 1**: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- STEP 2: Select Internet Protocol (TCP/IP) and click the Properties button.
- STEP 3: Select Obtain an IP address automatically as shown below.

Internet Protocol (TCP/IP) Pro	perties ? X
General	
You can get IP settings assigned this capability. Otherwise, you no the appropriate IP settings.	d automatically if your network supports sed to ask your network administrator for
Obtain an IP address auto	matically
C Uge the following IP addre	58:
IP address	
Sybret mask	
Refeat pereway	
Obtain DNS server addres	s automatically
C Use the following DNS set	iver addresses
Ereferred DNS server	
Alemate DNS server	· · · · · · · · · · · · · · · · · · ·
	Advanced
	OK Cancel

STEP 4: Click OK to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead, as described on the next page.

STATIC IP MODE

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

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

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

- **STEP 1**: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- STEP 2: Select Internet Protocol (TCP/IP) and click the Properties button.
- **STEP 3:** Change the IP address to the domain of 192.168.1.x (1<x<255) with subnet mask of 255.255.255.0. The screen should now display as below.

Internet Protocol (TCP/IP) Prop	erties	<u> </u>
General		
You can get IP settings assigned this capability. Otherwise, you nee the appropriate IP settings.	automatically if your network supports id to ask your network administrator for alically	
Use the following IP address	ē	
IP address:	192 . 168 . 1 . 133	
Subnet mask:	255 . 255 . 255 . 0	
<u></u> elauit gateway:	+	
C Obtain DNS server address.	automotically	
. Use the following DNS serve	er addresses.	4
Preferred DNS server:		
Alternate DNS server:	+ + +	
	Advanced	
	OK Cano	el l

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

3.3 Login Procedure

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

NOTE:	The default settings can be found in section 3.1.	
	The deladit settings can be rearia in sootion of the	

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

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the <u>Quick Setup</u>

After login, the Quick Setup screen will appear as shown.

Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Quick Setup This Quick Setup will guide you through the steps necessary to configure your DSL Pouts ATM PVC Configuration Select the check box below to enable DSL Auto-connect process. IDSL Auto-connect
	Next

NOTE: The selections available on the main menu are based upon the configured connection type and user account privileges.

The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband 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 router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.

NOTE: Up to sixteen 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.

3.4 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

STEP 1: Select Quick Setup to display this screen.



- **STEP 2**: Click **Next** to start the setup process. Follow the online instructions to complete the settings. This procedure will skip some processes such as the PVC index and encapsulation mode selection.
- **STEP 3:** After the settings are complete, you can use the ADSL service.

3.5 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 Virtual Path I change VPI and V	dentifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not CI numbers unless your ISP instructs you otherwise.
VPI: [0-255]	0
VCI: (32-65535)	35
Enable Quality (Of Service
Enabling Qo5 for system resources, assign priorities fo	a PVC improves performance for selected classes of applications. However, since QoS also consumes the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to in the applications.
Enable Quality Of	Service
	Next

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

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION •
- PPPoE- LLC/SNAP RIDGING, VC/MUX MER- LLC/SNAP- RIDGING, VC/MUX •
- •
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX

	Router
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Connection Type Select the type of network protocol for IP over Ethernet as WAN interface C PPP over ATM (PPPA) PPP over Ethernet (PPPAE) C MAC Encapsulation Routing (MER) C IP over ATM (PoA) C IP over ATM (PoA) C IP over ATM (PDA) C IP over ATM (PDA)

NOTE: Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

Besides Linfle Quarks services Advected Sectory Winnies Disponetics Management If Winnies is used and Popowend to enderse your correction. In the boosts before, server the user memory provide Sectory Winnies Disponetics Management If User under Winnies Disponetics Management If Winnies Disponetics Management If User under Winnies Disponetics Management If Winnies Disponetics Management If User under Minnies Disponetics Management If Winnies Disponetics Management If Disponetics Management If Disponetics Management If Disponetics Management Management If Disponetics Management	COMTRINO	Router
(real free)	Device Info Quick Settap Advanced Settap Wireless Disprosetics Management	PPP Usersame and Papawerd PPP quarky repares that you have a same range and papaword to establish your correction. Is the bound before, infer the user name are parameter that your fifth that provided to you. PPP thermanic PPPP thermanic PPPP therm

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 WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.

N	Dial on demand (with idle timeout timer)
Inac	tivity 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. PPP IP Extension does the following:

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

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

Use Static IP Address

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

Retry PPP password on authentication error

Tick the box to select.

Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports

If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU

Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click Next to display the following screen.

COMPREND O	Router		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Enable IGMP Multicas Enable IGMP Multicast Enable WAN Service Service Name	it, and WAN Service	Back Next

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

STEP 6: After entering your settings, select Next. The following screen appears.

and the second	Device Setup		
and the second se	Configure the DSI	Router IP Address and Subnet Mask fo	r LAN interface.
Device Info	TO Address:	192 168 1 1	
Quick Setup Advanced Setup Wireless	Subnet Mask:	255.255.255.0	
Diagnostics	O Deable DHC	Server	
Management	Enable DHCP	Server	
	Start IP Addr	ISS: 192.168.1.2	
	End IP Addre	8: 192.168.1.254	
	Subnet Mask	255.255.255.0	
	Leased Time	hour): 24	
	Configure the	second IP Address and Subnet Mask for	LAN Interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the second I	P Address and Subnet Ma	isk for LAN interface
IP Address:		
Subnet Mask:		

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
Device Info	Wireless Setup Enable Wireless 🗵
Quick Setup Advanced Setup Wireless	Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back Next

Click **Next** to display the final setup screen.

ADSL	Router		
and the second second	WAN Setup - Summ	nary	
Device Info	Nake sure that the set	targs below match the se	things provided by your BSP.
Quick Setup	VPL / VCI:	0/38	
Advanced Setup	Connection Type:	PPPOE	
Wireless	Service Name:	pupoe_0_0_35_1	
Harragement	Service Category:	0.04	
nanayenen.	JP Address	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Enabled	
	Firewalt	Disabled	
	EGMP Multicast:	Chiabled	
	Quality Of Service:	Disabled	
	Clck "Save Reboot" to NOTE: The configurat	o save these settings and ion process takes about 1	reboot router, Click "Back" to make any modification minute to complete and your DSL Router will reboo Back Save-Reboot

 Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

3.5.2 MAC Encapsulation Routing (MER)

Step 4: Select the MAC Encapsulation Routing (MER) radio button and click **Next**.

	WAR P Settings
Devike Taila Quiki Settap Advancad Settap Management Management	The information provided to you by your DP to tondy or D port Chartest as WMA (P perform). Nature: DACP ten is a mainted for VVC on HER mode or P poor Chartest as WMA indefends & "Distance or P address indemnticably" in these should be address of address of the DEC of other ten sub-indexed to the VC on HER mode or P poor Chartest as WMA indefends & "Distance or P address of distability for indexed to represent from OCCP or other WMA consistent. Configuring them with indexed to the WMA consistent address of the DEC of other ten sub-indexed to the P address of the indexed to the VAN of the P address of the DEC of the P address of the IP address of the indexed of the P address of the IP a
	min min

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

NOTE:	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"
	field. Your ISP should provide the values to be entered in these fields.

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

	touter
	Hotsoork Address Toarslation Settings
Deske Julia	Network Address Translitter (1947) alove you to share one Wile Anal Network (WAR) IP address for multiple computers on your Local A Network (1946).
Quick Sotup Advanced Setial	trute NAT ET
www	Enable Fullcare full?
LAN Quality of Service Routing	Strates Prevail []
DSL Skove DSL	Evaple 1GHP Multitud, and WMA Service
Print Server	Engle X00 Puttont
1PSec	tolein sinte perven E
Certificate: Witning	Bervau Haven: Petr, 8, 0, 23
Newgeneri	linck [post]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

	Device Setup
Device Info	compute the DSL Houter of Address and Subnet Mask for LAW Interface.
Quick Setup	IP Address: 192,168.1.1
Advanced Setup	Subnet Mesk: 255,255,255,0
Diagnostics	C Disable DHCP Server
Management	C Enable DHCP Server
1990 - Tradition	Start IP Address: 192.168.1.3
	End IP Address: 192.168.1.254
	Subnet Mask: 255.255.255.0
	Leased Time (hour): 24
	C Enable DHCP Server Relay
	DHCP Server IP Address:
	Configure the second IP Address and Subnet Mask for LAN interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the seco	ind IP Address and Subnet Mask for LAN interface
IP Address:	
Subnet Mask:	

Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

COMTREND O	Router
	Wireless Setup
Device Info Quick Setup Advanced Setup	Enable Wireless Enter the wireless network name (also known as SSID). SSID: Comtrend
Wireless Diagnostics Management	Back Next

Click **Next** to display the final setup screen.

WAN Setup - Sum Nake sure that the s	mary ettings ballow match the se	tange provided by your 15#.
VPL/VCI:	0/36	
Connection Type:	MER.	
Service Name:	mer_0_0_25	
Service Category:	184	
IP Addressi	Automatically Assigned	
Service State:	Enabled	
NAT:	Enabled	
Firewalt	Deabled	
EGMP Hulticastz	Disabled	
Quality Of Service	Disabled	
Cick "Save/Reboot" NOTE: The configura	to save these settings and ton process takes about 1	neboot router. Click "Back" to make any modification minute to complete and your CSL Router wil reboot.

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

3.5.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.

Device Julio Quich Settup Advanced Settap Wireless Disgrootics Hanagement	Web IP Settings Enter information provided to you by your EP to configure the Web IP settings. Notice: 2010" is not supported in Prok made. Changing the default polynow or the DEC effects the whole system. Configuring them with static values will dealed in a subscription from other Web connection. Web IP Address: IIIIII Web IP Address: IIIIII IP use The following default generation IP use The following default generation IP use The following default generation: IP use The following default server midteneses: IP use the following default server: IP userver: IP use the fol
	[mar] mar]

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

	Router
Deske Isla (Jukk Setap Advanced Setap Wirekes Dispositio	Network Address Transletion (NFT) allow you to does one Web Ana Servers (NVH). IP address for multiple componence your Lacol Ana Retrieves (NVH). Exoto NRT (E) Exoto Fair (E) Exoto Friend FT
	Tradile TOMP Hubborg, and WWN Nervico Tradile TOMP Hubborg Ended WWN Service Annual WWN Service Annual WWN Service Annual WWN Service
	(Back) [Nort]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: This option becomes available when NAT is enabled

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

- and	Device Setup		
	Configure the DS	Router IP Address and Subnet Mask for LAN	interface.
Device Info Duick Setup	IP Address:	192.168.1.1	
Advanced Setup	Subnet Mask:	255.255.255.0	
Diagnostics	O Disable DHCP Server		
Management	Enable DHCR	Server	
	Start IP Addr	ess: 192.168.1.2	
	End IP Addre	ss: 192.168.1.254	
	Subnet Mask	255.255.255.0	
	Leased Time	(hpur): 24	
	Configure the	second JP Address and Subnet Mask for LAN a	nterface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the sec	cond IP Address and Subnet Mask for LAN Interface
IP Address:	
Subnet Mask:	

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
	Wireless Setup
Device Info	Enable Wireless 🖾
Quick Setup Advanced Setup Wireless	Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back, Next

Click **Next** to display the final setup screen.

ADSL	Router WAN Setup - Summ Hale sure that the set	tary Dings below match t	ie settings provided by your 257.
Device Info	MRE / MCT-	0.035	
Advanced Setup	Councilian Tamar	WY JU:	
Wireless	Sandra Name:	ince (1.0.25)	
Diagnostics	Service Category	000,0,0,0,00	
Management	ID Address:	123 124 125 126	
	Service States	Follow	
	HAT:	Enabled	
	Growalt	Okabled	
	IGNP Multicast:	Onatled	
	Quality Of Services	Cisabled	
	Clek "Save/Raboot" I NOTE: The configurat	o save these setting on process takes ab	and reboot router. Clok "Back" to make any modifications out 1 minute to complete and your DSL Router will reboot.

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

3.5.4 Bridging

Step 4: Select the ridging radio button and click Next. The following screen appears. Select Enable Bridge Service and click Next.

	Router		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Unselect the check b Enable Bridge Service: Service Name:	iox below to disable t	his WAN service Back Tiest



	Router		
Device Info Quick Setup Advanced Setup	Device Setup Configure the D IP Address: Subnot Mask :	3. Router IP Address and Sub 192.168-1.1 255.255.255.0	net Mask för your Local Area Network (LAN).
Wireless Diagnostics Management			Back Barrt

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

COMTREND O	Router
- and	Wireless Setup
Device Info	Enable Wireless 🗵
Quick Setup Advanced Setup	Enter the wireless network name (also known as SSID).
Wireless Diagnostics Management	Back Next

Click Next to display the final setup screen.

ADSL	Router WAN Setup - Summ	nary	
	Make sure that the se	ttings below mat	to the settings provided by your ISP.
Device Info Quick Setup	VPL/ VCE	0/35	
Advanced Setup	Connection Type:	thradige	
Wireless	Service Name:	br.0.0.28	
Diagnostics	Service Category:	UBR	
rianagement.	IP Address:	Not Applicable	
	Service State:	Childled.	
	NAT:	trabled	
	Firewalt:	Disabled	
	IGNP Hubicestr	Not Applicable	
	Quality Of Services	Deabled	
	Click "Save/Relicot" I NOTE: The configurat	o save these set ton process take	ings and reboot router. Click "Back" to make any modification about 1 minute to complete and your DSL Router tell reboot

 Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

Device Information screen and login with remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter the default

username and password, as defined in section 3.1 Default Settings.

Connect t	o 192.168.1.1	? 🗙
7		
The server 192.1 and password. Warning: This se password be serv without a secure	68.1.1 at DSL Router requires a rver is requesting that your user t in an insecure manner (basic au connection).	username name and thentication
User name:	🖸 root	*
Bassword:		
	Remember my password	
	ok [Cancel

Click **OK** to continue.

NOTE: The login password can be changed later (see section 0).

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



Chapter 4 Quick Setup

After login, the **Quick Setup** screen will appear as shown.





The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband 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 router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.
NOTE: Up to sixteen 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.

4.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

STEP 1:	Select Quick	Setup to dis	play this screen
NO.			

	Router
Sec. 10	Quick Setup
and the second	This Quick Setup will guide you through the steps necessary to configure your DSI. Router
Device Info Quick Setup	ATM PVC Configuration
Advanced Setup	Select the check box below to anable DSL Auto-connect process.
Diagnostics Management	DSL Auto-connect

- **STEP 2**: Click **Next** to start the setup process. Follow the online instructions to complete the settings. This procedure will skip some processes such as the PVC index and encapsulation mode selection.
- **STEP 3:** After the settings are complete, you can use the ADSL service.

4.2 Manual Quick Setup

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

*	
COMTREND O	
ADSLI	Router
	Quick Setup
Design Info	This Quid: Setup will guide you through the steps necessary to configure your DSL Router
Duick Setup	ATM PVC Configuration
Advanced Setup	
Wireless	Select the check box below to enable DSL Auto-connect process.
Diagnostics	Disk Auto-connect
Management	
	Untick this checkbox to enable manual
	setup and display the following screen.
The Virtual Path Identifier	(VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not
change VPI and VCI numb	ers unless your ISP instructs you otherwise.
VPI: [0-255] 0	
un ha const	
Art: (15,000101 [20	
Enable Quality Of Servi	CP
and the second second	
Enabling QoS for a PVC in	proves performance for selected classes of applications. However, since Qo5 also consumes
system resources, the num	der of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to intrations
marga priorities for the ap-	anaporta.
Enable Quality Of Service	
	Next

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

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP RIDGING, VC/MUX
- MER- LLC/SNAP- RIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX



NOTE: Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

ADS	Router
-	PRO (Nermanie and Postaneed
	FPP standy reparts that you have a sam reave and personni to establish your connection in the toxets before, letter the user mere an parameterid that your their has provided to you.
Quick Setup Quick Setup Wireless Dioprostics Masagement	PHH Udertwirze: PHH Udertwirze: PHH Schwirze:
	Hentry PEP pareneted in addentication error Evalue PEP Debug Marke Evalue PEP Debug Marke
	East Test

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 WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.

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

PPP IP Extension

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

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

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

Use Static IP Address

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

Retry PPP password on authentication error

Tick the box to select.

Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports

If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU

Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click Next to display the following screen.

BOMHRITED O	outer		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Enable IGMP Multicas Enable IGMP Multicast Enable WAN Service Service Name	et, and WAN Service	Back North

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

STEP 6: After entering your settings, select **Next**. The following screen appears.

jure the DSL R fress: it Mask:	outer IP Address and Subnet Mask for 192.168,1.1 255.255.255.0	LAN interface.
tress: et Mask:	192.168.1.1 255.255.255.0	
it Mask:	255.255.255.0	
it Planet.	433.433.433.0	
	BALACE IN THE REPORT	
Hable DHCP 5	erver	
inable DHCP S	erver	
tart IP Address	8 192.168.1.2	
nd IP Address:	192.168.1.254	
ubnet: Mask:	255.255.255.0	
eased Time (ho	our): 24	
	tart IP Address nd IP Address abnet Mask: eased Time (ho	tart IP Address: 192.168.1.2 nd IP Address: 192.168.1.254 ubnet Mask: 255.255.255.0 eased Time (hour): 24

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the second I	P Address and Subnet Ma	isk for LAN interface
IP Address:		
Subnet Mask:		

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

GOMTREND O	Router
- Series	Wireless Setup
Device Info Quick Setup Advanced Setup Wiseless	Enable Wireless 🖻 Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back Next

Click Next to display the final setup screen.

ADSL	Router		
	Hate sure that the set	sary tangs below match the se	ttings provided by your ISP.
Quick Setup	VPE / VCE:	0/35	
Advanced Setup	Connection Type:	PPPOE	
Wireless Diagnostiks Management	Service Name:	pppoe_0_0_35_1	
	Service Category:	UDR.	
	IP Address:	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Enabled	
	Firewalt	Disabled	
	EGMP Multicast:	Deabled	
	Quality Of Service:	Disabled	
	Clck "Save Reboot" to NOTE: The configurat	o save these settings and ion process takes about 1	reboot router, Click "Back" to make any modification minute to complete and your DSL Router will reboo

 Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.



Step 4: Select the MAC Encapsulation Routing (MER) radio button and click Next.

	WWW IP bettings
Deeks Inio Ookis Setap Advanced Setap Markes Hastaperent Mastaperent	Exter Information provided to you by your UP to configure the WMA 2P patterns. Instrum. DATE: The tax is included to you by your UP to configure the WMA reactions of "determs automatically" is showed which reaction or the URE effects the indust sources. Configure there will determ will determ the industry of the URE effects the indust sources. Configure there will determ and the term of the industry of the URE effects the industry of the URE effects the industry. If workpare the original automatically automatically a statement. If which an industry of the URE effects the industry of the URE effects the industry of the URE effects the industry of the URE effects and there exists a statement of the industry of the URE effects the tax industry of the URE effects and the industry of the URE effects

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

NOTE: 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" field. Your ISP should provide the values to be entered in these fields.

Step 5: Click Next to display the following screen.

	Router
	Notwork Address Translation Settings
Deske tala Caka Setua	Sensors, Address Translator (SAT) alone you to share one Wile-Ana Nebork (WAR) 37 address for multiple computers on your Local An Nebolin (LAN).
Advanced Settings	Structure HART EE
WAN	Knatter Fallbane teht
LAN Quality of Service Reading	from Prevail []
DSL Slave DSL	Enable IGNEP Multitant, and WMA Service
Print Server	Dage 300 Particult.
Port Mapping 1PSec	tume ministervan gr
Certificate: Witelawa	The out Harms: Prof. R.O. 21
Reseguent	linck [rust]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

	Device Setup
Device Info	Configure the DSL Notice of Address and Sublet Mask for LAW Interface.
Quick Setup	IP Address: [192.168.1.1
Advanced Setup	Subnet Mesk: [255.255.255.0
Diagnostics	C Dispile DHCP Server
Management	G Enable DHCP Server
	Start IP Address: 192.168.1.3
	End IP Address: 192.168.1.254
	Subset Mask: 255.255.255.0
	Leased Time (hour):24
	C Enable DHCP Server Relay
	DHCP Server IP Address:
	10199-1446-001005940-0031
	Configure the second IF Address and Subnet Mask for LAN interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the seco	ind IP Address and Subnet Mask for LAN interface
IP Address:	
Subnet Mask:	

Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
- Jow -	Wireless Setup
Device Info Quick Setup Advanced Setun	Enable Wireless Enter the wireless network name (also known as SSID).
Wireless Diagnostics Management	Back Next

Click **Next** to display the final setup screen.

WAN Setup - Sum Nake sure that the s	mary ettings ballow match the se	tange provided by your 15#.
VPL/VCI:	0736	
Connection Type:	MER.	
Service Name:	mer_0_0_25	
Service Category:	184	
IP Address	Automatically Assigned	
Service State:	Enabled	
NAT:	Enabled	
Firewalt	Deabled	
EGMP Hulticastz	Disabled	
Quality Of Service	Disabled	
Cick "Save/Reboot" NOTE: The configura	to save these settings and ton process takes about 1	neboot router. Click "Back" to make any modification minute to complete and your CSL Router wil reboot.

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

4.2.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.

Device Sala Qoks Setup Advanced Setup Mircless Diagnostics Management	WAR IP Sortings Enter information provided to you by your EP to configure the WAR IP antitings. Notice: DHO* is not supported in Prokematic compression from other Walk connection. WAR IP Address: WAR IP Address: In the following default generation If use the following default is not entimenant: If use the following default is not entif u
	Back North

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

	Router
Deske Isla (sakk Setap Advanod Setap Workes Dispositio	Network Address Transletion (NFT) allow you to does one Web Ana Servers (SUND) IP address for multiple componence your Local Ana Retrieves (SUND) Exoto NRT (E) Rindle Faktore NRT (E) Rindle Faktore NRT (E)
Heigenest	Enable TUNP Hulticor, and WWN Nervice. Enable 12/4 Multicor Enable WWN Service Anytic WWN Service Anytic Units
	(Back) [Next]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: This option becomes available when NAT is enabled

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

- And	Device Setup		
	Configure the DS	Router IP Address and Subnet Mask for LAN	interface.
Device Info Duick Setup	IP Address:	192.168.1.1	
Advanced Setup	Subnet Mask:	255.255.255.0	
Diagnostics	O Disable DHCP Server		
Management	Enable DHC	Server	
	Start IP Addr	ess: 192.168.1.2	
	End IP Addre	ss: 192.168.1.254	
	Subnet Mask	255.255.255.0	
	Leased Time	(hpur): 24	
	Configure the	second IP Address and Subnet Mask for LAN a	nterface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the sec	cond IP Address and Subnet Mask for LAN Interface
IP Address:	
Subnet Mask:	

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
	Wireless Setup
Device Info	Enable Wireless 🖾
Quick Setup Advanced Setup Wireless	Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back, Next

Click **Next** to display the final setup screen.

ADSL	Router WAN Setup - Sum	sary These below match t	to setting provided by your 707
Device Info	Phone succession of the sec	tings blow match t	a actuada tresiente pA liner ma-
Quick Setup	VPL/ VCI:	0.1.32	
Advanced Setup	Connection Type:	\$POR	
Wireless	Service Name:	(poe_0_0_35	
Diagnostics	Service Category:	UBR	
reanagement.	IP Address:	123.124.125.126	
	Service States	Enabled	
	NAT:	Enabled	
	Firewall:	Osabled	
	IGHP Multicast;	Clivabled	
	Quality Of Services	Created	
	Clerk "Sava-Weboot" to NOTE: The configurat	o save these setting on process takes ab	and reboot router. Clok "Back" to make any modifications out 1 minute to complete and your DSL Router will reboot.

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

4.2.4 Bridging

Step 4: Select the ridging radio button and click Next. The following screen appears. Select Enable Bridge Service and click Next.

	Router		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Unselect the check b Enable Bridge Service: Service Name:	ox below to disable t P br_0_0_35	his WAN service Bock Tiest



	Router		
Device Info Quick Setup Advanced Setup	Device Setup Configure the D IP Address: Subnot Mask :	3. Router IP Address and Sub 192.168-1.1 255.255.255.0	net Mask för your Local Area Network (LAN).
Wireless Diagnostics Management			Back Barrt

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

COMTREND O	Router
- and	Wireless Setup
Device Info	Enable Wireless 🗵
Quick Setup Advanced Setup	Enter the wireless network name (also known as SSID). SSID: Comtrend
Wireless Diagnostics Management	Back Next

Click Next to display the final setup screen.

	Router		
Davies Info	WAN Setup - Summ Note sure that the se	nary ttings below mat	th the settings provided by your ISP.
Quick Setup	VPL/ VCE	0/35	
Advanced Setup	Connection Type:	thridge	
Wireless	Service Name:	br_0_0_28	
Diagnostics	Service Category:	UBR	
ranagement	IP Address:	Not Applicable	
	Service State:	Enabled.	
	NAT:	trabled	
	Firewalt	Diskiel	
	IGNP Hubicast:	Not Applicable	
	Quality Of Services	Deabled	
	Click "Sews/Reboot" t NOTE: The configurat	o save these set ton process take	ngs and reboot router. Click "Back" to make any modifications about 1 minute to complete and your DSL Router tell reboot. Back Same/Reboot

 Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

Chapter 5 Device Information

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

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

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

COMTREND O	Router				
and the	Device Info				
	Board ID:	96358	AT-1221N		
Device Info	Model Name:	CT-53	64A		
WAN	Software Version:	A431-	312CTU-T02_	R04.A2p8025c1.d20i	
Statistics	Bootloader (CFE) Version:	1.0.37	-12.1-15		
Route	Wireless Driver Version:	4.174	4.174.64.12.cpe1.1		
ARP DHCP	Serial Number:	08A53	64A30(F-AL00	0046	
Quick Setup Advanced Setup	This information reflects the cu	rrent st	atus of your D	SL connection.	
Wireless	Line Rate - Upstream (Kbp	is):			
Diagnostics	Line Rate - Downstream ((bps):			
Management	LAN IPv4 Address:		192.168.1.1		
	Default Gateway:				
	Primary DNS Server:		192.168.1.1		
	Secondary DNS Server:		192.168.1.1		

The Device Info Summary screen displays at startup.

This screen shows hardware, software, IP settings and other related information.

5.1 WAN

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



5.2 Statistics

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

NOTE:	These screens are updated every 15 seconds.	

5.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

	Router								
	Statistics LAN	_	Dore	head			rance	nitto	đ
Device Info	ancone	Bytes	Plets	Ens	Drops	Bytes	Dists	Fres	Droos
Summary	Ethernet ENET(1-4)	401409	4330	0	0	666255	2491	0	0
WAN	Ethernet eth0	0	0	0	Ű.	2478	21	0	a.
LAN	Wireless	0	0	0	0	23588	241	0	0
WAN ATM ADSL	Reset Statistics								

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

5.2.2 WAN Statistics

This screen shows data traffic statistics for each WAN interface.

	Router		
Device Info Summary WAN Statistics LAN WAN ATM ADSL	Statistics WAN ServiceVPI/VCIProtocolInterface By Reset Statistics	Received tesPktsErrsDrop	Transmitted sBytesPktsErrsDrops

Service	Shows the service type
VPI/VCI	Shows the values of the ATM VPI/VCI
Protocol	Shows the connection type, such as PPPoE,
	PPPoA, etc.
Interface	Shows connection interfaces
Received/Transmitted - ytes	Rx/TX (receive/transmit) packets in bytes
- Pkts	Rx/TX (receive/transmit) packets
- Errs	Rx/TX (receive/transmit) packets with errors
- Drops	Rx/TX (receive/transmit) dropped packets

Heading		Description
Interface		WAN interfaces
Description		WAN service label
Received/Transmitted	- ytes - Pkts - Errs - Drops	Number of bytes Number of packets Number of packets with errors Number of dropped packets

5.2.3 ATM Statistics

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

	Router											
1000					AL	4 Interfac	e Statisti	ica .				
Device Info Summary	Ju Octuta	Out Octobs	Ju Eirors	lte Unikkown	In Hec Errors	In Invalid Vpi Vci Errors	la Port Not Errors	la PTI Enors	in Jile Celle	In Circuit Type Errors	In OAM BM CRC Errors	In GPC Envis
WAN	- 11	0	0	11	6	6	- 11	- 0	. 8	.0	- 11	- 8
Statistics		ANS Interfere Statistics										
WAN	In Och	eta Out	Octeta	In Dust P	kfa Out	Heavt Pid	in In Erro	rs Out I	anara (In Discar	the Out D	tecarrile
ATM			ų.	10		Ð	0		b	- 0		0
ADS					· .	and service	Ci attallar	1.0				
ARP DHCP	8	PL/WCI	CIIC D	turs SAR I	lineout	0versia	ed 500s	Short Po	chet Đ	nors Le	ligth Error	19
Quick Setup Advanced Setup						Reset	Cinse					

ATM Interface Statistics

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

AAL5 Interface Statistics

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

AAL5 VCC Statistics

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

ADSL	Router				
- Charles	Statistics - ADSL				
	Mode:				
	Type:				
Device Info	Line Coding:	Concerne and			
Summary	Status:	Link Down			
WAN	Link Power State:	1.0			
Statistics					
LAN	Down	stream Upstream			
WAN	SNR Margin (dB):				
ATM	Attenuation (dB):				
ATM	Output Power (dBm):				
ADSL	Attainable Rate (Kbps):				
Route	Rate (Kbps):				
ARP	Super Frames:				
DHCP	Super Frame Errors:				
Quick Setup	RS Words:				
Advanced Setup	RS Correctable Errors:				
Wireless	RS Uncorrectable Errors:				
Diagnostics	HEC Errors:				
Management	OCD Errors:				
	LCD Errors:				
	Total Cells:				
	Data Cells:				
	Bit Errors:				
	Total ES:				
	Total SES:				
	Total UAS:				

5.2.4	xDSL	Statistics
-------	------	-------------------

Field	Description
Mode	Line Coding format, that can be selected G.dmt, G.lite,
	T1.413, ADSL2
Туре	Channel type Interleave or Fast
Line Coding	Trellis On/Off
Status	Lists the status of the DSL link
Link Power State	Link output power state.
PhyR Status:	A new impulse noise protection technology that uses to
-	improve voice, data and video services.
SNR Margin (d)	Signal to Noise Ratio (SNR) margin
Attenuation (d)	Estimate of average loop attenuation in the downstream
	direction.

Output Power (d m)	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 Cells:	Total number of ATM cells (including idle and data cells)
Data Cells:	Total number of ATM data cells
it Errors:	Total number of bit errors
Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

In G.DMT mode the following section is inserted.

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

In ADSL2+ mode the following section is inserted.

MSGc	Number of bytes in overhead channel message
	Number of bytes in Mux Data Frame
Μ	Number of Mux Data Frames in FEC Data Frame
Т	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delav	The delay in milliseconds (msec)

In ADSL2+ mode the following section is inserted.

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

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

🗟 http://192.168.1.1/berstart.tst?berState=0 - M 🔳 🗖 🔀
ADSL BER Test - Start The ADSL BIT Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern
and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20 💌
Start Close
Done Done

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

5.3 Route

Choose **Route** to display the routes that the CT-5364A has found.

	ss Router						
Devke Info	Device Info - Flags: U - up, 1 D - dynamic (re	- Route - reject, G edirect), M	- gabeway, H - h modified (redir	eit, R ect).	- reinsta	te .	
Summary	Destination	Gateway	Subnet Hask	Flag	Metric	Service	Interface
Statistics Route ARP DHCP	192.168.1,0	0.0.0.0	255.255.255.0	u	0		htū

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

5.4 ARP

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

COMTREND O Wirele	SS Router	ARP		
	IP address	Flags	HW Address	Device
Summary WAN Statistics Route ARP	192.168.1.2	Complete	00:05:5D:A0:CD:E9	brū

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

5.5 DHCP

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

COMTREND (ss Router			
Device Info	Device Info Hostname	MAC Address	IP Address	Expires In
Summary WAII Statistics				
Route ARP DHCP				

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

Chapter 6 Advanced Setup

This chapter explains the following screens:



ADSL R	outer			
	IPSec Tunnel Node C	innectio	m	
Device Info	reat, successful to the same pro-		FEER CATEGORY AG	or one hade-
Advanced Sebap WAN		Enable	Connection Nome	Remote Galeway: Local Addresses: Remote Addresses
LAN				ASI New Committee
Security				
Parental Control Quality of Service				
Routing				
DSL				
Print Server				
Interface Group				
Certificate				

Click Add New Connection to add a new IPSec termination rule.

The following screen will display.

A STATISTICS OF A STATISTICS O	and the second	
	IPSec Settings	
	IPSec Connection Name	new connection
Device Info	Ramote IPSec Gateway Address	0.0.0.0
Advanced Setup	Tunnel access from local IP addresses	Subnet +
WAN	3P Address for VPN	0.0.0.0
NAT	1P Subnetmask	250.255.255.0
Security Parental Control	Turnel access from remote IP addresses	Subnet w
Quality of Service	IP Address for VPN	0.0.0.0
Routing DRS	IP Subnetmask	255,255,255,0
OSL	Key Exchange Method	Auto(IKE) +
Print Server	Authentication Method	Pre-Shared Key
IPSec	Pre-Shared Key	key
Certificate Wireless	Perfect Forward Secrecy	Disable w
Diagnostics Management	Advanced IKE Settings	Show Advanced Setting

IPSec Connection Name	User-defined label
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP
	address or domain name can be used.
Tunnel access from local IP	Specify the acceptable host IP on the local
addresses	side. Choose Single or Subnet.
IP Address/Subnet Mask for VPN	If you chose Single, please enter the host IP
	address for VPN. If you chose Subnet, please
	enter the subnet information for VPN.
Tunnel access from remote IP	Specify the acceptable host IP on the remote
addresses	side. Choose Single or Subnet.
IP Address/Subnet Mask for VPN	If you chose Single, please enter the host IP
	address for VPN. If you chose Subnet, please
	enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method		
Pre-Shared Key / Certificate (X.509) Input Pre-shared key / Choose Certificate		
Perfect Forward Secrecy	Enable or Disable	

Advanced IKE Settings	Select Show	v Advanced Setting	js to reveal
	the advance	ed settings options sh	nown below.
Advanced IKE Settings		Hide Advanced !	Settings
Phase 1		82	
Mode		Main	
Encryption Algorithm		3DES .	
Integrity Algorithm		MD5 💌	
Select Diffie-Helman Group for Key Exch	ange	1024bit •	
Key Life Time		3600	Seconds
Phase 2			
Encryption Algorithm		3DES 🖃	
Integrity Algorithm		MD5 -	
Select Diffie-Helman Group for Key Exch	ange	1024bt *	
Key Life Time		3600	Seconds
Advanced IKE Settings	Select Hide advanced se	Advanced Settings ettings options shown	s to hide the above.
Phase 1 / Phase 2	Choose sett options are	ings for each phase, separated with a "/"	the available character.
Mode	Main / Aggr	essive	
Encryption Algorithm	DES / 3DES	/ AES 128,192,256	
Integrity Algorithm	MD5 / SHA1		
Select Diffie-Hellman Group	768 – 8192	bit	

The Manual key exchange method options are summarized in the table below.

Manual Key Excha	nge Method	
Key Exchange Method	Manuel	
Encryption Algorithm	3DES 💌	1
EncryptionKey		DES: 16 digit Hex, 3DES: 48 digit Hex.
Authentication Algorithm	MES ·	
Authentication Key		MD5: 32 digit Hex, SHA1: 40 digit Hex
591	101 Hex 1	00-FFFFFFF
	Save / Ac	zeiv -
Encryption Algorith	าทา	DES / 3DES / AES (aes-cbc)
Encryption Key		DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Alg	orithm	MD5 / SHA1
Authentication Key	/	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

Certificate

6.1 WAN

This screen allows for the advanced configuration of WAN interfaces.

Wireless Ro	outer
Device Info Advanced Sotap Layer2 Interface WAB Service UAI Secartly Forestal Control Quality of Service Routing DBS DBS DBS DBS DBS DBS DBS DBS DBS DBS	Wide Area Betapik (WAN) Service Ketap Crocus Add, or Remove to corligans a WAN service over a selected mightee. ATH and PTM/ATM service can not caused. Interfaces [Insectiption] Type [Viscott222] [Viscottadd] (Insectint Igray BAT Prevail Remove (Interfaces] (Insectiption] Type [Viscott222] [Viscottadd] (Insection] (I

To Add a WAN connection, click the Add button. To edit an existing connection, click the Edit button next to the connection. To complete the Add or Edit, on the opening screen, select VLAN Mux (see section 5.1.1) and then proceed to STEP

2 in section Manual Quick Setup.

- To remove a connection select its radio button under the **Remove** column in the table and click the **Remove** button under the table.
- **Save/Reboot** activates the new configuration.

VPI/VCI	VPI (0-255) / VCI (32-65535)					
VLAN Mux	Shows 802.1Q VLAN ID					
Con. ID	ID for WAN connection					
Category	ATM service category, e.g. U R, C R					
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					
NAT	Shows enable or disable NAT					
Firewall	Shows enable or disable Firewall					
QoS	Shows enable or disable QoS					
State	Shows enable or disable WAN connection					
Remove	Select or deselect the connection for removal					
Edit	Click Edit to change connection settings					

6.1.1 VLAN Mux

VLAN Mux is a form of VLAN tagging that allows multiple protocols over a single connection. It is especially useful for VDSL2 connections in packet transfer mode.

This option is found on the Advanced WAN Setup screen. This is the first screen you will see when adding or editing a connection. VLAN Mux can be enabled by selecting the **VLAN Mux – Enable Multiple Protocols Over a Single PVC** check box, outlined in red below. Enter a value between 0 and 4095 for **802.Q VLAN ID**.

- Starter	ATM PVC Configuration This screen alows you to configure an ATM PVC identifier (VPI and VCI) and select a
Name and Address	enable t.
Device Info	586/32.322
Quick Setup	VP[: [0-255] 0
Advanced Setup	WTI- 132-655351 35
WAN	And for second for
Quality of Service	VLAN Mux - Enable Multiple Protocols Over a Single PVC 🕑
Routing	802 10 VLAN ID: [0.4095][2
DSL	several stress to Tournal is
Slave DSL	Service Category: UBR Wahaut POR 🖌
Print Server Port Mapping	Enable Quality Of Service
IPSec Certificate Diagnostics Management	Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Reatime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
100	Enable Quality Of Service, IT

After proceeding to **STEP 3** in section Manual Quick Setup, the screen will appear as follows. Notice that PPPoA and IPoA are not available.

Connection Type						
Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.						
O PPP over Ethernet (PPPoE)						
MAC Encapsulation Routing (MER)						
• Bridging						
Encapsulation Mode						
Back Next						

PVCs can be added using the regular procedure, however, now multiple protocols can exist over the same connection, as long as the 802.1Q VLAN IDs differ.

The graphic below shows an example of three protocols over the same connection.

Wide Area Network (WAN) Setup

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

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat -	Firewall	QoS	State	Remove	Edit
0/35	1	1	UBR.	br_0_0_35.1	nes_0_0_35.1	Bridge	N/A	N/A	N/A	Disabled	Enabled		Eðt
0/35	2	2	UBR	mer_0_0_35.2	nas_0_0_25.2	MER	Disabled	Enabled	Enabled	Disabled	Enabled		Eðt
0/35	3	3	UBR.	pppoe_0_0_35_3	ppp_0_0_35_3	PPPoE.	Disabled	Disabled	Disabled	Disabled	Enabled		Eðt

Add Remove Save/Reboot

6.1.2 MSP

Multi-Service over PVC (MSP) supports multiple protocols over a single connection. As with the VLAN Mux function, PPPoE, ridge and MER protocols can coexist, while IPoA and PPPoA are not supported. This function supports remote management by bridge protocol in addition to multimedia applications over a single PVC.

Configuring MSP is a two-part process:

Part 1 - Create multiple PVCs (One ridge + multiple PPPoE / One MER)

Part 2 - Use Port Mapping to connect LAN / WAN interfaces

The following example shows how to configure a ridge / PPPoE MSP connection. The same process can be used for ridge / MER MSP connections.

NOTE: If QoS is configured on the first MSP connection, it will be configured by default for all subsequent connections. If a MSP connection is removed every other MSP connection should be removed to avoid port mapping configuration problems.

Part 1 – Create Multiple PVCs

On the Advanced Setup – WAN screen, create one PPPoE connection and one ridge connection on the MSP supporting PVC. The screen will display as follows.
Wide Area Network (WAN) Setap

Choose Add, Edit, or Ramonie to cardigues VANI interfaces. Choose Some/Reduct to apply the changes and reboot the system

YPE/YCE	VLAR Phot	Con. ID	Category	Service	Interface	Protocal	Jana	Ret	treval	015	State	Remove	the
4/28	0#	1	UR.	RUUR	106.0.3.35	Bridge.	hjh	hβk.	14/4	Disabled	fradied	п	2011
0.738	-017	2	Link	popte_0_0_30_3	CILLURE I	HERE	Dashed	Enabled	Budled	Disbled	Budded	г	1201

All Remove SeverArthood

Part 2

Go to Advanced Setup – Interface Group screen and select the **Enable Virtual Ports** checkbox. The screen will display as follows.

Interface Grou	m – A ma	cetense	m 16 entries can be cor	Report
interface Group ou must create and add the ung R Enable virtu	sapports en mepping g rooped into mi ports en	ratiple projes enfects	e perfs to PVC and bridging with appropriate LAN and to the Default group. Geb 7(1-4)	groups, Each group will perform as an independent network. To support this featur WAN interfaces using the Add button. The Remove button will remove the grouping the default group has IP interface.
Group Name	Remove	Edit	Interfaces	
			1250	
			4700	
			Wireless(SSID1)	
			Wirekes_Guest(95102)	
the local sectors of			Wireless, Guents (55800)	
Desaut			Wirelens, Guerr2 (SSID4)	
			ENETS	
			ENET2	
			ENETJ	
			ENET4	



the format of "nas_x_y_z" where x=port, y=vpi, and z=vci.

To continue, click the **Add** button at the bottom of the screen shown above. On the next screen, select the bridge connection and one Ethernet virtual port (ENET 1-4) and enter a **Group Name**, such as "MSP1", as shown below. Click **Save/Apply**.

Grouped Interfaces		Available Interfaces		
ENET2 Wireless(SSID1)	-> <-	eth0 ENET1 ENET3 ENET4 USB Wireless_Guest(SSID2) Wireless_Guest1(SSID3) Wireless_Guest2(SSID4)		

If successfully configured, the Port Mapping screen will display as follows.

derfate Group	supports m	uitple p	arts to FVC and bridging gro
ou must create	mapping g	respt wi	th appropriate LAN and WA
nd not the only	roopes mis	510CES 10	The Deletic group. Only the
Bugble virta	el ports en	ENET!	1.40
Group Name	Remove	THE	Interfaces
			1.521
			100
			Wireless_Gasel(SSID2)
			Wheten_Guest1(SSID3)
Contraction			Wheless_Geiest2(SSID4)
			EVET1
			EVET2
			EVET4
MSPt		249	Wielesi(SSBD1)
	- 64	L'UR.	ENET2

NOTE: If you wish to maintain local access to the web user interface, avoid grouping the Ethernet interface that is attached to the host PC.

6.2 LAN

Configure local area network (LAN) settings here.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

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

Force IGMP Proxy version on WAN side: V2 is selected by default. Select V3 if required.

Enable IGMP Snooping: Enable by ticking the checkbox \square .

Standard Mode:	In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.
locking Mode:	In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

Enhanced IGMP: When enabled, IGMP packets will not flood to all bridge ports.

Allowed Mac Address: Displays the MAC address(es) allowed to pass throughput LAN interface.

DHCP Server: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. <u>This option is hidden if NAT is enabled or</u> <u>when the router is configured with only one Bridge PVC.</u>

Static IP Lease List: A maximum 32 entries can be configured.



To add an entry, enter MAC address and Static IP and then click Save/Apply.

Enter the Mac address	and desired IP address then click "Save/Ap
	N
MAC Address:	12:34:56:78:90:12
IP Address:	192.168.1.33

To remove an entry, tick the corresponding checkbox \square in the Remove column and then click the **Remove Entries** button, as shown below.

MAC Address	IP Address	Remove	
12:34:56:78:90:12	192.168.1.33		
Add Entries	Remove Entri	es	

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

2ND LAN INTERFACE

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

Configure the second I	P 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.

IP Address:		
Subnet Mask:		
	Save Sav	e/Reboot

NOTE:	The Save button saves new settings to allow continued configuration
	while the Save/Reboot button not only saves new settings but also
	reboots the device to apply the new configuration (i.e. all new settings).

Ethernet Media Type: Select from Auto, 10_Half, 10_Full, 100_Half or 100_Full for each Ethernet port.

6.3 NAT

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

6.3.1 Virtual Servers

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

	Route								
	NAT-VIE	taal Servers Setup	5						
Device Sofo Advorced Softage WAR LAN	Valual Serve addresse (or) pt the LAN	er allows you to door for LAN polo. The Int aldo: 4 machinety 32	traccounty tarffit b produpert to require archies part to card	yen, közek sár nő csely té bla Aggivent,	a ddentfod by Pr orderof peltine Acti Ration	olocsi mol Esterni ik koʻbe converted	(part) to the tab in a different pre	end server with Courtber used)	printis 19 11 Basierroy
NAT Virtual Servers Port Eriggering DNZ Hosi	Server Reter	External Part Short	External Part End	Protocol	Informal Part Start	Informal Part Eral	Server 0 ⁴ Address	Ricearia Ruel	Birunys

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

	Router
Device July Advanced Series WAR LAN NAT Without Servers Port Triggering DR2 Host AGS	MAT - Virtual Servers Select Reservice tarse, and other first server IP address and dolt. "Sever Apple" to invested IP projects for first service to the specified server. MOTE: The "Informal Fort Darf" correct bot the server is included. The "Informal Fort Darf" correct bot the server is included. Betternal Fort Darf" address bot theraped. II is the server as "Enformal Part Traf" assembly and sett bot the server as the "Information" part for a "Informal Part Traf" assembly and sett bot the server as the "Information" assembly and sett bot the server as the "Information" assembly a setting to the server as the "Information" assembly a setting to the server as the "Information" assembly assembly assembly a setting to the server as the "Information" assembly asse
Socarity	Extensial Part Start External Part Loal Produced Informal Part Start External Part Lad. Remarks for
Permital Central	TO [#]
Quality of Service	30F 😹
Roeting	107
UNEN INC.	10
Brick Server	729
Interface Group 1PSec	[See(Arste]

Consult the table below for field and header descriptions.

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

Field/Header	Description
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

6.3.2 Port Triggering

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

ADSL	Router								
Desice balo Advanturd Setag WAN LAN BAT	NAT — Part Trippering Setup Same applications reaches that up He Caper Port? In the Investiganty to Reader allows the rescale party to reasineers 12 intries can be config	ectile perta to the en an opplication no the Walte size point.	t factors fi on the LX r to relatio	result for upo A millules à T à tres contract Artic 6	ond the accel CP/20 P com Stone back to ethics	a by the remo wetter to a re the application	n partne, in mote párty le a na 11 e 1.M	nt Trigger dynamiaal alng the "Triggering P A date aalng the Ugen	r torris ig trib. The (Right', A
Virtual Servers		Application	10	500+F .:		por:	Birmerve:		
Port Triggering		News	Protocol	Perl Hange	Professi	Post Sarge	1		
ALG				Start End		Slat tod			

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

ADSL	Router					
Denice Tarlo Advanced Setap WAN LAN MAT Writeal Servers Port Triggering DHZ Heal ALG Secarity Perential Control Quality of Service Portice	NAT — Platt Traggering Some approximation and an annual for access for the Distance applications of a Application Nature & Select on application O Center application Dispace Point Start Leg	garves, eldeo conform policites. Tais car to las "Savelaget" to at intrine That can be o con Pret Coll Insper Top Top Top	org, which social ap of gare the part solver 12. orfsperst 12 bin ProtocolOpen Port	evalues and others recome in trees this screws to solve the evalues stant ligner. Post (SoldDares TOP TOP	fruit specific parts in the Hautar's fro op an outring application or crueing attraction	ned by poor ree
DRIS		TOP	1	TOP	1	
tes.		TOP		104	10	
and the second second		TOP		TOP	10	
PERSONAL INFORMATION					and the second se	

Consult the table below for field and header descriptions.

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

6.3.3 DMZ Host

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



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

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

6.3.4 ALG

SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) devices to initiate communication. A SIP ALG (Application Layer Gateway) assists VoIP packet traffic from a SIP-compliant IP phone or VoIP gateway to passthrough a NAT enabled router.

To enable the SIP ALG select the SIP Enabled checkbox and click Save/Apply.

	Router	
Device Info Advanced Setup WAN LAN NAT Virtual Servers Port Triggering DMZ Host	ALG Select the ALG below. SIP Enabled 5050	Save/Apply

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

6.4 Security

To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions, with examples, please consult Appendix A - Firewall.

6.4.1 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering (pg. 61) performs a similar function.

格式化: 醒目提示

OUTGOING IP FILTER

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

CONTINO (Router
Device Isla Afraacool Settap WAW LAN NAT Security IP Filtering Defigures Defigures	Oxfgeling IP Filtering Setup By dehait, of extgeling 3P fielfs from LAN is offered, but some IP buffs can be BLOCKED by setting as files. Oxone Add in Remove to configure oxyging IP filter. [Filter Nome:] Protocol [Source Address / Mask: Source Part Dest, Address / Mask Dest, Part Itemene [Add] _ Remove

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

ADSL	Router		
	Add IP Filter - Unitpring		
Denics Jolo Advanced Series MAN LAN NAT Security B7 Elicency Codgoing Laceoing Decessing Parental Control Quality of Service Routing 1985 D95 D95 D95 D95	The screet allows you to create a thir rule specified scattlines in this filter rule result like flater Protocol; Senters IP address: Senters Fuelderss: Senters Fuelderss: Senters Fuelderss: Senters Fuelderss: Deductors IP address: Deductors IP address: Deductors Fuelderss: Deductors Fuelderss:	In Scheddy, and guing 2P traffic by specifying a rese fifter name and at least one involution in to satisfied for the role to take effect. Units Schedungs// to save and activate the little.	leius. Al of Be

Consult the table below for field descriptions.

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

INCOMING IP FILTER

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

ADSI	Router
-	Incoming IP Effering Setup
Device Info Advenced Setag WAN LAN	By default, all hearing IP to the the MAN is Bodiel West to thread is enabled. Hearin, sens IP hefe cor is ADCEPTED by writing Bars. Choose Add or Remove is configure incoming IP litters. [Effer Name: VPI/VC] Protocol Tearror Address / Mask Source Post [Dest. Address / Mask Dest, Post [Remove]
Security IP Ethering Outgoing	[Ault] [. Bernow.]

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

	Router	
	Add 19 Filter - Jaconing The course down one to made a three down in	with investor Druffe in surflaint s can the core and a last on earther tales. At a
the second second	the specified catolitizes in this like rule must be	satisfied for the rule for late offset. Cirk "lane, Apply to save and adjusts for film:
Desize Jaho Advanced Schup WAU JAN JAN Socarthy Di Filluning Outpaining	Piller Henne Protocol Bourne 19 addresse Bourne Ford (prot or port port) Source Ford (prot or port port) Destination (Prothese)	<u>u</u>
Incoming Forestal Control Quality of Service	Dedhaboe Salaet Hak: Dedhaboe Part (port ar part pert)	
Routing DRS	MAN Interfaces (Configured in Roating mo Saled at least one or costable WAN interfaces do	die and with Teronal mainled only) glaged below to exply the rule.
DSL Frist Server Jaterface Group	H 1abd Af H mass, 3, 8, 25, 1500, 0, 0, 25, 1	
UPSec Certificate:		. Same/Applie

Consult the table below for field descriptions.

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

At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

6.4.2 MAC Filtering

NOTE:	This option is only available in bridge mode. Other modes use IP Filtering
	(pg. 59) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the CT-5364A can be set according to the following procedure.

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

	Router
- Andrews	MAC Filtering Setup
Device tolo Advanced Setup MAN LAN NAT	Change Patter Change Patter MAC Fibring is only effective as ATM PyCs configured in Midge mode. TORMARDED means that all MAC layer frames will be TORMARDED model these multilegraphic and Piles specified values in the following table. BLOCKED request that all MAC layer frames will be BLOCKED model these multilegraphic and Piles specified values in the following table.
Security 3P Efforcing HAC Efforcing Parental Control Quality of Service	Openar AM or Farmer in surfaces IVAC (Review odes, WEL/WCE Produced Institution INAC) Secure INAC, Finance Directions Researce (add) (Instance)

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

ADSL	Router		
	A44 MAC Filler		
Denker Defe	Otofa a filler to identify the Otob. "Apply" to salar and an	NAC later Bartes by specificate the Effect	iting at load one condition before. If multiple conditions are specified, all of them bake offer
Advanced Setup	CONTRACTOR OF	NOT STREET, ST	
WMI	Potoso Type.	1 H	
LAN	Demandon MAC Address		
RAT	Sastor PAC Address		
Security		and the second second	
IP Filtering	Preme Clinictine:	Consectants (w)	
MAC Pilkering	WAY Litertons (Colligated	(drow where we had	
Parental Control			
quarty or service	E telectual	2	
DMS.	H (0,0,0,0000,0,0,0,0	9	
051			C. Davidsonk
Print Server			and the second

Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, Net EUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to selected WAN interfaces in bridge mode. These rules are arranged according to these interfaces, as shown under the Interface heading on the previous screen.

6.5 Parental Control

This selection provides WAN access control functionality.

6.5.1 Time of Day Restrictions

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 9.5, so that the scheduled times _____ 格式化 醒目提示 match your local time.



Click Add to display the following screen.

	Router	
-	Time of Day Hestriction	
Denics Infe Advanced Settan	This page adds been of day re- polyness of the LAN device of w address of the sthet LAN device	blicker to a special LAR device connected to the Houles. The 'Wessen's MAC Address' automatically deplays the HAC ex the browner is rearring. To restrict other LAW device, club; the 'Other NAC Address' botter and when the MAC as, To their out the MAC address of a Windows based PC; go to command window and type "spooting /dif".
WAN	Line States	
LAN NAT Socarity Parovtal Cantrol	 B. Brawer's HRC Address D. Other HRC Address (internetional sector) 	000-25-11-0411-110-110
URL Filter Quality of Service	Days of the week Olick to week	Must FaceWord Disatest Soldiers
Roefing DHS DSL Print Sover Interface Group	Hart Hooking Trise (bk such) End Hooking Time (shown)	Somuligatio

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

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

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

Other MAC Address: MAC address of another LAN device.

Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

End Blocking Time: The time the restrictions end.

6.5.2 URL Filter

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

	Router	
	URL Filter - A maximum 100 entries can be configured.	
	URL List Type: O Exclude O Include	
Device Info	and the second relation denotes a bit on the	
Advanced Setup		
LAN	Address Port Rem	ov
NAT Security	Add Remove	
Parental Control URL Filter		

Click Add to display the following screen.

Parental Control — I	JRL Filter Add	
Enter the URL address	and port number then click "S	ave/Apply" to add the entry to the URL filter.
URL Address:	www.yahoo.com	-
Port Number:	80	(Default 80 will be applied if leave blank.)
		Save/Apply

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

URL Filter A maximum 10)0 entries can be	configured.		
URL List Type: 🔘 Exclude	O Include			
	[Address	Port	Remove
		Address www.yahoo.com	Port 80	Remove

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

6.6 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.

6.6.1 Queue Management Configuration

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

Click Save/Apply to activate QoS.

	Router
	Qu8 - Queve Management Configuration
Device Jafo	# Enable QcS checkine is selected, choose a default ESCP mark to automatically mark incoming teaffic without reference to a particular classifier. Click Sami/Apply/Saffine to associate
Advanced Setup WAR	Note: If Enable Qus checkbox is not selected, all QuS will be disabled for all interfaces.
LAR NAT	Note: The default DSCP mark to used to mark all egress packets that do not realch any classification rules.
Security Parental Control	E Inside Qrd
Quality of Berslow Quality Config	Scored Default (SSCP Hash Nis Change(-1)
Qe5 Classification Routing	Tearring Appropria

QoS and DSCP Mark are defined as follows:

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

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

6.6.2 Queue Configuration

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

the second se	Sect. Downey, Sund	and the second second	and the second	a search in search	farmer a	
and the second second	If you disable Wi	904 function in Wire	iless Pape, qu	s can be com even related	to wirele	ton life as
autos Info	Interfacename	Description	Precedence	Queue Key	Enable	Remove
dvanced Setup	wirobana	WMM Value Priority	1	1		
WAN	utreleas	WHM Water Priority	2	2		
NAT	wentered	WMM Video Priority	3	3		
Security	wheeless	WHM Video Priority	4	4		
arental Control Juality of Service	wheelers	WHIM Baat Effort	5;	5		
Queue Config	wheleas	WHM Background	6	0		
QoS Classification	windess	WMM Background	2	7		
NS	adaptation .	MARKA Hart Elbert			-	

Click Add to display the following screen.

	Router				
Device Jafo Advanced Setup WAN	QoS Queue Configuration The ensues allown per to a low discuted three gueues, will be used by the classifier priority for this queues	on orifyine a QuS (power o ly ninkal), Such of the or to place begins pack relative to others (2);	etry and assign it to a sy gamma can be cardigate of a operarticle). Note: A Steel Apple To Steel of	activ, rationik interface, i Flur a specific president Lower infogat valvea at activitic the litter,	Carly interface with Qell another will a. The galaxie with configured faces for precedence tegrily higher
LAN	Quesi Carlipsottes Mate	•{	in.		
MAT Security	Qwee:				
Parantal Control Quality of Service Queue Coofig Qu5 Classification	Queue Nocedesca:		in Roots (Apart		

Queue Configuration Status: Select Enable or Disable the Queue entry.

Queue: Assign queue to a specific network interface with QoS enabled.

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

6.6.3 QoS Classification

The network traffic classes are listed in the following table.

ADSL	outer
Annese Mala Addressed Versus	Quality of Society Interest is configure selected traffic means (Society - Review is configure selected traffic means) If your disation PART francisco in this class Pages, classific plate codded for an only on this set take officing
1.08	Anne Ander Same All 12 in Anne Ander Same Anne Anne Anne Anne Anne Anne Anne An
Parential Eastwol Quality of Involve Quarter County	East

Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

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

-	
THE REPARTMENT OF	
ADSL	Router
	Add theirsen's Yurffe Class Fale
	The screen probes a light station or plantly for qubits of the sample game which advant the products will be reinformed provide the P institute 2005 light A water second of a deep wave and is basis on excising balance. All of its specified continents to the simulations on work is another for the value field which. This filter "tagget to same and
Areke bdo	within the rule
Advectment Service	Traffic Harrison
1.00	and solar
641	Non-Tenner
describy	
Parantal control	Analysis A De Prior By gend (or DBCP Hards Air the close
Quality of Service	Fight and the set of the set o
Brane Lenity	
Bob ObsetBoather	trap last des an
rue de la	and in the state of the state o
100	Page 422.2 P 422-2 D and the manual sector and the
Print Surger	Recently Profile Classification Robert
Interface Lenue	Later the following conditions althor for 2" lend, 827 L, or for 311 852 Lg, 817 L
(Phot	m(F A
Cariffonia	Thylaco (all that
Riveline .	hand a second
Begroutes	(Warkenmar) are text (2018 First (2017) (Sector
Hangement	If Address a
	Territy Editori Hade
	upped a final and the set of perspector
	Industry Fullman
	Nutrition Tuber Heads
	and the factorial of the section of
	Trans N.C. Million
	the of the state
	Reduction MAT And was
	Institution PAIC Name.
	81.0
	Milig Proving
	(_Ine.ine)

Click **Save/Apply** to save and activate a rule.

Field	Description
Traffic Class Name	Enter a name for the traffic class.

Field	Description
Rule Order	Last or null are the only options.
Rule Status	Disable or enable the rule.
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece <u>P</u> &Queue <u>Q</u> " where <u>P</u> and <u>Q</u> are the Precedence and Queue Key values for the corresponding Interface as listed on the Queue Config screen.
Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Mark 802.1p if 802.1q is enabled	Select between 0-7. The lower the digit shows the higher the priority.
SET-1	
Physical LAN Port:	Select eth0-eth4 or Wlan from the dropdown menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Differentiated Services Code Point (DSCP) Check	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
IP Address	Select IP Address, Vendor Class ID (DHCP Option 60), or User Class ID (DHCP Option 77)
Source Subnet Mask	Enter the subnet mask for the source IP address.
UDP/TCP Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
UDP/TCP Destination Port (port or port:port)	Enter destination port number or port range.
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

6.7 Routing

This option controls Default Gateway, Static Route, Policy Routing and RIP.

NOTE: In bridge mode, the **RIP** screen is hidden while the other configuration screens are shown but ineffective.

6.7.1 Default Gateway

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

ADSL	Router
	Resting – Defusit Galenaug
Dovice Info Advanced Setup	In trades whether a surgery strategies converse converses is smaller, the reader and work the field readers draw approach readers are the Prior (Physics, Physics) Physics (Physics) in the checkbox is not adapted, only the data's draw at AD(OR a WMI straffers. Cds Samy/Apply Instantia serves.
LAN	NOTE: If therefore, the Automatic Assigned Default Takeney from undefault to selected, You must related the mater to get the automatic assigned initiality prevents.
Security Parential Control Quality of Service Routing	III Exaile Automotic conpect (which consent)
Default Gelanway Static Route RDF	Som/Appro-

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

6.7.2 Static Route

This option allows for the configuration of static routes by destination IP. Click **Add** to create a static route or click **Remove** to delete a static route.

	Router	~					
- Contraction	Routing	Static Route (A r	naidmum 32 entries o	an be configu	red)		
Dentice Info			Destination	Subnet Mask	Gateway	Interface	Remove
Advanced Setup				Add	Remove		
LAN							
NAT Security							
Parental Control							
Quality of Service							
Routing							
Default Gateway							
DIP							

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

ADSL	Router
Device Info Advanced Setup WAN LAN MAT Security Parential Control Quality of Service Rooting Dofast Galenway Staffs Rante RF	Bitsting - Static Rooks Add State the destination network address, saleset mask, gateway ANEXCH weaksite Wate interface them disk."Save/dop/s" to add the entry to the setty the test mask. Destination Retwork Address: Setter than it Interface Them (IP Address) Interface Them (IP Address) Interface Them (IP Address) Interfaces Interfaces Setter than Interfaces Interfaces Setter than in

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

6.7.3 RIP

To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox \square for at least one WAN interface before clicking **Save/Apply**.

ADSL R	outer
Device Info Advanced Setup W/H	Reading — RIP Configuration To subvise RIP for the desire, select the Teached radio better for Global RIP Resit. To configure an indefidual bits free, select the desired R involve and approxime, followed by placing a check in the Teached checklose for the bineface. Clok the Serve/Appl/ Indian is save the configuration, and its start or step RIP based on the Global RIP roots elected.
LAN NAT Security Parental Control	Beforfine 3FT/MEI Werster Technol b-0 (LWU 2 m Action C
Quality of Service Bouring Default Gateway Static Route BDF	Section:

6.8 DNS

6.8.1 DNS Server

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



6.8.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the CT-5364A to be more easily accessed from various locations on the Internet.

	Router
Device Infe Advanced Setup WAN LAN NAT Security Porestal Control Quality of Service Booting DMS Server DMS Server DMS Server	Bypeansis DNS The Operands DNS service allows you for allow a dynamics DF actions to a static business in one of the many domains, allowing your COL reader to be many administic businesses to configure Dynamic DE Service December 20 configure Dynamic DE Service December December 20 configure Dynamic DE Service December December December 20 configure Dynamic DE Service December December December 20 configure Dynamic December De

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

	Router	
<i>111</i>	Add dynamic DDNS This page allows you to	add a Dynamic DNS address from DynDNS run or TZO.
Device Info Advanced Setup WAN LAN NAT Security Parental Control Quality of Service Routing DNS DNS Server Dynamic DNS	D-DNS provider Hostname Interface DynDNS Settings Username Password	DynDNS.org *

Consult the table below for field descriptions.

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

6.9 DSL

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



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

6.10 Print Server

The CT-5364A provides printer support through a high-speed US 2.0 host port. Please refer to Appendix E for detailed installation instructions.

	Router	
Device Info Advanced Setup WAN LAN NAT Security Parental Control Quality of Service Routing DNS DSL DSL	Print Server settings This page allows you to enable / disable printer support. Enable on-board print server. Save/App	ły ·

6.11 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.

The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

	Router				
	Jaterlaiz Gro			on tri entries can be co	Agaest
Device Julio Querk Schap Advanced Schap WAN	EditeFace Group yes start could and all the org C bubbs onto	inggents a changing p proposition and proteins		e parts to FVC and bridge with appropriate LAN and Clo the Defeel group. Or (TO -4).	r groups. Dack group will perform an anti-Schpanisher solvanik. To support this feature, WAM interfaces using the Achi Latter. The Remons Earties will remove the grouping the dataset group has 30 orbitizes.
Quality al Service	Group Name	Bernet	T-RI	Balorfases.	
Heating (14)				030	
Print Server				4010	
Juberface Group				0610-4L	
IPSec.	Liefa.R			Winims(SSDE)	
Wardens				Wreters, Garet[31200]	
Diagnostics Management				Attrainer, FarmH1552011]	
				Alteriana, Gamil2(53)(14)	

To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown here.



格式化: 醒目提示

	Router					
	Interface Group Configuration					
Device Jato	To insite a new startan group 1. Enter the temp name and select startage make the required reaging of the picts. The	from the available interface but and add it to the propert interface that using the arrese betters to group name must be using a.				
Advanced Setup WAR (All Guilde of Sectors	3. If you like to automatically add LAN cleans to a PAC in the new group add the DEGP vector ID string, by configuring a DEGP vector ID string and the DEGP vector ID string and					
Routing	have that the selected interfaces will be	respond how they existing groups and added to the new group.				
DSL Frist Server Interface Group IPSec	IMPORTANT If a sender ID is configured allow it is ubball, or appropriate IP add Group Barnes	For a specific client device, please REBOUT the client device attached to the modern to ress.				
Weeless	Group Marten					
Disposition Hanopresent	Grauged Interfaces	Available Interfaces				
		effil DisT(1-4) USB Windows,S2xD1) Workes,Caust(255D2) Windows,Caust(255D2) Windows,Caust(255D2)				
	Autonutsally Add Clients With the Following DBCP Vonder 30s					
		Section				

DHCP Vendor IDs

Add support to automatically map LAN interfaces using DHCP vendor ID (option 60). The local DHCP server will forward these types of requests to a remote DHCP server.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38), VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box use, and the LAN interfaces are ENET1, ENET2, ENET3, and ENET4. The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.

2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

The local DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

Default: ENET2, ENET3, and ENET4.
 Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

6.12 IP Sec

You can add, edit or remove IPSec tunnel mode connections from this page.

ADSL R	outer
	IPSec Tunnel Hude Cannectione
Denter Info	Add, still \pm reveals PSsc haved reads convertions here this page.
Advances Into Advances Data UAN IAN NAT Security Paranetal Control Quality of Service Routing DBS DBL Print Server Interface Group IPSec Certificate	Enable Connection Nome Remote Galeway Local Addresses Remote Addresses Add New Connection

Click Add New Connection to add a new IPSec termination rule.

The following screen will display.

	IPSec Settings	
	IPSec Connection Name	new cannection
Device Info	Ramote IPSec Gateway Address	0.0.0.0
Advanced Setup	Turesel access from local IP addresses	Subnet (#)
WAN	IP Address for VPN	0.0.0.0
NAT	IP Satinetmask	253,255,255,0
Security Parental Control	Tunnel access from remote IP addresses	Subnet v
Quality of Service	IP Address for VPN	0.0.0.0
Routing DNS	IP Subnotmask	255,255,255,0
DSL	Key Exchange Method	Auto(IKE)
Print Server	Authentication Method	Pre-Shared Key =
IPSec	Pre-Shared Key	key
Certificate Wireless	Perfect Forward Secrecy	Disable w
Diagnostics	Advanced IRE Settings	Show Advanced Setting
Management		Save J Apply

IPSec Connection Name	User-defined label
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.

Tunnel access from local IP	Specify the acceptable host IP on the local
addresses	side. Choose Single or Subnet.
IP Address/Subnet Mask for VPN	If you chose Single, please enter the host IP
	address for VPN. If you chose Subnet, please
	enter the subnet information for VPN.
Tunnel access from remote IP	Specify the acceptable host IP on the remote
addresses	side. Choose Single or Subnet.
IP Address/Subnet Mask for VPN	If you chose Single, please enter the host IP
	address for VPN. If you chose Subnet, please
	enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select Show Advanced Settings to reveal the advanced settings options shown below.
Advanced IKE Settings	Hide Advanced Settings
Phase 1	627
Mode	Main
Encryption Algorithm	3DES .
Integrity Algorithm	MD5 💌
Select Diffie-Hellman Group for Key Exchan	nge 1024bt •
Key Life Time	3400 Seconds
Phase 2	
Encryption Algorithm	3DES 🖃
Integrity Algorithm	MD5 -
Select Diffie-Helman Group for Key Exchan	1024bt 💌
Key Life Time	3600 Seconds
Advanced IKE Settings	Select Hide Advanced Settings to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

The Manual key exchange method options are summarized in the table below.

Manual ·			
MD5 💌		DES: 16 digit Hex, 3DES: 48 digit Hex	
101 H	ies 100-FFFFFFFF	Post az ugi norjanku in ugi nor	
nm	DES / 3D	DES / AES (aes-cbc)	
Encryption Key		DES: 16 digit Hex, 3DES: 48 digit Hex	
Authentication Algorithm		MD5 / SHA1	
Authentication Key		digit Hex, SHA1: 40 digit Hex	
SPI (default is 101)			
	Manual 3 3DES 501 501 hm lorithm	Mercai Image: State of the sta	

6.13 Certificate

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

CONTEIND CADSL	Router		
	Local Certificates		
Device Info	Add, View or Remove certif Maximum 4 certificates can	lates from this page. Local cartificates are used by be stored.	poirs to virify your identity.
Advanced Setup			
WAN		Manual In Thus Subland	Toron Ballins
LAN		name in use subject	Type Action
NAT		Create Certificate Request	Instart Cettificate
Security		COMPACT INTO A COMPACT	and our constraint
Parental Control			
Quality of service			
DNS			
DSL			
Print Server			
Interface Groop			
IPSec			
Certificate			
Local			
Trusted CA			

6.13.1 Local

CREATE CERTIFICATE REQUEST

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

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

	Router			
Device Jato Absorced fortup WAN LAN MAI Security Parental Castrol Quality of Service Banthug Dets Banthug Dets Test Print Server Interface Group IPSe Cartificate Local Treated CA	O earls was cartificated a To generate a sertificate of Ende for the cartificate Certificate tarion Desenant Rame: Organization tarion States Providen tarion States Providen tarion	request print request yes read to be had used to be had and used to be	in Connects Hamm, Gr	anisation biarys, State Proston Name, and Pro J Mitter County

The following table is provided for your reference.

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

IMPORT CERTIFICATE

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

	outer	
	Import certificate	
	Enter contribute name, p	anda cartificato contant and privata kay.
Device Info Advanced Setup WAN	Cettifuals Name:	
NAT Secarity Parental Control	Catilizatio	
Quality of Service Renting DNS DSL		
Print Server Interface Group IPSec	Private Revi:	
Certificate Local Trasted CA		[.handy]

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

6.13.2 Trusted CA

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



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

laget CA certiliate		
iste ostilass sans o Getilasis lana	illusta carifician contest. intera carificiana sineri carificiana homo 90 1211/12.20	
Gettinis		
	Cettain	Cettain:

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

Chapter 7 Wireless

The Wireless menu provides access to the wireless options discussed below.

7.1 Basic

The asic option allows you to configure basic features of the wireless LAN interface. Among other things, 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.

	Wenfow - Basic								
Device Jala	This page of activities for Click "Apply	town you to configure home in active scient, and the orbit 7 to configure the family whe	Instants of file y ass referent more rest options.	e dess L e (pha le	AN Interface meets in 202	The con D) and r	endis at shalle the site of the latertage, and the decord set local or country requi	Note the presents.	
Minime Masic	E sature Wardesa								
	E YBW Access Port								
Security	E Cer	Chevia Justifian							
MAC Filter	E 244	the WMMI Advection							
Advanced	SSEC	Currine 6							
Station Into	80200 00:10:30:76:48:38								
Diegeneent Maragement	Country:	Country: UNITED STATES							
	Has Cliebs	10 Guest/Virtual Access Par	intec						
	Enabled 5	am	Hiddon	helate Cloubs	Disable WHH Alterative	Max Clients	nosin		
	10	Savid	0	12	12	16	Ng//A		
	13	Ganatt	0	0	0	35	14/4		

Click **Save/Apply** to apply the selected wireless options.

Option	Description
Enable Wireless	A checkbox \square that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open Network Connections from the start Menu and select View Available Network Connections . If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.

Option	Description
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Not supported.
SSID [1-32 characters]	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.
SSID	The SSID is a 48-bit identity used to identify a particular SS (asic Service Set) within an area. In Infrastructure SS networks, the SSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent SS or ad hoc networks, the SSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes \square in the Enabled column. To hide a Guest SSID select its checkbox \square in the Hidden column.
	Do the same for Isolate Clients and Disable WMM Advertise . For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF , Max Clients and BSSID , consult the matching entries in this table.
	NOTE: Remote wireless hosts cannot scan Guest SSIDs.
7.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.

Device Info Advarced Setup Windows Boot Security HAC Filter Weekes Brickpe Advarced Station Info Diagnostics Hasagement	Router Weeks - Security Masse elses - Security This page elses ends to influence OR Terraryin min instituted Security WSC Security Ender WSC Massed Security AP Nacion end the restands address OR SecurityPy Massed Security AP Massed Security	Usecutto features of the version Lättertarian. Table Disatiled Constant, selecting data encryptum, required to authoritaria to the version mitmorik and assorie the ancryption strangth. Constant, 2001
---	--	--

Click **Save/Apply** to implement new configuration settings.

WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see section 7.2.1) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID

Select the wireless network name from the drop-down box. 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 client will not be granted access.

Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

	Network Authentication:	802.1×			
	DUDUG Desize ID Address	0000			
	PADERS SHARE PROMINES.	1013			
	DADAGE PORC	10042			
	KALAUS Key:	Evabled F			
	Encountion Character	128.62			
	Current Network kiny:	2 -			
	Network Key 1:				
	Network Key 2:				
	Notwork Koy 21				
	Moharek Kay 21				
	national cross 4.	Enter 13 ASCIL:	haracters or 26 hexadecimal	diaits for 128-bit encry	ation laws
		Enter 5 ASCIE dh	eracters or 10 hexadecimal of	ligits for 64-bit encrypt	an keys
			Save/Apply		
The set	tings for WPA authe	entication a	are shown below.		
	Network Authen	tication:	WPA	*	
	WPA Group Rek	oy Interval:	٥		
	RADJUS Server	IP Address:	0.0.0.0		
	RADIUS Port:		1812		
	PADILIS Kov:				
	WEAR Consisting		TVID		
	West Encryption		Disabled a		
	WEP Encryption				
				Save/Apply	
-					
The set	tings for WPA-PSK a	authenticat	tion are snown ne	xt.	
	Select SSID:		Comtrend 💌		
	Network Authentia	ation:	WPA-PSK	•	
	1575 Dec Closed				
	WEAPIC-DI BIO			CITCLIFE & COSPAN	
	WHA Group Rekey	unterval: U			
	WPA Encryption:		TKJP		
	WEP Encryption:	1	Disabled 💌		
				Save/Apply	
					1
WEP Er	ncryption				
This opt	tion specifies wheth	er data se	nt over the netwo	ork is encrypte	d. The same
network	key is used for da	ta encrypti	on and network a	uthentication.	Four network
keys car	n be defined althoug	gh only one	e can be used at ar	ny one time. U	se the Current
Network	k Key list box to sel	ect the app	propriate network	key.	
Security	voptions include au	thenticatio	n and encryption	services base	d on the wired
equivale	ent privacy (WFP) a	laorithm	WFP is a set of s	ecurity service	es used to
protect	802 11 networks fr	om unauth	norized access su	ch as eavesdr	opping in this
case th	e capture of wirele	ss 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.

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

Encryption Strength This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

7.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The CT-5364A has both a WPS button on the side panel and a virtual button accessed from the web user interface (WUI).

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



NOTE: WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below. <u>You must</u> choose either the Push- utton or PIN configuration method for Steps 6 and 7.

I. Setup

Step 1: Select WPA-PSK, WPA2-PSK or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The figure here shows WPA2-PSK.

Network Authentication:	WPA2-PSK	
WPA Pre-Shared Key:	•••••	
WPA Group Rekey Interval:	0	
WPA Encryption:	AES .	
WEP Encryption:	Disabled ·	
WEP END YPOOR	Save/Apply	
	110	

Note: The WSC AP mode is Configured by default.

Step 2: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key (The WPA Pre-Shared Key is set by default).

Step 3: Click the **Save/Apply** button at the bottom of the screen.

IIIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	The wireless AP on the router searches for 2 minutes.	If the router stops
	searching before you complete Step 5, return to Step	4.

Step 4: First method: WPS button

Press the WPS button on the rear panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Second method: WUI virtual button

From the WUI, select the Push- utton radio button in the WSC Add Client section of the Wireless Security screen. Then click the Add button.

Add Client (This feature is available only when WPA-PSK,	WPA2 PSK or OPEN mode is configured)	
@ Push-Button C PIN	Add Enrolee	

Step 5: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.

01	123456789012	54%	00-19-15-32-F9-56	11	-	decision.
ID : 8x0064	Contrend 536	44	00-19-15-32-79-07	"	٩	Pin Code 00021838
		WPS Profile Lt				Canfig Hode Dreaker
						Convert Setel: Discorrect
EN	WPS Associate IE		Progress >> 35K			Correct Artela Dacomect Zatala
	WPS Associate IE	PBC - Sendry	Progress >> 35N EAPCK-Start			Decement Deconnect

Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IIIb. WPS – PIN CONFIGURATION

Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: The wireless AP on the router will search for WPS clients for 2 minutes. If the router stops searching before you complete Step 5, then return to Step 4 and try again.

Step 6: Select the PIN radio button in the WSC Add Client section of the Wireless Security the client PIN in the box provided and click Add.

Add Client (This feature is available only when WPA-I	PSK, WPA2 PSK or OPEN mode is configured)
C Push-Button 💿 PIN	Add Enrolee
	Help

Step 7: Go to your WPS certified client device and activate the PIN function. A screenshot of typical WPS client software is given below as an example.

		WP	S AP List			
ID :	Combred 53644		00-19-15-32-F9-16	11	0	Prison.
ID : 0x0004	Combrend 5364A		00-19-15-32-F9-07	11	9	Information
						Pin Code
						00021838
		WPS Profile List				-Config Hode -
						Enrolee
						Petat.
						Connect
						Ristele.
						Disconnect
EIN	WPS Associate IE		Progress >> 15%			Delete
-	WPC Prohe IF	Party Banda and	cisting to wild all	_	_	-

Proceed to Step 8 to check the connection.

III. CHECK CONNECTION

Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The figure below shows an example of a successful connection.

			AP LEA			
0:0:0004	Costs ed 50	54A	00-19-15-33/79-07	1.85	-	- Peccer.
						Menators
						Per Carle
						00011636
		WPS Profile Ltd.				Config Hode
Continued 5363	00-1	9-15-33-19-07				Donke *
						Detail
						Cenet
						- Autor
						Disconnect
174	WFI Accessive IE		Property Allers			Leieta
HOC .	The West Probe 12	WPS status to re	evented successfully - Contro	CaC2 (1991		

Double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the new connection.

It should appear as shown in the dialog-box below.

¹¹⁰ Wireless Network	Connection	5 Status	? ×
General Support			
Connection			
Status:			Connected
Network:		Com	krend 5364 A
Duration:			00.06.14
Speed:			54.0 Mbps
Signal Strength:			att
Activity	Sent —	<u>_</u>	Received
Packets:	121	I	71
Properties	<u>D</u> isable	⊻iew Wireless	Networks
			Dose

7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.

	Router
	Wireless MAC Filter
Device Info Advanced Setup	Select SSID: Comtrend
Wireless Basic Security	MAC Restrict Mode:
MAC Filter Wireless Bridge	MAC Address Remove
Station Info Diagnostics Management	Add Remove

Option	Description
Select SSID	Select the wireless network name from the drop-down box. 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.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears. Enter the MAC address in the box provided and click **Save/Apply**.

CONTREND O Wirele	ss Router
Device Info Advanced Sertup Wireless Basic Security HAC Filter Wireless Bridge Advanced Station Infe	Wiredow HAC filter Exter the MAC address and click "Apply" to add the MAC address to the socialism NAC address filters. MAC Address:

7.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WLAN interface. See the table beneath for detailed explanations of the various options.



Click Save/Apply to implement new configuration settings.

Feature	Description
AP Mode	Selecting Wireless Bridge (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
ridge Restrict	Selecting Disabled disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in the Remote ridges list will be granted access. Click Refresh to update the station list when ridge Restrict is enabled.

7.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate (**In the U.S only channel 11 can be selected**), 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 **Save/Apply** to set new advanced wireless options.

46			
CONTRACTOR O	0		
ADSL	Router		
	and the second se		
	Wreness - Advanced		
	This page allows you to config the transmission rate to a single	per all ordered formers of the storage states	stratege 1,2% interfaces. When the select is particular estament an unleft to operating from the
Desire has	made, set the beator interval	for the scorio point, set XPres	mode and set synthesis about or long preambles are used.
Oakk Settap	Click "Apply" to configure the	advanced wireless options.	
Advanced Setup	Beat	Tartest an	
Wireless.	Chinaid	11 4	Column +1
Sud:	Add (Dennel Timerinia)	···	
Security.	BUILLING CONTRACTOR	Ada ini	
MAC Fiber	Bandard Ba	and the part of the second	Window amin
Windless Bridge	Control Schemant	Linest a	Caract lines
Station Info	Din 11a Rain	Auto Ini	
Disguestics	INTO THE PRODUCTION OF	Adv at	
Hangement	Second 653 1 to Clart Only	0214	
1010100000000000	Tax" has	100 million	
	mathing links	Ada la	
	Ball Rev.	Detail	
	Praymandation Throughout	2185	
	ETT. Throubeld	2542	
	DTDN internal:		
	Reacting Laboration	194	
	Godal The Clerity	10	
	Thes - Ishedow	Crisibed in	
	Metwow Televisor	Canada 10	
	Prografile Type:	tong last	
	Transmit Porter	100%	
	WHEN A BURNER	Auto at	
	URM he Administration	Dealahed +	
	DHN APSD	Divided (a)	
	- 100 CT	ALCOURT TO	
			Sevel Apple

Field	Description
and	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel. Note: In the U.S only channel 11 can be selected.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)

Field	Description			
andwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.			
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.			
802.11n Rate	Set the physical transmission rate (PHY) from 6.5 to 130 Mbps.			
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.			
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.			
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.			
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)			
asic Rate	Setting for basic transmission 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) is also known as eacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs 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.			
eacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. y default, network devices passively scan all RF channels listening for beacons coming from access points. efore 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).			

Field	Description			
Global Max Clients	The maximum number of clients that can connect to the router			
Xpress [™] Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.			
Afterburner Technology	Afterburner technology is an enhancement for the 54g [™] platform and can achieve optimal speeds when all network devices include the new technology.			
Transmit Power	Set the power output (by percentage) as desired.			
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.			
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.			
WMM APSD	This is Automatic Power Save Delivery. It saves power.			

7.6 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.



Consult the table below for descriptions of each column heading.

Heading	Description
MAC	Lists the MAC address of all the stations.
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.

Heading	Description
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

Chapter 8 Diagnostics

8.1 Diagnostics

Diagnostics screens for ATM ridge and PPPoE connection types are shown below.

Bridge Connection

	Router			
Dester John Qaith Softer Advanced Softer Wireless Dispendics Management	Hageworks They modern to applied of facting year (2) Treats" at the bottom of this page to make providers. Test the connection to year local net fact year ENE [1] -4] Connections fact year Window Connections fact year Window Connections fact the connection to year [19], serv	A terminality term File for PASS PASS INT provide	en Theil I status Hally Hally	edivident frata are foliad bolow. If a test displayer is full status, elek. "Novae Disposition a consistent, If the leaf continues in ball, dirk "Neig? and bolow free inside booling
	Test ADM: Nynchronitathan	FAR	Here	kons lingusta lette

PPPoE Connection

ADSI	Router						
Device Tals Advanced Selap Weekss	pppers, R. R. 25, 1 Dispersentities Your resolves is capable of barling pour DG Tests' at the central of the paperts make a precedures. Tool the pursuantilism he your local aerbs Tool processing the Test pour District Test pour DBCT(1-4) Cannecticue	ere the fue mek PASSS	n, The is status n	fielded hely are lided below. If a test displays a full status, shit Nerve Disprovis consisted. If the last continues to full, shit Neigr' and fullow the tradiesfacebog			
Disposition	Test per Wirkes Convertise:	PASS Help					
Management	Test the concertion to your DSL work	Fest the connection to your DSL workler provider					
	Test ADSL Synchronication:	TAIL	tela				
	Test ATM DAM IS segment plag:	FAIL	tela				
	Sest ATH DAH iS end to end prog-	EAB	Heles				
	Tost the connection to your fatement veryice provider						
	Tost PPP server connection:	TAR	their .				
	Test adhestication with 252	EAR.	Heg-				
	Test the assigned IP address:	EAR	1115				
	Ping default splewing	E.M.D.	1441				
	Plag printing Diskalls State Server)	19855	Hirty				
			Test	Task Islan (Jan 14			

The Diagnostics menu provides feedback on the connection status of the CT-5364A. If a test displays a fail status, click the **Test** button to retest and confirm the error. If the test continues to fail, click <u>Help</u> and follow the troubleshooting procedures provided.

Chapter 9 Management

The Management menu has the following maintenance functions and processes:

- 99.1 Settings 9.2 System Log9.66 Access Con0 SNMP Agent9.7 Update Software 9.4
- 9.5 Internet Time 9.66 Access Control

9.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select desired values and click Save/Apply to configure SNMP options.

	Router		
Device Info Quick Sectop Advanced Setup Wiroless Diagnostiks Management Settings System Log System Log	19949 - Cooling e al Simple National Ma agent in This Herical Salect the classifier of Coo Salect Community : Salet Community : System Locations System Contact	ken ugernert Protocol (DM stam and chiti Septyr') uiter & Enable Exclusion Exclusion Exclusion Exclusion Exclusion Exclusion Exclusion Exclusion Exclusion Exclusion	P) altres a nunagement application to relations electrics and status from the 5940 is configure the 5944 options.
Update Softwore Seve/Reboot	meninger an	him	Gave Report

TR-069 Client



9.1 Settings

This includes ackup Settings, Update Settings, and Restore Default screens.

9.1.1 Backup Settings

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

	s Router
	Settings - Backup Backup the router configurations. You may save your router configurations to a file on your PC.
Device Info Advanced Setup Wireless Diagnostics Hanagement Settings Backup Update Restore Default	Beckip Settinge

9.1.2 Update Settings

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

COMTREND O	s Router
Device Info Advanced Setup Wireless Diagnostics Hanagement Settings Backup Update Restore Default	Tools — Update Settings Update the nuter settings. You may update your muter settings using your seved files. Settings File filame:

9.1.3 Restore Default

Click Restore Default Settings to restore factory default settings.



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

DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If recessary, reconfigure your PC's IP address to match your new configuration.

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

NOTE: This entry has the same effect as the **Reset** button. The CT-5364A board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

9.2 System Log

This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click Configure System Log, as shown below (circled in Red).



	Router			
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management Settings System Log SNMP Agent TR-069 Client Internet Time	System Log The System Log dalog allow Click "View System Log" to v Click "Configure System Log	s you to view the System Log an lew the System Log. * to configure the System Log op Wew System	d configuen tions. Log	e the System Log options. Cooligure System Log
Access Control Update Software Save/Reboot				

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

	Router
Desico Jako Quick Setup Advanced Setup Windens Diogenetics Management Settings System Log SMIP Agent 18-009 Class Internet Time Access Control Update Software Servi Rebool	Systems Log - Configuration If the lag mode is enabled, the partners will begin to log all the strength events. For the up takes, all events alone or equal to the strength lower will be instance of the table of the strength or the strengt or the strength or the strength or the strengt

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

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. y default, it is disabled. To enable it, select the Enable radio button and then click Apply/Save .

Option	Description
Log Level	 Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-5364A 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. y default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: Emergency = system is unusable Alert = action must be taken immediately Critical = critical conditions Error = Error conditions Warning = normal but significant condition Informational= provides information for reference Debugging = debug-level messages
	Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or oth mode is configured, the WE UI will prompt the user to enter the Server IP address and Server UDP port.

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

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

9.3 SNMP Agent

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

COMPETIND OC			
ADSL R	louter		
-	1994 - Configurat	line	
Device Info	Simple Network Mar agent in this device.	ingernert Protocol (2N	(P) altres a numagement application to relations elabolities and status from the SPA
Oxick Setup Advanced Setup	Select the desired of	alam and chill "Apply"	to carfigate the SARE options.
Wireless Diagnostics	SWP April Cos	usta # Enable	
Management	Read Constantly :	pith:	
Settings	Set Community :	private	
System Log	Gystern Harse	European .	
18-009 Client	Bysteri Locations	introve	
Internet Time	System Contact:	Printern.	
Access Control Update Software	Thip Manager 31	n+na	
Save/Hebcot			Save Hegers

9.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.

ADSL	Router		
Device Info Quark Setup Advanced Setup Wireless Disposetics Nanogeneent Settings System Lag System System Lag System Lag	 TH-009 cleart - Configuration WWO Hamapement Protocol (TH-009) also diagonatics to this anxies. Infect the desired values and talk "Apply" Inferm Inferm Inferm Interval ACS-URL: ACS-	es a Auto-Coellig-auto to cardigate the Tix-O III Isaatile O Itradite admin H (Isaatile O Itradite H (Isaatile O Itradite admin H (Isaatile O Itradite	n Server (ACS) to perform auto-confligeration, orientation, collection, o Bit sherit optimer.

The table below is provided for ease of reference.

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

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

9.5 Internet Time

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

ADSL	Router			
	Time settings			
Service 1	This page allows you to the	le modem's time corifi	guration.	
evice Info wick Setup	Automatically synchro	unize with Internet time	e servers	
Incic Secure Idvanced Secure	-			
Vireless	First NTP time server:	clock.tmt.tre.net	*	
lagnostics	Second NTP time server:	None	- C + C	
anagement	the second s		A Children of the	
Settings	Time zone offset:	(GMT-12:00) Internal	tional Date Line West	1
System Log				
SNMP Agent			Save/Apelly	
TR-069 Client				
Internet Time				
Access Control				
Sum/Dahaak				

NOTE: Internet Time must be activated to use Parental Control (page 62). In addition, this menu item is not displayed when in ridge mode since the router would not be able to connect to the NTP timeserver. 格式化: 醒目提示

9.6 Access Control

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

9.6.1 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/App1y.



9.6.2 IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the router. efore you enable it, configure the IP addresses by clicking the Add button. Enter the IP address and click App1y to allow the PC with this IP address managing the DSL Router.

CONTRACTOR OF A CONTRACTOR OF				
ADSL R	outer			
All Property lies:				
Barriel and	Access Cardrol 1P Address			
	The TA Address Access Control on	the Rest and American Street	a he had a her an an and a second second	sectors have 10 addresses contained to fire Assess Control
Incident Parks	List, 27 the Access Cardeol Pixels in	chariter, the solute sill re-	statisticale 12 autoresants	territors your or additioned comprises or the econe control for incentive markets. The sanding and the econes and instr-
which Endown	Inded to the Service Control List			
deserved Sectors				
dentere serap		Anne Colt	of Parity B. (Bassia)	O Exake
income the				
and an and a second				
Editors		37 Address (isteet Hole: Jointy	aca- Hummove
Section for				
Sporter Log			Atta Seema-	
The fail (last			Energy Support and	
Interest Lines			/	
Automatic Control				
Access Control				
Services				
IP Addresses				
Passwords.				
Update Software			/	
Sive/Rebool			/	
	Router	•		
ADSL	Router Access Control	+		
ADSL	Router Access Control Eray The IP address of th	e management station p	erriðad ta access fi	e kool nonaprovet services, and dick SoveyAppl
COMPETED ADSL water Info	Router Access Control Enter the IP address of the IP Address	e rtungernert station p Siebnet Mook	erriðid la accesa D Dirterface	e kool management services, and click ServeyApply
ovice lafe wice lafe wice stage	Router Access Control Erate The IP address of the IP Address	e rtanagement stafan p Seboert Mosk	emitted to access th Deterface	e kool management services, and click SeverAppl
COMPETING) C ADSL MOSE lafe ank Sebus dwaced Sebus trates	Router Access Control Eray: The IP address of th IP Address	e rungenert datan p Sebret Mook	entided to access th Deterface Teste +	e koi narapreet sevice, and dick SeverAppi
COMTELLO ADSL evice lafu exice lafu	Router Access Control Eray for IP address of th IP Address	e stanagenest elation p Sebret Mork	emidted ta access th Deterface reste 💌	e koal management tervices, and dick Save/Aggi
evice Info acts Setup diversed Setup tratesa agrospics	Router Access Control Erain the IP address of the IP Address	e stanagement station p Sieboet Mook	emitted ta access th Deterface retre (ac)	e kool management services, and dick SeverAugi
execution of the second	Router Access Control Erain The IP address of th IP Address	e rungerent datas p Selmet Mosk	erniðed ta ercess ti Deterface reine 💌	e kosi manaperawit services, and disk SaveyAggi me/Apple
vice lafe and Setup hased Setup trates anagenent Settings	Router Access Control Eray: The IP address of Th IP Address	e rungevert datan p Sebret Mask	erreiðied ta access ti Detterface resta 💌	e koal management sevices, and dick SeverAgat een/Aagis
vice lafa ark Setup huaced Setup indesa appenent Settings System Log	Router Access Control Erzy: The IP address of th IP Address	e rtungement station p Siehnet Mook	erniðed ta access 0 Deterface Teste (ac	e koal management services, and disk SieverAgai envillagig
evice Info ack Setup dvaced Setup dvaced Setup dvaced Setup trates anagement Settings System Log System Log System Log	Router Access Control Erate The IP address of th IP Address	e stanagement station p Seboort Mosk	emitted la access th Deterface Tests ac	e kool management services, and disk SaverAgat nov/Again
evice lafe evice lafe evice lafe evice lafe evice lafe water Schap trailess anagement Settings System Log Stem P Agent 18-609 Client	Router Access Control Eray The IP address of th IP Address	e rungevert dation p Selmet Mask	ertiëled ta access th Deterface rate *	e koal management services, and disk SaverAggi
COMTETED ADSL ADSL avice lafu ank Setup dvaccd Setup trates iagnostics anogenent Settings System Log SNIP Agent TR-609 Chart bistoard Tops	Router Access Control Erzy: the IP address of th IP Address	e dungened dation p Selmet Mook	erniðad ta accesa ti Distorface Textes	e kool management services, and dick SeverAqui
evice Info and Setup diveced Setup tradese laposetics anagement Settings System Log Settings System Log Setup Charit TR-609 Charit Informed Tange	Router Access Control Erzir fler IP address of IP IP Address	e rtænagersært støtion p Sielmert Mook	emitted ta access th Deterface rense	e kool management services, and dick SeverAugi
evice lab unk satur dvarced Sebap trates lagoostics anagement Settings System Log State Agent TR-600 Claret latemet Tane Access Control	Router Access Control Erain The IP address of th IP Address	e stanagement station p Seboort Mosk	emitted to access th Deterface	e koal management services, and dick SeverAppl
evice lafe ack Setup divaced Setup tratese lagoostics anagement Settings System Log Stell Agent TR-600 Client laternet Trate Access Control Services	Router Access Control Erain the IP address of th IP Address	e rungevert ebten p Sehnet Mosk	emided is access it Deterface	e koal management tervices, and dick Save/Aggi
evice lafe ank Selay duaced Selay trates iagnostics anogeneoit Settings System Log State Log Sta	Router Access Control Erzir file IP address of th IP Address	e rtunagement station p Siehmet Mook	erniðed ta access ti Deterface Teste (m)	e kool management services, and dick SeverAugi envikazie
COMTELEO ADSL ADSL ADSL ADSL ADSL ADSL ADSL ADSL	Router Access Control Erain The IP address of th IP Address	e stanagersert station p Seboet Mook	emitted ta access th Deterface Tests	e kol neegenet sevice, and did. SevelAppl
evice Info unk Setup doesed Setup trates langement Settings System Log Stellings System Log Stellings Stellings System Log Stellings System Log Stellings System Log Stellings Stellings System Log Stellings Stellings System Log Stellings System Log Stellings Stelling	Router Access Control Erain the IP address of the IP Address	e rungevert status p	emiðled ta access ti Detterface rene 💌	e koal management tervices, and dick Save/Aggi

9.6.3 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5364A is controlled through the following three user accounts:

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

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

	touter	
Device John Quick Softap Advanced Serlap Workess Disposition Management Settings Spoten Log Stitlip Agent Till 460 Cherri Internet Time Access Control Services JP Adference Parameth Update Software Save (Refeared	Anness Condrol — Possage Anness to your 120, ranks to 1 The user name "suggest" in o The user name "suggest" in o User file failed before to enter User file failed before to enter	de ministed Prough three user accounts: root, segment, mel user. satisfied accounts to decays and view configuration of sour DEL Rooter. ad to allow an DP techniciae to access your DEL Rooter. an the DEL Router, view configuration settings and statisfies, we will se, splate the restor's sufference. ar to DD classifiers and disk. "Apply" he change or oracle presents in. Note: Research second contain a spece

NOTE: Passwords can be up to 16 characters in length.

9.7 Update Software

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

	Router
1000	Tools - Update Software
	Step 1: Obtain an updated software lenge file from your 257.
Device Infe	Other to Color-the parts to the barrier His barreline in the two fighter of shirt the Weinstein In these to both the matter His
Quick Setup	20th Xt build are build to an surface as an procession, or only are. Butters, for the process are surface or
Advanced Setup Wireless	Step 3: Clok the "Update Software" bottom mare to upload the new Image Re.
Diagnostics	NOTE: The update process takes alread 2 minutes to complete, and your 25L Nouter will releval.
Management	
Settings	Software Hie Name: BRWS0
System Log	
SNNP Agent	Update Software
TR-069 Client	
Internet Time	
Access Control	
Update Software	
Save/Reboot	

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

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

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

NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the **Quick** Setup

After login, the **Quick Setup** screen will appear as shown.

	Router
Device Info Quick Setup Advanced Setup Wireless 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. IP DSL Auto-connect
	Pácwit

NOTE: The selections available on the main menu are based upon the configured connection type and user account privileges.

The Quick Setup screen allows the user to configure the CT-5364A for ADSL connectivity and Internet access. It also guides the user though the WAN network setup first and then the LAN interface setup. You can either do this manually or follow the auto quick setup (i.e. DSL Auto-connect) instructions.

This router supports the following data encapsulation methods.

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

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration in the Central Office and roadband 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 router is to run the PPPoE client. The router can support both cases simultaneously.
- If none of the LAN-side devices run PPPoE clients, then select PPPoE.
- NAT and firewall can be enabled or disabled by the user in router modes (PPPoE, PPPoA, MER or IPoA) and they are always disabled with ridge mode.
- Depending on the network operating mode, and whether NAT and firewall are enabled or disabled, the main menu will display or hide NAT and Firewall.

NOTE: Up to sixteen 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.

9.8 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL router will automatically detect the PVC, so just follow the easy online instructions.

STEP 1: Select Quick Setup to display this screen.



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

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

9.9 Manual Quick Setup

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

	Router
and the second second	Quick Setup
	This Quick Setup will guide you through the steps necessary to configure your DSL Router.
Quick Setup	ATM PVC Configuration
Advanced Setup Wireless Diagnostics Management	Select the check box below to enable DSL Auto-connect process.

The Virtual Path I change VPI and V	dentifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not CI numbers unless your ISP instructs you otherwise.
VPI: [0-255]	0
VCI: [32-65535]	35
Enable Quality	Df Service
Enabling QoS for system resources, assign priorities for	a PVC improves performance for selected classes of applications. However, since QoS also consumes the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to or the applications.
Enable Quality Of	Service
	Next

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

STEP 3: Choose an Encapsulation mode.

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP RIDGING, VC/MUX
- MER- LLC/SNAP- RIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC MUX
- ridging- LLC/SNAP- RIDGING, VC/MUX



NOTE: Subsections 4.2.1 - 4.2.4 describe the PVC setup procedure further. Choosing different connection types pops up different settings requests. Enter settings as directed by your Internet Service Provider (ISP).

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

STEP 4: Select the PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) radio button and click **Next**. The following screen appears.

	PPP Diemane and Pestweed
Device Info	passed that your the has provided to you.
Quick Settap	PPP Literraria:
Advanced Setup	1017 Tamorett
Discounting	PPINE Service Nome:
Masagement	Authentization Hethod: [AUTO]
	Dial on demand (with the invest time)
	[2] PPF IP acturates.
	E Statis MAT
	El Enate Autome tol
	D Gatte Reval
	ET UNITADO PANINESE
	III Antry FEE parented on adherication error
	G State PPV Debag Mode
	📋 Ristige PPPsE France Retrieve WWI and Land Parts (Debat District)
	E readints
	HT12 1452

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 WE user interface allows a maximum of 256 characters for the PPP user name and a maximum of 32 characters for the PPP password.

PPPoE Service Name: For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or RAS) of ISP check this service label to make a connection.

Dial on Demand

The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.

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

PPP IP Extension

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

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

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

Use Static IP Address

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

Retry PPP password on authentication error

Tick the box to select.

Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. This is used for debugging purposes.

Bridge PPPoE Frames Between WAN and Local Ports

If Enabled, the function can create a local PPPoE connection to the WAN side.

Fixed MTU

Select the checkbox to enable Fixed MTU and adjust the MTU value for WAN Interface, PPPoE and PPPoA. Default values are 1492 for PPPoE and 1500 for PPPoA.

STEP 5: Click Next to display the following screen.

	Router		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Enable IGMP Multicas Enable IGMP Multicast Enable WAN Service Service Name	et, and WAN Service	Back Next

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

STEP 6: After entering your settings, select **Next**. The following screen appears.

- Andrew	Device Setup		
10.00 M 10.00 M	Configure the DS	Router IP Address and Subnet Mask for LA	N interface.
Device Info	TO Address	1003 100 1 5	
Juck Setup	ar Address.	172.198.1.1	
Advanceu Setup	SUDNET Masic	255,255,255,0	
Diagnostics	O Disable DHC	P Server	
Management	Enable DHCI	Server	
40967-849.232	Start IP Addr	ess: 192.168.1.2	
	End IP Addre	58: 192.168.1.254	
	Subnet: Mask	255.255.255.0	
	Leased Time	(hour): 24	
	Configure the	second IP Address and Subnet Mask for LAM	l interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the second I	P Address and Subnet Ma	isk for LAN interface
IP Address:		
Subnet Mask:		

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

GOMTREND O	Router
- Series	Wireless Setup
Device Info Quick Setup Advanced Setup Wiseless	Enable Wireless 🖻 Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back Next

Click Next to display the final setup screen.

and a second	WAN Setup - Summ	вагу	
	Hake sure that the set	tangs below match the se	tangs provided by your ISP.
Quick Setup	VPE / VCE:	0/35	
Advanced Setup	Connection Type:	PPPOE	
Wireless Diagnostics Harragement	Service Name:	pppoe_0_0_35_1	
	Service Category:	U04.	
	IP Address:	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Enabled	
	Firewalt	Disabled	
	EGMP Multicaste	Chilabled	
	Quality Of Service:	Disabled	

 Step 9: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.



Step 4: Select the MAC Encapsulation Routing (MER) radio button and click Next.

Dealer Tala	Exter information provided to you by your USP to configure the WMA 3F antings.
Quick Setup	Retrait: DECE tay be enabled for PVC or HER model or 3F over Chartest as WMA mechanis # "Othern as 3F althress automatically" is
Advanced Setup	choose. Charging the default patiency or the DEC affects the reliate system. Configuring there will static values will double the
Workers	automatic anopyment from DECF or other WMA considers.
Diagnostics	The state and chart patiency or the The PVC or HER mode, you must enter the 3F address af the intende galaxies in the "Use
Management	FF address", The "the label statefault patiency is uptareal.
	C Obtait of P address addressing P address Wei P Address Novi P A

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

NOTE: 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" field. Your ISP should provide the values to be entered in these fields.

Step 5: Click Next to display the following screen.

	Router
	Hotsourk Address Translation Settings
Deske tala Caka Setua	Sastaces Address Translater (SAT) alone you to share one Wile Ana Nebork (WAR) 37 address for maliple computers of your Local An Nebolin (SAN)
Advanced Settings	from that E
WWW	Knadaw Fallbane teht
LAN Quality of Service Reading	Environ Provide 🖂
DSL Slave DSL	Enable IGNEP Multitant, and WMA Service
Print Server	Engle X249 Particult.
Post Mapping 195ec	toute must beven E
Certificate: Wireless	Sterous Harms: jran at 0.21
Hangement	anack [treat]
Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

- State	Device Setup Configure the DGL Brister IB Address and School Mark for LAN interface
Device Info	Compare the Loss House' to Address and Statilet Mask for LAW Interface.
Quick Setup Advanced Setup	IP Address: 192.168.1.1 Subnet Mesk: 255.255.255.0
Diagnostics	C Disable DHCP Server
Management	Enable DHCP Server Start IP Address: 192.168.1.3
	End IP Address: 192.168.1.254
	Subnet Mask: 255.255.255.0
	Leased Time (hour): 24
	C Enable DHCP Server Relay
	DHCP Server IP Address:
	Configure the second IP Address and Subnet Mask for LAN Interface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the seco	ond IP Address and Subnet Mask for LAN Interface
IP Address:	
Subnet Mask:	

Step 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
/	Wireless Setup
Device Info	Enable Wireless 🗹
Quick Setup	Enter the wireless network name (also known as SSID).
Advanced Setup Wireless	SSID: Comtrend
Diagnostics	Back Next

Click **Next** to display the final setup screen.

ADSL R	outer		
	WAN Setup - Summ	ury	
	Make sure that the set	itings below match the set	tings provided by your BP.
	VPL / VCE	0735	
	Connection Type:	MER	
	Service Name:	mer_0_0_35	
	Service Category:	1194	
	IP Address:	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Enabled	
	Firewalt	Deabled	
	IGMP Hulticast:	Diabled	
	Quality Of Service:	Disabilid	
	Cick "Save/Reboot" to	o save these settings and	reboot router. Cick "Back" to make any modificati

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

9.9.3 IP Over ATM

Step 4: Select the IP over ATM (IPoA) radio button and click **Next**.

Device Sala Qoks Setup Advanced Setup Mircless Diagnostics Management	WAR IP Sortings Enter information provided to you by your EP to configure the WAR IP antitings. Notice: DHO* in refl. supported in Prol. marks. Oursping the default polynomy or the DHE affects the whole system. Configuring them with states volume will state the whole system. Configuring them with states volume will state the set of search to support the transmitter component from other Walk connection. With IP Address: IF LEFE With Extend that you by your IP to configure the Walk connection. If LEFE With Extend that: IF LEFE With: IF Extend that: With: IF Extend that:
	Back North

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

	Router
Deske Isla (sakk Setap Advanod Setap Workes Dispositio	Network Address Transletion (NFT) allow you to does one Web Ana Servers (SUND) IP address for multiple componence your Local Ana Retrieves (SUND) Exoto NRT (E) Rindle Faktore NRT (E) Rindle Faktore NRT (E)
Heigenet	Enable TUNP Hulticor, and WWN Nervice. Enable 12/4 Multicor Enable WWN Service Anytic WWN Service Anytic Units
	(Back) [Next]

Enable NAT

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu will display after the next reboot. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected so as to free up system resources.

Enable Fullcone NAT: This option becomes available when NAT is enabled

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

Enable Firewall

If the firewall checkbox is selected, the Security submenu will display after the next reboot. The user can then configure firewall features. If the firewall is not used, this checkbox should not be selected so as to free up system resources.

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

Enable WAN Service:

Tick this item to enable the ATM service. Untick it to stop the ATM service.

Service Name: This is a user defined label.

Step 6: Click Next to display the following screen.

- And	Device Setup		
	Configure the DS	L Router IP Address and Subnet Mask for LAN i	nterface.
Device Info Duick Setup	IP Address:	192.168.1.1	
Advanced Setup	Subnet Mask:	255.255.255.0	
Diagnostics	O Disable DHCP Server		
Management	Enable DHCI	² Server	
	Start IP Addr	ess: 192.168.1.2	
	End IP Addre	ss: 192.168.1.254	
	Subnet Mask	255.255.255.0	
	Leased Time (hour): 24		
	Configure the	second JP Address and Subnet Mask for LAN in	iterface

The Device Setup screen allows the user to configure the LAN interface IP address, subnet mask, and DHCP server. To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time.

Since the router occupies the first two IP addresses (192.168.1.1 and 192.168.1.2), the default private address range provided by the ISP server in the router is 192.168.1.3 through 192.168.1.254.

If NAT is disabled, **Enable DHCP Server Relay** will be displayed as an option. To enable it, select the **Enable DHCP Server Relay** radio button and enter the DHCP Server IP Address. This allows the router to relay the DHCP packets from 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 checkbox shown.

Configure the sec	cond IP Address and Subnet Mask for LAN interface
IP Address:	
Subnet Mask:	

STEP 7: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
	Wireless Setup
Device Info	Enable Wireless 🖾
Quick Setup Advanced Setup Wireless	Enter the wireless network name (also known as SSID). SSID: Comtrend
Diagnostics Management	Back, Next

Click **Next** to display the final setup screen.

ADSL	Router WAN Setup - Summ	шту	
Device Info	Hana surd that the set	tings below match t	e settings provided by your zay,
Quick Setup	VPL/ VCI:	0.7.35	
Advanced Setup	Connection Type:	\$POR	
Wireless Diagnostics	Service Name:	(poe_0_0_35	
	Service Category:	UBR	
manargenen.	IP Address:	123.124.125.126	
	Service States	Enabled	
	NAT:	Enabled.	
	Firewall:	Osabled	
	IGHP Multicast;	Claubled	
	Quality Of Services	Cleabled	
	Clock "Saves'Reboot" 1 NOTE: The configuration	o save these setting on process takes ab	and reboot router. Clok "Back" to make any modifications out 1 minute to complete and your DSE. Router will reboot.

 Step 8: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

9.9.4 Bridging

Step 4: Select the ridging radio button and click Next. The following screen appears. Select Enable Bridge Service and click Next.

	Router		
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Unselect the check b Enable Bridge Service: Service Name:	ox below to disable t P br_0_0_35	his WAN service Bock Tiest



	Router		
Device Info Quick Setup Advanced Setup	Device Setup Configure the D IP Address: Subnot Mask :	3. Router IP Address and Sub 192.168-1.1 255.255.255.0	net Mask för your Local Area Network (LAN).
Wireless Diagnostics Management			Back Barrt

NOTE: In bridge mode, the router is not associated with a WAN IP address. This means that it can only be managed from a PC on the LAN. For remote management, you must select a routing type (PPPoE/A, MER, or IPoA).

STEP 6: Click **Next** to continue. To enable the wireless function, select the radio button (as shown) and input a new SSID (if desired).

	Router
Sent 1	Wireless Setup
Device Info	Enable Wireless 🗵
Quick Setup	Enter the wireless network name (also known as SSID).
Wireless	SSID: Comtrend
Diagnostics	
Management	Back

Click Next to display the final setup screen.

and the second	WAN Setup - Summ Make sure that the se	nary ttings below mat	the settings provided by your 15P
Quick Setup	VPL/ VCE	0/35	
Idvanced Setup	Connection Type:	thradigie	
Wireless	Service Name:	br_0_0_28	
Diagnostics Management	Service Category:	UBR	
	IP Address:	Not Applicable	
	Service State:	Childed.	
	NAT:	trabled	
	Firewalt:	Diabid	
	IGNP Hubicastz	Not Applicable	
	Quality Of Services	Deabled	

 Step 7: The WAN Setup-Summary screen presents the proposed configuration. Click Back to modify these settings. To apply these settings, click
 Save/Reboot. The router will save the configuration and reboot. After the router reboots, the Web UI will refresh to the Device Info screen.

Device Information screen with the firmware version installed, to confirm the installation was successful.

9.10 Reboot

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



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

Appendix A - Firewall

STATEFUL PACKET INSPECTION

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

DENIAL OF SERVICE ATTACK

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

TCP/IP/PORT/INTERFACE FILTER

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

OUTGOING IP FILTER

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

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

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

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

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

INCOMING IP FILTER

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

Example 1:	Filter Name	:	In_Filter1
	Protocol	:	ТСР
	Policy	:	Allow
	Source IP Address	:	210.168.219.45
	Source Subnet Mask	:	255.255.0.0
	Source Port	:	80
	Dest. IP Address	:	NA
	Dest. Subnet Mask	:	NA
	Dest. Port	:	NA
	Selected WAN interface	:	br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:	Filter Name	:	In_Filter2
	Protocol	:	UDP
	Policy	:	Allow
	Source IP Address	:	210.168.219.45
	Source Subnet Mask	:	255.255.0.0
	Source Port	:	5060:6060
	Dest. IP Address	:	192.168.1.45
	Dest. Sub. Mask	:	255.255.255.0
	Dest. Port	:	6060: 7070
	br0		

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in ridge mode. After a ridge mode connection is created, navigate to Advanced Setup \rightarrow Security \rightarrow MAC Filtering in the WUI.

Example 1:	Global Policy	: Forwarded
	Protocol Type	: PPPoE
	Dest. MAC Address	: 00:12:34:56:78:90
	Source MAC Address	: NA
	Src. Interface	: eth1
	Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00: 12: 34: 56: 78: 90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:	Global Policy	: locked
	Protocol Type	: PPPoE
	Dest. MAC Address	: 00:12:34:56:78:90
	Source MAC Address	: 00:34:12:78:90:56
	Src. Interface	: eth1
	Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the CT-5364A, as per chosen days of the week and the chosen times.

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

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

Appendix B - Pin Assignments

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

ETHERNET Ports (RJ45)

Appendix C - Specifications

Hardware Interface

RJ-11 X 1 for ADSL, RJ-45 X 1 for ETH WAN, RJ-45 X 4 for LAN, US Host, Power Switch X 1, Reset utton X 1, WPS X 1, Wi-Fi Antenna X 2

WAN Interface

ADSL standard ITU-T G.992.5,	ITU-T G.992.3, ITU-T G.992.1	I, ANSI T1.413 Issue 2
G.992.5 (ADSL2+)	Downstream : 24 Mbps	Upstream : 1.3 Mbps
G.992.3 (ADSL2)	Downstream : 12 Mbps	Upstream : 1.3 Mbps
G.DMT	Downstream : 8 Mbps	Upstream : 0.8 Mbps

LAN Interface

Standard		IEEE 802.3, IEEE 80	2.3u
10/100	aseT	Auto-sense	
MDI/MD>	support	Yes	

WLAN Interface

Standard	IEEE 802.11n (IEEE 802.11b/g compatible)
Encryption	64/128-bit Wired Equivalent Privacy (WEP)
Channels	11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate	Up to 270Mbps
WPA/WPA2	Yes
IEEE 802.1x	Yes
WDS	Yes
WMM	Yes
WPS	Yes
MAC Filtering	Yes
Optional	Afterburner mode (Turbo mode)***

ATM Attributes

Management

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

Networking Protocols

RFC2684 VC-MUX, LLC/SNAP encapsulations for bridged or routed packet RFC2364 PPP over AAL5 IPoA, PPPoA, PPPoE, Multiple PPPoE sessions on single PVC, PPPoE pass-through PPPoE filtering of on-PPPoE packets between WAN and LAN Transparent bridging between all LAN and WAN interfaces 802.1p/802.1q VLAN support Spanning Tree Algorithm IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave Static route, RIP v1/v2, DHCP Server/Client/Relay, DNS Relay, Dynamic DNS, ARP, RARP, SNTP

Security Functions

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

Application Passthrough

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

Power Supply	Input:	220 - 230 Vac
	Output:	15 Vdc / 0.8 A

Environment Condition

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

Kit Weight

(1*CT-5364A, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 0.9 kg

Certifications CE, FCC

NOTE: Specifications are subject to change without notice

Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -I root 192.168.1.1

For WAN access, type: ssh -I support WAN IP address

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

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

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

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

Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

STEP 1: Enable Print Server from Web User Interface. Select Enable on-board print server checkbox ☑ and enter Printer name and 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.

COMPREND O		
ADSL R	Router	
- All	Print Server settings	
	This page allows you to	enable / disable printer support.
Device Info Advanced Setup	Enable on-board prir	nt server.
WAN LAN	Printer name	
NAT	Make and model	
Security		
Quality of Service		
Routing		Save/Apply
DNS		58.
DSL		
Slave DSL		
Print Server		

STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).

Printers and Feam						E	
Elt Est Seu l'guertes	Locis	30					27
Q Q . #	p	wardh 🜔 Politiers 🚺	<u>1</u> -				
Approx 12 History and Fores							
Printers Tanks	0	Mane -	Documents 0	Status Ready	Lonnentz	He Excusion	1
🔛 Allanim		Please of the	0 0	Roady Roady		Statestics and a	19
Construction and the add	Printer	where distant is the second se	ntal a pirter.	Ready	00004-1 the On Level 0 00004-1 the On Level 0	0015A-1 0015A-1	10
Sec Abo	*						
🐒 bodied sot proting 🛃 Get help odd proting							
Other Places							
Constraint Scanner and Cameral Scanner and Cameral So December Ny Peterse Ny Computer							
Details							
		0					

STEP 3: Click **Next** to continue when you see the dialog box below.

Add Printer Wizard	
	Welcome to the Add Printer Wizard
	This wizard helps you install a printer or make printer connections
	You have a Plug and Play printer that connects through a USB pot (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you. To continue, click Next.
	Cancel

STEP 4: Select Network Printer and click Next.



STEP 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE: The printer name must be the same name entered in the ADSL modem WE UI "printer server setting" as in step 1.

Specify a Pr If you don that meets	Inter I know the name or address of the pinter, you can search for a preserving your needs.
What print	er do you want to connect to?
OBrida	printer in the directory
Ogerre	t to this preter (or to bossee for a preter, select this option and click Next)
None	
	Example: \\aerver\printer
⊙ Cgrine	s to a printer on the internet or on a home proffice network:
URL	ntp://192.168.1.1.631/pinters/hp.3846
	Example: http://werver/printers/hyperinter/printer
	SRetk Net 2 Carcel

STEP 6: Click **Have Disk** and insert the printer driver CD.

Select the r an installan pitter docu	nanufactur on dak, de mentation	er and model of your printer. If your printer can ok Have Dak. If your printer is not listed, cons for a competible printer.	në WEN ult your
Manufacturer	(n)	Fitnbers	ín
Agle Apolo Apolo Apple APS-PS AST	4	AGFA AccuSet v52.3 AGFA AccuSet SF v52.3 AGFA AccuSet B00 AGFA AccuSet B00 AGFA AccuSet B00SF v52.3 AGFA AccuSet B00SF v52.3 AGFA AccuSet B00SF v2013.108	×
This driver is digit	tely signed	Linsofart	Diek

STEP 7: Select driver file directory on CD-ROM and click **OK**.

Install F	rom Disk	×
, H	Inset the manufacturer's installation disk, and then make sure that the correct drive is selected below.	OK Cancel
	Croy manufacturer's files from: Ditenuitdervestaantite; yee	Down

STEP 8: Once the printer name appears, click **OK**.

dd Pr	inter Wizard	3
3	Select the menufacture and model of an installation date, click Have Date. If printer documentation for a compatible	your partier. If your partier came with your partier is not listed, consult your printer.
Parts	rs P Deskjet 3840 Seres	
E T	his driver is not digitally signed	Hove Dak
		OK Canoel

STEP 9: Choose Yes or No for default printer setting and click Next.

d Printer Wizard	
Default Printer Your computer will always send documents to the default printer unless you specify otherways.	Ŷ
Do you want to use this printer as the default printer?	
○Yes	
⊙№	
Back Next >	Cancel

STEP 10:Click Finish.

Completing the Add Printer Wizard				
You have successfully completed the Add Printer Wizard. You specified the following printer actings:				
Name: hp3845 on http://192.168.1.1:631 Default: No Location: Comment:				
To close this wizard, click Finish.	1			

STEP 11:Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.

Witness wid I am						alf to
the life per factors live :	*					2
0 0 0	en El Banno III-					
Active Transmission						
Aller Scher and Anne (1997)	New 7 SPACE INCOME SPACE INCOME	8 8 9 9 9	1100111	Service Street	The local data	Nor