

# CT-5374 Multi-DSL WLAN Router User Manual

Version A2.1, April 30, 2010



261099-005

#### 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.



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

#### 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.

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.

#### FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B 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 changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

# **Table of Contents**

CHAPTER	1 INTRODUCTION	5
1.1 Featu	RES	5
1.2 Applic	CATION	6
		_
CHAPTER	2 INSTALLATION	7
2.1 HARD	WARE SETUP	7
2.2 LED II	NDICATORS	9
CHAPTER	3 WEB USER INTERFACE	11
3.1 DEFAU	UT SETTINGS	11
3.2 IP CON	JEIGURATION	11
3 3 LOGIN	PROCEDURE	14
5.5 LOON		1 .
CHAPTER	4 DEVICE INFORMATION	16
4.1 WAN.		17
4.2 Statis	TICS	17
4.2.1	LAN Statistics	18
4.2.2	WAN Statistics	18
4.2.3	ATM Statistics	19
4.2.4	xDSL Statistics	21
4.3 ROUTE	3	27
4.4 ARP		28
4.5 DHCP	)	29
	5 ADVANCED SETUD	20
CHAPIER 5 1 LAVED	5 AD VANCED SETUP	30
5.1 LAYER	Z INTERFACE	30
5.1.1	AIM Interface	30
5.1.2	PIM Interface	31
5.1.3	ETH WAN INTERFACE	31
5.2 WAN		32
5.3 LAN		33
5.4 IPV6 L	AN HOST	35
5.5 NAT		36
5.5.1	Virtual Servers	36
5.5.2	Port Triggering	38
5.5.3	DMZ Host	39
5.6 SECUR	JTY	40
5.6.1	IP Filtering	40
5.6.2	MAC Filtering	42
5.7 PAREN	TAL CONTROL	44
5.7.1	Time Restriction	44
5.7.2	URL Filter	45
5.8 QUALI	TY OF SERVICE (QOS)	46
5.8.1	Queue Management Configuration	46
5.8.2	Queue Configuration	46
5.8.3	$\widetilde{Q}oS$ Classification	47
5.9 Routi	~~~~~ NG	49
5.9.1	Default Gateway	50
5.9.2	Static Route	
593	Policy Routing	51
594	RIP	52
595	IPv6 Static Route	52 53
5 10 DNS		55 54
5 10 1	DNS Server	54 51
5 10 2	Dynamic DNS	54 51
5 11 DSI		54 56
	D	50 59
5.12 UFNI	г Г Серулер	30 50
5 14 INTER		59 50
J.14 INTER	MACE UNUFINU	59

5.15 CERT	FICATE	
5.15.1	Local	
5.15.2	Trusted CA	
5.16 POWE	R MANAGEMENT	
CHAPTER	6 WIRELESS	
6.1 BASIC.		
6.2 SECUR	ТΥ	
6.2.1 W	PS	
6.3 MAC I	FILTER	
6.4 WIREL	ESS BRIDGE	
6.5 ADVAN	CED	
6.6 Statio	N INFO	
CHAPTER <sup>4</sup>	7 DIAGNOSTICS	
CUADTED	9 MANACEMENT	01 01
8 1 Settin	B MANAGEMEN I	82 82
8.1 SETTIN	Backun Settings	
812	Undate Settings	
813	Restore Default	83
8.2 System	A LOG	
8.3 SNMP	AGENT	
8.4 TR-069	9 Client	
8.5 INTERN	vet Time	
8.6 ACCES	S CONTROL	
8.6.1	Passwords	
8.7 Updat	E SOFTWARE	
8.8 REBOO	Т	
APPENDIX	A - FIREWALL	
APPENDIX	B - PIN ASSIGNMENTS	
APPENDIV	C - SPECIFICATIONS	05
APPENDIX	D - SSH ULIENT	
APPENDIX	E - WSC EXTERNAL REGISTRAR	
APPENDIX	F - PRINTER SERVER	
APPENDIX	G - CONNECTION SETUP	

# **Chapter 1 Introduction**

The CT-5374 Multi-DSL WLAN Router provides wired and wireless access for high-bandwidth applications in the home or office. It includes four fast Ethernet ports and supports ADSL2/2+ and VDSL2 connections with DSLAM switching. ADSL2+ connections support multiple simultaneous Internet connections while VDSL2 connections are suitable for triple play (Video + Voice + Data) applications.

An integrated 802.11n (draft) WLAN Access Point (AP) provides faster wireless connections with increased range, when compared with 802.11b and 802.11g, without sacrificing backwards compatibility with these older wireless standards. WPS (Wi-Fi Protected Setup) and Wi-Fi On/Off buttons are positioned on the front panel for easy wireless network setup and control.

### 1.1 Features

- Integrated 802.11n AP (802.11b/g backward-compatible)
- VDSL2 17a profile support
- IP and Per-VC packet level QoS
- WPA/WPA2 and 802.1x
- RADIUS client
- Static routing & RIP/RIP v2
- NAT/PAT
- IGMP Proxy and fast leave
- Web-based management
- Supports remote administration
- Configuration backup and restoration
- Firmware upgrade and configuration

- Automatic ADSL2+ / VDSL2 switching based on DSLAM setting
- Auto PVC configuration
- Supports up to 16 VCs
- WMM & UPnP
- IP/MAC filtering
- Dynamic IP assignment
- Parental Control
- DHCP Server/Relay/Client
- DNS Relay/Proxy
- FTP/TFTP server
- TR-069/TR-098/TR-104/TR-111

# 1.2 Application

The following diagrams depict typical applications of the CT-5374.





# **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.



#### Power ON

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

Caution 1: If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.
Caution 2: Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

#### **Reset Button**

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

**NOTE:** If pressed down for more than 20 seconds, the CT-5374 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

#### Ethernet (LAN) Ports

Use 10/100 BASE-T RJ-45 cables to connect up to four network devices. These ports are auto-sensing MDI/X; so either straight-through or crossover cable can be used.

#### **DSL Port**

Connect to an ADSL2/2+ or VDSL with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

#### FRONT PANEL

The Wi-Fi & WPS buttons are located on the bottom-left of the front panel, as shown.



#### WiFi Switch

Press this button to enable/disable the wireless LAN (WLAN).

#### **WPS Button**

Press this button to begin searching for WPS clients. These clients must also enable WPS push button mode (see 6.2.1 WPS for instructions).

# 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.

INTERNET POWER	ETH 1	ETH 2	ETH 3	ETH 4	WIRELESS	A/DSL	GbETH

LED	Color	Mode	Function
INTERNET		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.
	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.
		Blink	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
	Green	On	The device is powered up.
		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.
FTH 1X-4X	Green	Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
		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).
		Blink	Data transmitting or receiving over WLAN.
		On	xDSL Link is established.
A/DSL	Green	Off	xDSL Link is not established.
		Blink	fast: xDSL Link is training or data

			transmitting. slow: xDSL training failed.
	Green (for 10/100 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.
GbETH	Amber (for 10/100/1000 Base-T)	On	Powered device connected to the associated port.
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port.
		Blink	Traffic is passing.

# **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 (username: **support**, password: **support**)
- WLAN access: enabled

#### **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-5374 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

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

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

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

Internet Protocol (TCP/IP) Propert	ies ?X				
General					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
<ul> <li>Obtain an IP address automatic.</li> </ul>	ally				
${}_{\!$					
[P address:	· · · ·				
S <u>u</u> bnet mask:					
Default gateway:					
Obtain DNS server address auto	omatically				
$_{\Box} \odot$ Use the following DNS server a	ddresses:				
Preferred DNS server:					
Alternate DNS server:					
	Ad <u>v</u> anced				
	OK Cancel				

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

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

#### **STATIC IP MODE**

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

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

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

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

Internet Protocol (TCP/IP) Propertie	es <mark>?</mark> ×				
General					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
O <u>O</u> btain an IP address automatica	lly				
<ul> <li>Use the following IP address:</li> </ul>					
IP address:	192.168.1.133				
S <u>u</u> bnet mask:	255.255.255.0				
<u>D</u> efault gateway:					
C Obtain DNS server address auto	matically				
─● Use the following DNS server ad	dresses:				
Preferred DNS server:	· · ·				
Alternate DNS server:	· · ·				
Ad <u>v</u> anced					
	OK Cancel				

**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 3.1 Default Settings.

- **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 Chapter 4 Device Information screen and login with remote username and password.
- **STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.

Enter Netw	vork Passwor	d _	''×
<b>?</b> >	Please type yo	our user name and password.	
8	Site:	192.168.1.1	
	Realm	DSL Router	
	<u>U</u> ser Name		
	<u>P</u> assword		
	□ <u>S</u> ave this p	password in your password list	
		OK Cancel	
			_

Click **OK** to continue.

**NOTE:** The login password can be changed later (see 8.6.1Passwords).

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

Wireless	/DSL2 Router				
N	Device Info				
Dourise Info	Board ID:	96368	M-1331N		
Advanced Setun	Software Version:	0411-4	0411-402CTU-C01_R01.A2pv6bC013a.d22		
Wireless	Bootloader (CFE) Version:	1.0.37-102.6-10			
Diagnostics	Wireless Driver Version:	ion: 5.10.85.0.cpe4.402.4		4	
Management	Serial Number:	0985374xxxf-an000070			
	This information reflects the current status of your connection.				
	Line Rate - Opstream (Kbp	(bps):			
	Line Rate - Downstream (i	vuha).	102 160 1 1		
	Default Cateway		192,100,1,1		
	Default GateWay:				
	Primary DNS Server:		a an		
	Secondary Divs Server:				
	LAN IPV6 Address:				
	Default IPv6 Gateway:				

# **Chapter 4 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.

COMPRESS Wireless	<b>DSL2 Router</b>				
	Board ID:	96368	M-1331N		
Device Info Advanced Setun	Software Version:	0411-4	402CTU-C01_F	R01.A2pv6bC013a.d22	
Wireless	Bootloader (CFE) Version:	1.0.37-	-102.6-10		
Diagnostics	Wireless Driver Version:	5.10.85	5.0.cpe4.402.4	4	
Management	Serial Number:	098537	374xxxf-an000070		
	This information reflects the cu	urrent si	tatus of your o	connection.	
	Line Rate - Downstream (I	(bps):			
	LAN IPv4 Address:		192.168.1.1		
	Default Gateway:				
	Primary DNS Server:				
	Secondary DNS Server:				
	LAN IPv6 Address:				
	Default IPv6 Gateway:				

The Device Info Summary screen displays at startup.

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

# 4.1 WAN

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

	VDSL2 Router											
A						WA	N Info					
Device Info		Interface	Description	Туре	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address
Summary WAN Statistics												

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Туре	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows WAN IPv6 address
IGMP	Shows Internet Group Management Protocol (IGMP) status
MLD	Shows Multicast Listener Discovery (MLD) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address

### 4.2 Statistics

This selection provides LAN, WAN, ATM/PTM and xDSL statistics.

**NOTE:** These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update.

### 4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

GOMMEND O Wireless V	DSL2 R	oute	ər						
N	Statistics -	LAN							
Davies Infe	Interface		Rece	ived		Т	ransn	nitteo	t
Support		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
wan	eth0	0	0	0	0	0	0	0	0
Statistics	eth1	180887	1536	0	0	476098	1571	0	0
LAN	eth2	0	0	0	0	0	0	0	0
WAN Service	eth3	0	0	0	0	0	0	0	0
хтм	eth4	0	0	0	0	0	0	0	0
xDSL	wl0	0	0	4	0	23968	244	16	0
Route ARP DHCP	Reset Si	tatistics							

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

#### 4.2.2 WAN Statistics

This screen shows data traffic statistics for each WAN interface.

Wireless VI	<b>DSL2 Router</b> Statistics WAN		
Device Info	Interface Description	Received	Transmitted
Summary WAN		руцезркізсті з рі ор	sbytespitiserrsbrops
Statistics	Reset Statistics		
LAN WAN Service			
xTM xDSL			

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

### 4.2.3 ATM Statistics

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

				In	terface S	tatisti	cs				
Device Info	Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cel Errors
Summary WAN Statistics LAN WAN Service XTM xDSI					Rese	۹t					

#### **ATM Interface Statistics**

Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of received octets over the interface

Heading	Description
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.

Heading	Description
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

#### 4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type. The two examples below (VDSL & ADSL) show this variation.

#### VDSL

Wireless	VDSL2 Router				
- And	Statistics xDSL				
levice Info	Mode:		VDSL2		
Euromany	Traffic Type:		PTM		
Summary	Status:		Up		
WAN	Link Power State:		LO		
Statistics					
LAN		Downstrea	mUpstrea	m	
WAN Service	Line Coding(Trellis):	On	Off		
хTM	SNR Margin (0.1 dB):	214	0		
xDSL	Attenuation (0.1 dB):	10	þ		
Route	Output Power (0.1 dBm):	10	-28		
ADD	Attainable Rate (Kbps):	140272	52960		
AKP					
DHLP		Path 0		Path 1	
dvanced Setup		Downstrea	m Upstrea	m Downstre	am Upstream
Vireless	Rate (Kbps):	84995	49997	0	0
iagnostics					
lanagement	B (# of bytes in Mux Data Frame):	238	223	0	0
-	M (# of Mux Data Frames in an RS codeword):	1	1	0	0
	T (# of Mux Data Frames in an OH sub-frame):	19	3	0	0
	R (# of redundancy bytes in the R5 codeword):	16	12	0	0
	5 (# of data symbols over which the R5 code word spans)	0.0895	0.1426	0.0000	0.0000
	L (# of bits transmitted in each data symbol):	22800	13240	0	0
	D (interleaver depth):	44	1	0	0
	I (interleaver block size in bytes):	255	118	0	0
	N (RS codeword size):	255	236	0	0
	Delay (msec):	1	0	0	D
	INP (DMT symbol):	0.00	0.00	0.00	0.00
	HEC Errors:	0	0	0	0
	OCD Errors:	0	0	0	0
	LCD Errors:	0	0	0	D
	Total Cells:	296828551	0	0	0
	Data Cells:	1150	0	0	D
	Bit Errors:	0	þ	0	þ
	Total FS:	10	1		
	Total SES:	10	n	-	
	Total UAS:	55	55	-	
	rotaroms.	00	20		

#### ADSL

COMTREND O					
Wireless V	DSL2 Router				
	Statistics xDSL				
AV					
	Mode:		VDSL2		
evice Info	Traffic Type:		PTM		
Summary	Status:		Up		
WAN	Link Power State:		μo	_	
Statistics		<b>_</b>		-	
LAN		Downstrea	mUpstream	n	
WAN Service	Line Loding(Trellis):	Un	Un	_	
vTM	SNR Margin (U.1 dB):	1/8	104	_	
··DEI	Accenuation (0.1 dB):	0	0	_	
RUSL	Output Power (0.1 dBm):	92	F7202		
Rouce	Accalitable Kace (Kbps):	103156	p7362		
ARP		Dath 0		Dath 1	50
DHCP		Downstrees	mUnchean	Downstream	Unchena
idvanced Setup	Rate (Khnc):	pownstrea	FOOD	n	n
Vireless	Race (RDps).	22222	poooo	p	p
agnostics	B ( # of bytes in Muy Data Frame)	04	124	h	0
- 1anagement	M (# of Muy Data Frames in an PS codeword):	1	1	р b	6
	T (# of Mux Data Frames in an K5 codeword).	49	2	<u>р</u> Б	6
	P (# of redundancy bytes in the PS codeword):	16	16	р b	6
	5 (# of data symbols over which the DS code word sr	ans):0.0302	0.0795	0.0000	0.0000
	1 (# of bits transmitted in each data symbol);	29376	14193	n	n
	D (interleaver depth):	532	178	n n	6
	I (interleaver block size in bytes):	111	141	0	6
	N (RS codeword size):	111	141	<u>n</u>	6
	Delay (msec):	4	4	<u>n</u>	6
	INP (DMT symbol):	1.00	0.50	0.00	0.00
		1100	pice	pice	pres
	OH Frames:	108921	50796	b	0
	OH Frame Errors:	0	0	6	0
	R5 Words:	15684402	1796754	6	6
	RS Correctable Errors:	0	0	6	0
	RS Uncorrectable Errors:	0	0	6	0
		15		1.	15
	HEC Errors:	0	0	ю	0
	OCD Errors:	0	0	6	0
	LCD Errors:	0	0	0	0
	Total Cells:	22882542	0	0	0
	Data Cells:	1952	D	D	0
	Bit Errors:	0	0	0	0
	Total ES:	0	6		
	Total SES:	0	6		
	Total UAS:	314	314		
		1.000 A			

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

Field	Description
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2
Traffic Type	Channel type Interleave or Fast
Status	Lists the status of the DSL link
Link Power State	Link output power state.

Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

#### In VDSL mode, the following section is inserted.

В	Number of bytes in Mux Data Frame
М	Number of Mux Data Frames in a RS codeword
Т	Number of Mux Data Frames in an OH sub-frame
R	Number of redundancy bytes in the RS codeword
S	Number of data symbols the RS codeword spans
L	Number of bits transmitted in each data symbol
D	The interleaver depth
Ι	The interleaver block size in bytes
Ν	RS codeword size
Delay	The delay in milliseconds (msec)
INP	DMT symbol

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

MSGc	Number of bytes in overhead channel message
В	Number of bytes in Mux Data Frame
М	Number of Mux Data Frames in FEC Data Frame
Т	Mux Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

#### 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)

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

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

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

#### **xDSL BER TEST**

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.

🗿 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 🔮 Internet 🦼

Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.

🕘 http:	//192.168.1.1/berstop.	tst?berState=0 - Mi									
	ADSL BER Test - Result										
The ADSL BER test completed successfully.											
	Test Time (sec):	20									
	Total Transferred Bits:	0x0000000000000000									
	Total Error Bits:	0x00000000000000000									
	Error Ratio:	Not Applicable									
Close											
			~								
ど Done		🌍 Internet									

#### **xDSL TONE GRAPH**

Click **Draw Tone Graph** on the xDSL Statistics screen and a pop-up window will display the xDSL bits per tone status, as shown below.



# 4.3 Route

Choose **Route** to display the routes that the CT-5374 has found.

COMMEND O	DSL2 Ro	uter								
-47	Device Info Route									
Device Info	Flags: U - up, I D - dynamic (n	l - reject, G edirect) M -	- gateway, H - h - modified (redin	iost, R ect)	- reinsta	te				
Summary	D ayrianne (i	Surcey, m	moanica (realit							
WAN	Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface			
Statistics	192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0			
Route	L	1								
ARP										

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

### 4.4 ARP

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

Company Company Company Company	VDSL2 Ro	uter		
N	Device Info	ARP		
Douico Info	IP address	Flags	HW Address	Device
Summary WAN Statistics Route	192.168.1.2	Complete	00:25:11:AF:FD:F8	br0
ARP				
DHCP				

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

### **4.5 DHCP**

Click  $\ensuremath{\textbf{DHCP}}$  to display all DHCP Leases.

COMPREND O Wireless	DSL2 Ro	uter		
Device Info Summary	Device Info - Hostname	MAC Address 00:25:11:af:fd:f8	<b>IP Address</b> 192.168.1.2	Expires In 55 seconds
WAN 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 5 Advanced Setup**

Click on the link to jump to a specific section:

5.1 Layer 2 Interface	5.9 Routing
5.2 WAN	5.10 DNS
5.3 LAN	5.11 DSL
5.4 IPv6 LAN Host	5.12 UPnP
5.5 NAT	5.13 Print Server
5.6 Security	5.14 Interface Grouping
5.7 Parental Control	5.15 Certificate
5.8 Quality of Service (QoS)	5.16 Power Management

### 5.1 Layer 2 Interface

The ATM, PTM and ETH WAN interface screens are described here.

### 5.1.1 ATM Interface

Add or remove ATM interface connections here.

	L2 Router
- AN	DSL ATM Interface Configuration Choose Add, or Remove to configure DSL ATM interfaces.
Device Info	
Advanced Setup	Interface Vpi Vci DSL Latency Category Link Type Connection Mode QoS Remove
Layer2 Interface ATM Interface PTM Interface ETH Interface	(Add) Remove

Click **Add** to create a new ATM interface (see Appendix G).

**NOTE:** Up to 8 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

#### 5.1.2 PTM Interface

Add or remove PTM interface connections here.

Wireless VDSL2 Router	,					
		DSL I Choose Add, or	<b>PTM Interface</b> Remove to con	Configuration	aces.	
Device Info			-			
Advanced Setup	Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove
Layer2 Interface ATM Interface PTM Interface ETH Interface	2		Add Rer	nove	l,	

Click **Add** to create a new connection (see Appendix G - Connection Setup). To remove a connection, select its Remove column radio button and click **Remove**.

#### 5.1.3 ETH WAN INTERFACE

This screen displays the Ethernet WAN Interface configuration.

NOTE:	This optio	n only a	applies	to mode	els wit	ch an Ether	ne	t WAN port.	
Bonne Wire		DSL2	Rout	er					
	N				cł	ETH WAR	l In	terface Configurati	ion
Device Info					CI.	Allow one	ETH	as layer 2 wan inter	face.
Advanced S	etup								
Layer2 Int	erface					Interface/(Nar	ne)	Connection Mode	Remove
ATM Inte	erface								
PTM Inte	erface						Add	d Remove	
ETH Inte	rface								

Click **Add** to create a new connection (see Appendix G - Connection Setup).

**NOTE:** One Ethernet WAN interface can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click remove.

# 5.2 WAN

This screen allows for the configuration of WAN interfaces.

COMPREND O Wireless VDSI	L2 Route	r										
- A		Choose	o Add ic	Wide Area	Network (W	/AN) Ser	vice Se	tup	ted interf	200		
Device Info Advanced Setup		Choose	, Add, C	ETH and P	TM/ATM serv	rice can no	ot coexi	st.		ace.		
ATM Interface	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Mld	Remove
PTM Interface ETH Interface WAN Service					Add Rei	move						

Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see Appendix G - Connection Setup.

NOTE:	ETH and ATM service connections cannot coexist. In Default Mode, up to
	8 WAN connections can be configured; while VLAN Mux and MSC
	Connection Modes support up to 16 WAN connections.

To remove a connection, select its Remove column radio button and click **Remove**.

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Туре	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
ConnId	Connection ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD	Shows Multicast Listener Discovery (MLD) status
Remove	Select interfaces to remove

To remove a connection, select its Remove column radio button and click **Remove.** 

To **Add** a new WAN connection, click the **Add** button and follow the instructions.

**NOTE:** Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist.

# 5.3 LAN

Configure the LAN interface settings and then click **Apply/Save**.

GOMTREND) O	
wireless v	DSL2 Router
	Local Area Network (LAN) Setup
A	
	Configure the router IP Aduress and Subnet Mask for LAN Interface. GroupName
Device Info	IP Address: 192.168.1.1
Advanced Setup	Subnet Mask: 255.255.0
Layer2 Interface	Concrete the sector of the sec
ATM Interface	Enable IGMP Snooping
PTM Interface	
ETH Interface	Enable LAN side firewall
WAN Service	O Disable DHCP Server
LAN	Enable DHCP Server
IPv6 LAN Config	Start IP Address: 192.168.1.2
Security	End IP Address: 192.168.1.254
Parental Control	
Quality of Service	Ctatic ID Lacas List: (A maximum 22 patrice are to configured)
Routing	Static IP cease cist; (A maximum 32 entries can be conligured)
DNS	MAC Address IP Address Remove
DSL	Add Entries Remove Entries
Upnp	
Print Server	C Enable DHCP Server Relay
Interface Grouping	DHCP Server IP Address:
Certificate	
Power Management	Configure the second IP Address and Subnet Mask for LAN interface
	Apply/Save

Consult the field descriptions below for more details.

**GroupName:** Select an Interface Group.

#### **1<sup>st</sup> LAN INTERFACE**

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

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

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

**Enable LAN side firewall:** Enable by ticking the checkbox **I**.

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

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

MAC Address	IP Address Remove
Add Entries	Remove Entries

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

Dhcpd Static IP Lease				
Enter the Mac address and desired IP address then click "Save/Apply" .				
MAC Address:	12:34:56:78:90:12			
IP Address:	192.168.1.33			
		Save/Apply		

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



**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. <u>This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.</u>

#### 2<sup>ND</sup> LAN INTERFACE

To configure a secondary IP address, tick the checkbox  $\square$  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.

### 5.4 IPv6 LAN Host

Configure the IPv6 LAN Host options (see below) and then click **Save/Apply**.

COMTRENDO	VDSI 2 Boutor
mireless	VDSL2 Router
M	IPv6 LAN Host Configuration
Device Info	Enable DHCPv6 Server
Advanced Setup Layer2 Interface	Enable RADVD
WAN Service LAN	IPv6 Site Prefix Configuration Type:
IPv6 LAN Config Security	Delegated from WAN
Parental Control	WAN Interface selected:
Quality of Service	O Static
Routing	Site Prefix:
DNS	Site Prefix Lenath:
DSL	
Upnp Duint Commun	
Print Server	Enable MLD Snooping
Certificate	
Power Management	<ul> <li>Standard Mode</li> <li>Riedking Mode</li> </ul>
Wireless	
Diagnostics	Save/Apply
Management	

- **DHCPv6 Server:** To enable DHCP for IPv6, select the **Enable DHCPv6 server** checkbox ∅. This setting enables the router to assign IP settings to every IPv6-capable LAN device (IPv6 clients).
- **RADVD:** Select the checkbox ☑ to enable the **R**outer **ADV**ertisement **D**aemon. This provides information that IPv6 clients can use for autoconfiguration according to the <u>Neighbour Discovery for IPv6</u> protocol (RFC2461).

#### **IPv6 Site Prefix**

This setting can be delegated from a WAN Interface or assigned statically.

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

### 5.5 NAT

To display this option, NAT must be enabled in at least one PVC shown on the Chapter 5 Advanced Setup - . *NAT is not an available option in Bridge mode*.

#### 5.5.1 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.

Gommand O Wireless	/DSL2 R	outer							
Jest "	NAT Vir	tual Servers Setu	ıp						
Device Info Advanced Setup Layer2 Interface WAN Service	Virtual Serv private IP a used by the	er allows you to dir ddress on the LAN s server on the LAN	ect incoming traff side. The Internal side. A maximum	fic from WA port is requ 32 entries	N side (identified iired only if the e) can be configured Add Remove	by Protocol and E (ternal port needs I.	xternal port) to ; to be converte	the Internal serv d to a different p	er with ort number
IPv6 LAN Config NAT	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Virtual Servers Port Triggering DMZ Host									

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

GOMTREND		
Wireless VI	DSL2 Router	
	NAT Virtual Serve	ers
N	Colored Management	
	select the service nam server. NOTE: The "In	he, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port"
Device Info	End". However, if yo	ou modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Po
Advanced Setup	Start".	
Layer2 Interface	Remaining number o	of entries that can be configured:32
WAN Service	l la a Taba Gara	
LAN	Ose Interface	bbboe_n_n_pp/bbbn
IPv6 LAN Config	Service Name;	SelectOne
NAT	<ul> <li>Select a Service;</li> </ul>	
Virtual Servers	O Custom Service:	
Port Triggering	Server IP Address	102 168 1
DMZ Host	Jerver I Address,	12.100.1
Security		
Parental Control		Apply/Save
Quality of Service		
Routing	External Port Start E	External Port End Protocol Internal Port Start Internal Port End
DNS		TCP 🗸
DSL		TCP
Upnp		
Print Server		
Interface Grouping		
Certificate		TCP V
Power Management		
		Apply/Save

Consult the table below for field and header descriptions.

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

### 5.5.2 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.

GOMMEND O	DSL2 Rout	ter									
- A	NAT Port Trig	gering Setup									
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Some applications opens up the 'Ope 'Triggering Ports'. side using the 'Opi	require that specific   n Ports' in the firewal The Router allows th en Ports'. A maximum	ports in the I when an a e remote pa 1 32 entries	Router's pplicatic arty fron can be (	s firew on on t n the W configu Add	all be open he LAN initi /AN side to red. Remove	ed for ad ates a Ti establis	ccess b CP/UDI h new	y the remote parti ? connection to a r connections back 1	es. Port Tri emote party to the applic	;ger dynamically : using the ation on the LAN
NAT			Tr	igger		C	)pen				
Virtual Servers		Application Name	Ductocal	Port R	ange	Dustanal	Port R	ange	WAN Interface	Remove	
Port Triggering DM2 Host			Protocol	Start	End	Protocol	Start	End			

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

Wireless V	DSL2 Router					
	NAT Port Triggering					
Device Info Advanced Setup	Some applications such as ga firewall be opened for access creating your own (Custom a <b>Remaining number of entr</b>	mes, video conferenci by the applications. Y aplication)and click "Sa ies that can be con	ing, remote acce 'ou can configure ave/Apply" to ac <b>figured:32</b>	ess applications ar e the port settings Id it.	d others require that s from this screen by se	pecific ports in the Router's lecting an existing application or
WAN Service	Application Name	hbboe_o_o_ootbbbc				
LAN	<ul> <li>Select an application.</li> </ul>	Select One	~			
IPv6 LAN Config	<ul> <li>Oustom poplication;</li> </ul>					
NAT	Custom application.	L				
Virtual Servers			Sa	ave/Apply		
Port Triggering	Trigger Port Start Trigge	r Dort End Trigger D	rotocol Open P	ort Start Onen D	Port End Open Protor	ol
DMZ Host	mggerrörtstartingge	TCP		or e ottar coperri		
Security						
Parental Control		TCP	~		TCP	
Quality of Service		TCP	<b>~</b>		TCP	
Routing		TCP	~		TCP	
DNS		TCP	~		TCP	
DSL		TOP			TOP	
Upnp			×			
Print Server		TCP	~		TCP	*
Interface Grouping Certificate		TCP	~		TCP	
Power Management			Sa	ave/Apply		

Consult the table below for field and header descriptions.

Field/Header	Description
Use Interface	Select a WAN interface from the drop-down box.
Select an Application <b>Or</b> Custom Application	User should select the application from the list. Or User can enter the name of their choice.

Field/Header	Description
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.

#### 5.5.3 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.

Wireless	/DSL2 Router
M	NAT DMZ Host
	The 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
Device Info	DMZ host computer.
Advanced Setup	
Layer2 Interface	Enter the computer's IP address and click "Apply" to activate the DMZ host.
WAN Service	Clear the IP address field and click "Apply" to deactivate the DMZ bost
LAN	cital site a data con fora and citex oppry to dedecidate the brite hold
IPv6 LAN Config	DMZ Host IP Address:
NAT	
Virtual Servers	Save/Apply
Port Triggering	
DMZ Host	

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**.

### **5.6 Security**

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

#### 5.6.1 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, 5.6.2 MAC Filtering (pg. 422) performs a similar function.
```

#### **OUTGOING IP FILTER**

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

Wireless V	DSL2	Route	,					
M	Outgoir	ng IP Filtering	j Setup		V-141			
	By defau	ult, all outgoing	) IP traffic f	rom LAN is allowed, but s	ome IP traffic can	be <b>BLOCKED</b> by setting up	o filters.	
Device Into	Chasses	add or Domou	o to configu	wa autonica 10 Altors				
Advanced Setup	CHOUSE	AUU OF REMOV	e w conngi	are oalgoing in mers.				
Layer2 Interface		Filtor Nomo	Drotocol	Courco Addroce / Ma	k Courco Dort	Doct Addross / Mask	Doct Dort	Popouo
WAN Service		riter Name	FIOCOCOF	Source Address / Ma	Source Port	Dest. Address / mask	Dest. Port	Kemove
LAN						1		
IPv6 LAN Config					Add Remove	J		
Security								
IP Filtering								
Outgoing								
Incoming								

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**.

COMPREND O	
Wireless	DSL2 Router
AN	Add IP Filter Outgoing
	The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition
Device Info	below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter
Advanced Setup	ure mean.
Layer2 Interface	Filter Name
WAN Service	
LAN	Protocol:
IPv6 LAN Config	
Security	Source IP address:
IP Filtering	Source Subnet Mask:
Outgoing	Source Port (port or port:port):
Incoming	Destination IP address:
Parental Control	
Quality of Service	
Routing	Destination Port (port or port:port):
DNS	
DSL	America
Upnp	Apply/Save

Consult the table below for field descriptions.

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

#### **INCOMING IP FILTER**

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

	DSL2 Ro	uter						
- A	Incoming IP F	iltering Set	up					
Device Info	When the firev ACCEPTED by	vall is enabled setting up filt	d on a WAN ærs,	or LAN interface, all incomir	ng IP traffic is B	LOCKED. However, some I	P traffic can b	)e
Advanced Setup Layer2 Interface	Choose Add or	Remove to c	onfigure ind	coming IP filters.				
WAN Service LAN	Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
IPv6 LAN Config Security IP Filtering Outgoing Incoming				Add R	emove			
Parental Control								

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**.

COMPREND O	DSL2 Router
	Add IP Filter Incoming
Device Info	The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Advanced Setup	
Layer2 Interface	Filter Name:
WAN Service	
LAN	Protocol:
IPv6 LAN Config	Source IP address:
Security	Source Subnet Mask:
IP Filtering	Source Part (nort or portmort)
Outgoing	
Incoming	Destination IP address:
Parental Control	Destination Subnet Mask:
Quality of Service	Destination Port (port or port:port):
Routing	
DNS	WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
DSL	Selectione of more www.yc.A.v interfaces displayed below to apply this fulle.
Upnp	✓ Select All
Print Server	🗹 br0/br0
Interface Grouping	
Certificate	
Power Management	Apply/Save
Wireless	

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.

#### 5.6.2 MAC Filtering

**NOTE:** This option is only available in bridge mode. Other modes use 5.6.1 IP Filtering (pg. 40) 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-5374 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.

Wireless V	DSL2 Router
- A	MAC Filtering Setup
Device Info Advanced Setup	MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
Layer2 Interface WAN Service LAN	MAC Filtering Policy For Each Interface: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
IPv6 LAN Config	Interface Policy Change
Security	
MAC Filtering	
Parental Control	
Quality of Service	Change Policy
DSI	Chance Add or Bornova to configure MAC filtering rules
Upnp	choose Add of Nemore to configure rake mitering rules.
Print Server	Interface Protocol Destination MAC Source MAC Frame Direction Remove
Interface Grouping	
Certificate	Add Remove

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

Wireless V	/DSL2 Router	
- w	Add MAC Filter	
Device Info Advanced Setup	Create a filter to identify the effect. Click "Apply" to save	MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take and activate the filter.
Layer2 Interface	Protocol Type:	✓
WAN Service	Destination MAC Address:	
LAN IPv6 LAN Config	Source MAC Address:	
NAT Security	Frame Direction:	LAN<=>WAN
MAC Filtering	WAN Interfaces (Configured	in Bridge mode only)
Parental Control	-	
Quality of Service	br_0_0_35/atm0 🐱	
Routing		
DSL		Save/Apply

Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface.

# **5.7 Parental Control**

This selection provides WAN access control functionality.

#### 5.7.1 Time Restriction

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 8.5 Internet Time, so that the scheduled times match your local time.

	V	Þ	ŞL:	21	Roi	ute	r												
- A			Acce	ess T	ime f	Restri	iction A	ma	ximum	16 er	ntries	can b	e con	figu	red.				
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 LAN Config Security							Userna	me	MAC	Mon	Tue	Add	Thu Re	Fri	Sat	Sun	Start	Stop	Remove
Parental Control Time Restriction Url Filter																			

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

Wireless V	DSL2 Router
A	Access Time Restriction
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 LAN Config Security Parental Control Time Restriction	This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /al". User Name    Browser's MAC Address Other MAC
Url Filter Quality of Service	Days of the week MonTueWedThuFri SatSun Click to select
Routing DNS DSL Upnp Dns Proxy Print Server Interface Grouping Certificate Power Management	Start Blocking Time (hh:mm)

See below for field descriptions. Click **Apply/Save** 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.

#### 5.7.2 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.

	DSL2 Router
- A	URL Filter Please select the list type first then configure the list entries. Maximum 100 entries can be configured.
Device Info Advanced Setup Layer2 Interface WAN Service LAN IPv6 LAN Config Security Parental Control Time Restriction Ittl filter	URL List Type: O Exclude Include

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

Par	Parental Control URL Filter Add							
Ent	Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.							
LIRI	Address;	www.yaboo.com	l					
Por	t 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 1	00 entries can b	e configured.			
URL List Type: 🔿 Exclude	🔘 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.

### 5.8 Quality of Service (QoS)

**NOTE**: QoS must be enabled in at least one PVC to display this option. (see Appendix G - Connection Setup for detailed PVC setup instructions).

#### 5.8.1 Queue Management Configuration

To Enable QoS tick the checkbox  $\square$  and select a Default DSCP Mark.

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

	VDSL2 Router
- A	QoS Queue Management Configuration
Device Info	If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.
Advanced Setup	
WAN Service	Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
IPv6 LAN Config	Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Security Parental Control	Enable QoS
Quality of Service	
QoS Classification	
Routing	
DISL	Apply/Save

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.

#### 5.8.2 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.

GOMMEND OF Wireless V	DSL2 Route	r						
- And	<b>QoS Queue Setup</b> If you disable WMM fu	- A ma	<b>ximum 24 e</b> in Wireless P	ntries can be ( age, queues rel	c <b>onfigured.</b> ated to wireless	will not take effi	ects	
Device Info	The OoP function b	e hoo	n disablad u	Ouques would	not take offer	te		
Advanced Setup	The gos function ha	is dee	n uisabieu.	queues would	not take enet	.15.		
Layer2 Interface	Namo	Key	Interface	Drecedence	DSI Latency	DTM Driority	Fnahle	Romovo
WAN Service		KCy	Interface	Treccachee	DOL LUCCILLY	Thirribitey	Endbic	Kemove
LAN	WMM Voice Priority	1	wl0	1			Enabled	
Security	WMM Voice Priority	2	wlo	2			Enabled	
Parental Control	WMM Video Priority	З	wl0	3			Enabled	
Quality of Service	WMM Video Priority	4	wl0	4			Enabled	
Queue Config	winim mideo miority	-	W10	-			Liableu	
QoS Classification	WMM Best Effort	5	wl0	5			Enabled	
Routing DNS	WMM Background	6	wlo	6			Enabled	-
DSL	WMM Background	7	wlo	7			Enabled	
Upnp Print Server	WMM Best Effort	8	wlo	8			Enabled	
Interface Grouping Certificate	Add Enable Re	move	]					

Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.

COMPREND O Wireless	/DSL2 Route	r
- A	QoS Queue Configu	ation
Device Info Advanced Setup Layer2 Interface	The screen allows yo configured for a spe appropriately. <b>Note:</b> 'Apply/Save' to save	I to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be fic precedence. The queue entry configured here will be used by the classifier to place ingress packets .ower integer values for precedence imply higher priority for this queue relative to others Click ind activate the queue.
WAN Service LAN	Name:	
IPv6 LAN Config Security	Enable:	Disable 🗸
Parental Control Quality of Service	Interface:	<b>v</b>
Queue Config QoS Classification	Precedence:	1 🛩
Routing DNS		Apply/Save

Name: Identifier for this Queue entry.

**Enable:** Enable/Disable the Queue entry.

**Interface:** Assign the entry to a specific network interface (QoS enabled).

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

#### 5.8.3 QoS Classification

The network traffic classes are listed in the following table.

	/DSL	2 R	out	er																
- AN	QoS Cla	assifica	ation S	etup -	- A maxin	num 32 en	tries ca	n be coi	nfigure	d.										
Device Info	Choose If you d	Add or isable \	Remov MMM fi	/e to co unction	in Wireless	twork traffic Page, clas	: classes sification	: related	tn wirel	ess w	ill not :	take effi	ects							
Advanced Setup Layer2 Interface	The Qo	S func	tion ha	as bee	n disableo	l. Classific	ation ru	iles wou	ld not	take (	effect	s.								
WAN Service						CLAS	SIFICAT	ION CRI	TERIA					CI	LASSI	FICATIO	N RESUL	.TS		
LAN IPv6 LAN Config Security	Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove
Parental Control Quality of Service Queue Config QoS Classification								Add	Enable	9 F	lemovi	e								

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.

Wireless	VDSL2 Router
	Add Naturality Teoffic Class Dula
N	Aud Network frame Gass Rule
	The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally our ways to the Tabadar DCCR but a 4 rule consist of a class page and at least one condition below. All of the precified conditions in this classification.
Device Info	rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Advanced Setup	
Layer2 Interface	Traffic Class Name:
WAN Service	Rule Order:
LAN	Rule Status: Disable 💌
IPv6 LAN Config	
Security	Specify Classification Criteria A black criterian indicate it is not used for classification
Parental Control	A blair cheilionn indicates in is not used foir classification.
Quality of Service	Class Interface:
Queue Config	Ether Type:
QoS Classification	Source MAC Address:
DNS	Source MAC Mask:
DSL	Destination MAC Address:
Upnp	Destination MAC Mask:
Print Server	Specify Placefication Results
Interface Grouping Certificate	Must select a classification queue. A blank mark or tag value means no change.
Power Management	Assign Classification Queue:
Wireless	Mark Differentiated Service Code Point (DSCP):
Diagnostics	Mark 802.1p priority:
	Tag VLAN ID [0-4094]:
	Set Rate Control(kbps):
	Apply/Save

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).

Field	Description
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.
Classification Results	
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece <u>P</u> &Queue Q" 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.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. Lower values have higher priority.
Tag VLAN ID	Enter a 802.1Q VLAN ID tag [2-4094]
Set Rate Control	The data transmission rate limit in kbps.

### 5.9 Routing

This following routing functions are accessed from this menu: **Default Gateway, Static Route, Policy Routing, RIP** and **IPv6 Static Route**.

**NOTE:** In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.