

CT-5365 ADSL2+ Wireless Router User Manual

Version C1.0, May 22, 2009



260094-001

Preface

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

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

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.

Copyright

Copyright©2009 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.

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, ask for disposal instructions from your municipal government.

Table of Contents

CHAPTER 1	SUMMARY	.5
1.1 Featur	ES	. 5
1.2 APPLICA	NTION	. 5
1.3 LED IN	DICATORS	.6
CHAPTER 2	INSTALLATION	7
2 1 HARDW	ARE INSTALLATION	7
2.1 11ARD W	ALL INGIALLATION	. /
CHAPTER 3	WEB USER INTERFACE	.8
3.1 DEFAUL	T SETTINGS	. 8
3.2 IP CONF	IGURATION	. 8
3.3 Login I	PROCEDURE	10
CHAPTER 4	OUICK SETUP	12
4.1 AUTO O	UICK SETUP	12
4.2 MANUA	L QUICK SETUP	13
4.2.1	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)	15
4.2.2	MAC Encapsulation Routing (MER)	19
4.2.3	IP Over ATM.	23
4.2.4	Bridging	26
		•••
CHAPTER 5	DEVICE INFORMATION	28
5.1 WAN		29
5.2 STATIST		30
5.2.1	LAN Statistics	50
5.2.2	WAN Statistics	31
5.2.3	ATM statistics	32
5.2.4	ADSL Statistics	34
5.3 ROUTE.		37
5.4 ARP		38
5.5 DHCP .		38
CHAPTER 6	ADVANCED SETUP	39
6.1 WAN		39
6.2 LAN		40
6.3 NAT		41
6.3.1	Virtual Servers	41
6.3.2	Port Triggering	43
6.3.3	DMZ Host	44
6.3.4	ALG	45
6.4 SECURI	ΓΥ	45
6.4.1	MAC Filtering	45
6.4.2	IP Filtering	47
6.4.3	Parental Control	50
6.5 QUALIT	Y OF SERVICE	51
6.6 ROUTIN	G	54
6.6.1	Default Gateway	54
6.6.2	Static Route	55
6.6.3	RIP	56
6.7 DNS		57
6.7.1	DNS Server	57
6.7.2	Dynamic DNS	57
6.8 DSL		59
6.9 Port M	APPING	50
6.10 Certii	FICATE	52
6.10.1	Local	52
6.10.2	Trusted CA	54
CHAPTER 7	WIRELESS	65
71 RASIC		55
7 2 SECURI	ΓΥ	56
, SLCOR		-0

7.3 MAC	C Filter	74
7.4 Wire	eless Bridge	
7.5 Adva	ANCED	
7.6 QUAI	LITY OF SERVICE	
7.7 Stati	ION INFO	
CHAPTER	R 8 DIAGNOSTICS	
СНАРТЕБ	R 9 MANAGEMENT	
9.1 Setti	INGS	
9.1.1	Backup	
9.1.2	Update Settings	
9.1.3	Restore Default	
9.2 Syst	тем Log	
9.3 SNM	IP AGENT	
9.4 TR-0	069 CLIENT	
9.5 Inter	rnet Time	
9.6 Acce	ESS CONTROL	
9.6.1	Services	
9.6.2	IP Addresses	
9.6.3	Passwords	
9.7 Upda	ATE SOFTWARE	
9.8 SAVE	E AND REBOOT	
APPENDE	X A - SECURITY	
APPENDE	X B - PIN ASSIGNMENTS	
APPENDE	X C - SPECIFICATIONS	
APPENDE	X D - SSH CLIENT	

Chapter 1 Summary

Comtrend's CT-5365 is an 802.11g (54Mbps) Wireless and Wired ADSL2+ Router. It comes equipped with four 10/100 Base-T Ethernet ports and an ADSL2+ port for wired connectivity. An integrated 802.11g WLAN Access Point (AP) with Wi-Fi Protected Setup (WPS) provides wireless coverage.

The CT-5365 contains state of the art security features, such as WPA data encryption, Firewall and VPN pass through. This model supports up to 16 contiguous virtual connections allowing for multiple simultaneous Internet connections. The front and back panels are TR-068 compliant, which means they are color-coded for easy installation and use. These features make the CT-5365 especially suited to a home or small business environment.

1.1 Features

- Dynamic IP assignment
- Up to 16 VCs
- IGMP Proxy
- Per-VC packet level QoS
- MAC address and IP filtering
- UPnP
- RADIUS client
- Embedded SNMP agent
- TR-069/TR-098/TR-111
- Remote administration
- Configuration backup and restoration
- Integrated 802.11g AP

- Auto PVC configuration
- NAT/PAT
- IP QoS & WMM
- Static and RIP v1/v2 Routing
- DNS Proxy
- FTP/TFTP server
- Web-based management
- Firmware upgrade and configuration
- DHCP Server/Relay/Client
- Backward compatible with 802.11b
- Wi-Fi Protected Setup (WPS)
- WPA/WPA2 and 802.1x security
- Optional Turbo mode in wireless (After burner)

1.2 Application

The following diagram depicts the application of the CT-5365 router.



1.3 LED Indicators

The LED indicators are shown below and explained in the table that follows.

Θ	WPS	WLAN	LAN1x	LAN2x	LAN3x	LAN4x	ADSL	ALARMA
							100	
							2.0	

LED	Color	Mode	Function
DOWED	Croon	On	The router is powered up.
FOWER	Green	Off	The router is powered down.
		On	WPS enabled.
WPS	Green	Off	WPS disabled.
		Blink	WPS client pairing in progress.
	Green	On	The wireless module is ready and idle.
WLAN		Off	The wireless module is not ready.
		Blink	Data transmitting or receiving over WLAN.
	Green	On	An Ethernet Link is established.
LAN 1x~4x		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
	Green	On	ADSL link is established.
ADSL		Off	ADSL link is not established.
		Blink	ADSL link is becoming established.
	Pod	On	The ADSL link is not available.
ALARMA	Reu	Off	The ADSL link is available.

Chapter 2 Installation

2.1 Hardware Installation

Follow the instructions below to complete the hardware installation.

BACK PANEL



ADSL PORT - Connect the ADSL line to the ADSL port with RJ11 cable.

LAN PORT

Use RJ45 straight through or crossover MDI/X cable to connect up to four devices.

RESET BUTTON

Restore the default settings of the device by holding down the Reset button until the front panel LED indicators blink simultaneously (\sim 5 seconds). This action may be required if the router fails to respond normally or if the router configuration changes. The router has rebooted successfully when the LED indicators display as expected.

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 indicator lights up (GREEN) then the device is ready for setup.

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

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

FRONT PANEL

(m) WPS

WI-FI BUTTON (1)

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. When WPS is available the WPS LED will be ON.

Chapter 3 Web User Interface

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

3.1 Default Settings

The following are the default settings for the device.

- Local (LAN) access (username: root , password: 12345)
- Remote (WAN) access (username: support, password: support)
- User access (username: user, password: user)
- LAN IP address: 192.168.1.1 Subnet Mask: 255.255.255.0
- WAN IP address: none
- Remote WAN access: disabled (except for ICMP)
- NAT and Firewall: enabled for PPPoE/A, disabled for Bridge/MER/IPoA
- DHCP server on LAN interface: enabled
- Wireless Access enabled
- SSID: Comtrend
- Wireless authentication open (no authentication)

This device supports the following connection types.

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

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, 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 or by clicking the Restore Default Configuration button on the Restore Settings screen of the web user interface.

3.2 IP Configuration

The following instructions describe how to set the IP configuration of the Ethernet connection so that a computer can connect to the CT-5365. Once this connection is established you will be able to access product features or manage the device using the web user interface described herein, or by other methods (e.g. FTP/TFTP).

NOTE: These instructions are written for a computer running Microsoft Windows XP SP2. For other operating systems (e.g. Windows Vista, Linux, etc.), the specific steps may vary but the general procedure is the same. Check the instructions provided with your operating system for further guidance.

DHCP Mode

When the CT-5365 powers up, the DHCP server (on the device) will start automatically. To obtain an IP address automatically, DHCP mode must be activated within the Internet Protocol properties of the Local Area Connection on your computer. To check the current IP configuration, do the following:

- **STEP 1:** From the Network Connections window, open Local Area Connection and click the **Properties** button. You may also access this screen by double-clicking the Local Area Connection icon on your taskbar.
- **STEP 2:** Select Internet Protocol (TCP/IP) and click the **Properties** button again. DHCP mode is activated if the dialog box displays as shown below.

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

STATIC IP Mode

Using static IP configuration, your computer must have an IP address within the same subnet as the CT-5365. Follow the steps below to configure your computer to use the default subnet of **192.168.1**.x.

- **STEP 1:** From the Network Connections window, open Local Area Connection and click the **Properties** button. You may also access this screen by double-clicking the Local Area Connection icon on your taskbar.
- **STEP 2:** Select Internet Protocol (TCP/IP) and click the **Properties** button again.

STEP 3: On the dialog box that appears, select the radio button labeled "Use the following IP address". Enter an IP address in this format {192.168.1.x, where x is any number greater than 2 and less than 254}. Enter the subnet mask as 255.255.255.0. The screen should display as follows.

Internet Protocol (TCP/IP) Propertie	s <u>? x</u>
General	
You can get IP settings assigned autom this capability. Otherwise, you need to a the appropriate IP settings.	natically if your network supports isk your network administrator for
C Obtain an IP address automatical	y I
Use the following IP address:	
IP address:	192.168.1.133
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	· · ·
C Obtain DNS server address autor	natically
☐ ─ • Use the following DNS server add	tresses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

STEP 3: Enter the default gateway and DNS server settings as provided by your ISP or enter **192.168.1.1**, which is the default IP address of the CT-5365. Click **OK** to submit these settings and thereby activate STATIC IP mode.

3.3 Login Procedure

NOTE:

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

The default settings can be found in section 3.1.

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

- **NOTE:** For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Info WAN screen and login with remote username and password.
- **STEP 2:** A dialog box will appear, such as the one shown. Enter the default username and password, as defined in section 3.1 Default Settings. Click **OK** to continue.

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

NOTE: The login password can be changed later (see section 9.6.3)

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

COMPREND O ADSL R	louter
M	Quick Setup
	This Quick Setup will guide you through the steps necessary to configure your DSL Router.
Device Info Quick Setup	ATM PVC Configuration
Advanced Setup	Select the check box below to enable DSL Auto-connect process.
Wireless Diagnostics Management	☑ DSL Auto-connect

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

Chapter 4 Quick Setup

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

4.1 Auto Quick Setup

This function provides an automated process to quickly setup a WAN connection. The device will auto-detect the best PVC profile available, provided that the ADSL link is up. For manual setup, please go to section 4.2.

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



STEP 2: Click Next to start the setup process. Follow the onscreen prompts.

STEP 3: After setup is complete, the device will reboot with the following shown.



NOTE: After the device reboots, the Device Information screen should appear. If the browser does not refresh automatically, close it and restart. You will need to login again. If you encounter difficulty, be sure to check the IP configuration (see section 3.2).

4.2 Manual Quick Setup

To setup the router manually follow these instructions.

STEP 1: Select **Quick Setup** from the main menu and uncheck the **DSL Auto-connect** checkbox ☑ to begin the manual quick setup process.

COMPRESS OF	Router	
Device Info	Quick Setup This Quick Setup will guide you through the steps necessary to configure your DSL Router.	
Quick Setup Advanced Setup Wireless Diagnostics Management	Select the check box below to enable DSL Auto-connect process.	
	Uncheck to begin the manual quick setup	
	process and display the following screen.	
		
Quick Setup		
This Quick Setup will gui	de you through the steps necessary to configure your DSL Router.	
Select the check hox held	II	
DSL Auto-connect	t	
The Virtual Path Identifie VCI numbers unless your	er (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and r ISP instructs you otherwise.	
VCI: [32-65535] 35		
Enabling QoS for a PVC i resources, the number o the applications.	mproves performance for selected classes of applications. However, since QoS also consumes system f PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for	
Enable Quality Of Servic		
	Next	

STEP 2: Adjust the VPI/VCI settings for the connection you wish to establish. Select Enable Quality Of Service if required. Click **Next** to continue.

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

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

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

COMPREND O ADSL	Router
ADSL Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	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 ATM (PPPoA) ^O PPP over Ethernet (PPPOE) ^O MAC Encapsulation Routing (MER) ^O IP over ATM (IPOA) ^O Bridging
	Enable 802.1q VLAN ID[0-4095]: 123 Back Next

Click **Next** to continue...

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

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

STEP 4: Select PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE) and click Next. The following screen appears. Enter the Username and Password and select the connection options you wish. Review the descriptions below for more details. Click Next to continue.

COMPREND CADSL	Router
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	PPP Username and Password PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. PPP Username: PPP Deservoire Name: Authentication Method: AUTO Dial on demand (with idle timeout timer) PPP IP extension Use Static IP Address Enable PPP Debug Mode

PPP Username / PPP Password

The PPP Username and the PPP password requirement are dependent on the particular requirements of the service provider. A maximum of 256 characters is allowed for the PPP user name and a maximum of 32 characters for PPP password.

PPPoE Service Name

For PPPoE service, PADI requests contain a service label. Some PPPoE servers (or BRAS) 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.

PPP IP Extension

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

PPP IP Extension does the following:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.

- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.

Use Static IP Address

Unless your service provider specially requires this setup, do not select the checkbox. If selected, enter the static IP address in the IP Address box. Don't forget to adjust the TCP/IP settings as described in section 3.2.

Enable PPP Debug Mode

More PPP connection information will be listed in the System Log. This is used for debugging. Please don't enable it for normal usage as it uses system resources.

STEP 5: This screen allows the user to control IGMP Multicast and WAN Service.

GOMHREND O	Router	
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Enable IGMP Multicast, and WAN Service Enable IGMP Multicast Enable WAN Service Service Name pppoe_0_35_1	Back Next

Enable IGMP Multicast checkbox:

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

Enable WAN Service checkbox:

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

Service Name: This is the WAN Service label.

GOMTREND C ADSL	Router
1V	Device Setup
	Configure the DSL Router IP Address and Subnet Mask for LAN interface.
Device Info	
Quick Setup	IP Address: 192.168.1.1
Advanced Setup	Subnet Mask: 255.255.255.0
Wireless	
Diagnostics	C Disable DHCP Server
Management	Enable DHCP Server
17	Start IP Address: 192.168.1.2
	End IP Address: 192 168 1 254
	Leased Time (hour): 24
	Configure the second IP Address and Subnet Mask for LAN interface
	Back Next

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.

This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN. Please be aware that the private address range (e.g. 192.168.1.2 \sim 192.168.1.254) does not include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

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

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

STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.

COMPREND O ADSL	Router	
A	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

STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

BOMWREND O ADSL RO	uter		
Device Infe	WAN Setup - Summ Make sure that the set	ary ttings below match the se	ttings provided by your ISP.
Ouick Setup	VPI / VCI:	0 / 35	
Advanced Setup	Connection Type:	PPPoE	
Wireless	Service Name:	pppoe_0_35_1	
Diagnostics	Service Category:	UBR	
Management	IP Address:	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Enabled	
	Firewall:	Enabled	
	IGMP Multicast:	Disabled	
	Quality Of Service:	Disabled	
	Click "Save/Reboot" to NOTE: The configurati	o save these settings and on process takes about 1	reboot router. Click "Back" to make any modifications. minute to complete and your DSL Router will reboot. Back Save/Reboot

STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in section 3.3.

4.2.2 MAC Encapsulation Routing (MER)

Step 4: Select MAC Encapsulation Routing (MER) and enter information provided to you by your ISP to configure the WAN IP settings. Click **Next**.

COMPREND O ADSL R	outer
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	WAN IP Settings Enter information provided to you by your ISP to configure the WAN IP settings. Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional. O Obtain an IP address automatically Image: Static default gateway automatically Image: WAN Subnet Mask: Image: Static default gateway automatically Image: Static default gateway automatically

DHCP is enabled in MER mode when **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 the 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.

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

	Router
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Network Address Translation Settings Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). Enable NAT Enable NAT Enable Firewall Enable IGMP Multicast, and WAN Service Enable IGMP Multicast Enable IGMP Multicast Enable WAN Service Service Name: mer_0_34
	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 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 (Proxy): Tick the checkbox to enable IGMP multicast. IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable WAN service.

Service Name: This is the WAN Service label.

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

GOMTREND O ADSL R	outer
- AN	Device Setup
	Configure the DSL Router IP Address and Subnet Mask for LAN interface.
Device Info	IP Address: 192 168 1 1
Quick Setup	Cubrat Made
Advanced Secup	Subher Mask: 255.255.0
Diagnostics	C Disable DHCP Server
Management	Enable DHCP Server
Management	Start IP Address: 192 168 1 2
	End ID Address: 102.160.1.254
	End IP Address: 192.108.1.254
	Leased Time (hour): 24
	C Enable DHCP Server Relay
	DHCP Server IP Address:
	Configure the second IP Address and Subnet Mask for LAN interface
	IP Address"
	Cubrat Made
	Subhet Mask:
	Back Next

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.

This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN. Please be aware that the private address range (e.g. 192.168.1.2 \sim 192.168.1.254) should not include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (not available if **NAT** enabled), and enter the DHCP Server IP Address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

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

Configure the second I	P Address and Subnet Mas	sk for LAN interface
IP Address:		
Subnet Mask:		

STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.

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

STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

BOMMEND O ADSL RO	outer		
	WAN Setup - Summa Make sure that the set	ary ttings below match the se	ttings provided by your ISP.
Device Info	NDT / NCT.	0.124	1
Quick Setup	VPI / VCI:	0/34	
Advanced Setup	Connection Type:	MER	-
Wireless	Service Name:	mer_0_34	
Diagnostics Management	Service Category:	UBR	
	IP Address:	Automatically Assigned	
	Service State:	Enabled	
	NAT:	Disabled	·
	Firewall:	Disabled	
	IGMP Multicast:	Disabled	•
	Quality Of Service:	Enabled	1
	Click "Save/Reboot" to NOTE: The configurati	o save these settings and on process takes about 1	reboot router. Click "Back" to make any modifications. minute to complete and your DSL Router will reboot. Back Save/Reboot

STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in section 3.3.

4.2.3 IP Over ATM

Step 4: Select IP over ATM (IPoA) and click **Next**. The following screen appears.

COMTREMD C ADSL	Router
- A	WAN IP Settings Enter information provided to you by your ISP to configure the WAN IP settings.
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection. WAN IP Address:

NOTE: Since DHCP is not supported over IPoA, users must manually enter the IP address or WAN interface for the default gateway and the DNS server addresses (primary and secondary), as provided by their ISP.

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

COMPREND O ADSL	Router
w	Network Address Translation Settings
Device Info	Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Quick Setup Advanced Setup	Enable NAT
Wireless Diagnostics	Enable Firewall
Management	Enable IGMP Multicast, and WAN Service
	Enable IGMP Multicast
	Enable WAN Service 🔽
	Service Name: ipoa_0_34
	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 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 (Proxy): Tick the checkbox to enable IGMP multicast. IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers.

Enable WAN Service: Tick the checkbox to enable WAN service.

Service Name: This is the WAN Service label.

Step 6: Click **Next** to display the following screen.

COMPLEXED O	Router
Device Info	Device Setup Configure the DSL Router IP Address and Subnet Mask for LAN interface.
Quick Setup	IP Address: 192.168.1.1
Advanced Setup Wireless	Subnet Mask: 255.255.255.0
Diagnostics	C Disable DHCP Server
Management	 Enable DHCP Server Start IP Address: 192.168.1.2 End IP Address: 192.168.1.254 Leased Time (hour): 24
	 Enable DHCP Server Relay DHCP Server IP Address: Configure the second IP Address and Subnet Mask for LAN interface R Address
	Back Next

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.

This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN. Please be aware that the private address range (e.g. 192.168.1.2 ~ 192.168.1.254) should not include the router's LAN interface IP address (e.g. 192.168.1.1 by default). Also, the Ethernet interface and wireless LAN share the same subnet since they are bridged within the router.

Select **Enable DHCP Server Relay** (not available if **NAT** enabled), and enter the DHCP Server IP Address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

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



STEP 7: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.

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

STEP 8: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

	Router WAN Setup - Summ	arv	
	Make sure that the set	ttings below i	natch the settings provided by your ISP.
Ouick Setup	VPI / VCI:	0 / 35	
Advanced Setup	Connection Type:	IPoA	
Wireless	Service Name:	ipoa_0_35	
Diagnostics	Service Category:	UBR	
Management	IP Address:	1.1.1.1	
	Service State:	Enabled	
	NAT:	Disabled	
	Firewall:	Disabled	
	IGMP Multicast:	Disabled	
	Quality Of Service:	Disabled	
	Click "Save/Reboot" to NOTE: The configurati	o save these s on process ta	ettings and reboot router. Click "Back" to make any modifications. akes about 1 minute to complete and your DSL Router will reboot. Back Save/Reboot

STEP 9: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in section 3.3.

4.2.4 Bridging

Step 4: Select Bridging and click **Next**. To enable bridging service, tick the **Enable Bridge Service** checkbox and enter a **Service Name**.

COMMEREND O	Router	
Device Info Quick Setup Advanced Setup Wireless Diagnostics Management	Unselect the check box below to disab Enable Bridge Service: ☑ Service Name: br_0_33	ble this WAN service

Step 5: Click the **Next** button to continue. On this screen, you may enter the IP address and Subnet Mask for the LAN interface. Click **Next**.

ADSL	Router	
A	Device Setup	
	Configure the DS	SL Router IP Address and Subnet Mask for your Local Area Network (LAN)
)evice Info Juick Setup	IP Address:	192.168.1.1
dvanced Setup	Subnet Mask:	255.255.255.0
Vireless		Pack Noxt
lanagement		DOCK NEXT

NOTE: The LAN IP interface in bridge mode is needed for local users to manage the device. In addition, there is no IP address for the WAN interface and therefore the device cannot be accessed remotely in this mode.

STEP 6: Enable (or disable) Wireless and input an SSID. Click **Next** to proceed.

GOMTREND O ADSL	Router	
A	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

STEP 7: Click **Next** to display the WAN Setup - Summary screen that presents the entire configuration summary. Click **Back** to modify the settings.

COMMEND O ADSL RO	outer		
Device Info	WAN Setup - Summa Make sure that the set	ary tings below mate	th the settings provided by your ISP.
Quick Setup	VPI / VCI:	0 / 33	
Advanced Setup	Connection Type:	Bridge	
Wireless	Service Name:	br_0_33	
Diagnostics	Service Category:	UBR	
Management	IP Address:	Not Applicable	
	Service State:	Enabled	
	NAT:	Disabled	
	Firewall:	Disabled	
	IGMP Multicast:	Not Applicable	
	Quality Of Service:	Enabled	
	Click "Save/Reboot" to NOTE: The configurati	save these setti on process takes	ngs and reboot router. Click "Back" to make any modifications. about 1 minute to complete and your DSL Router will reboot. Back Save/Reboot

STEP 8: Click **Save/Reboot** to apply these settings. The configuration will be saved to flash memory and then the device will reboot. After the device reboots, the Web UI should refresh the browser window. If the browser does not refresh, restart the browser and login again, following the steps in section 3.3.

Chapter 5 Device Information

The web user interface screen is divided into two parts, the main menu (at left) and the display screen (on the right). The main menu has the following options: Device Info, Advanced Setup, Wireless, Diagnostics, and Management. Selecting one of these options will open a submenu with more options.

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

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

COMPREND O ADSL RO	Device Info		
Douico Info	Board ID:		
Summary	Software Version:		
WAN	Bootloader (CFE) Version:		
Statistics	Wireless Driver Version:		
Route	ADSL Version:		
ARP	<u>.</u>		
DHCP	This information reflects the current s	tatus of your D	SL connection.
Quick Setup	Line Pate - Unstream (Khns):	022	
Advanced Setup	Line Kate - Opstream (Kops).	032	
Wireless	Line Rate - Downstream (Kbps):	/616	
Diagnostics	LAN IP Address:	192.168.1.1	
мападетенс	Default Gateway:		
	Primary DNS Server:	192.168.1.1	
	Secondary DNS Server:	192.168.1.1	

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

It provides summary information such as device hardware and software versions, data transmission (line rates) and IP Configuration settings.

5.1 WAN

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

ADSL Ro	uter										
- AN	WAN Info										
Device Info Summary WAN Statistics Route ARP DHCP Quick Setup Advanced Setup Wireless	VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address

The column headings above are described in the table below.

Heading	Description
VPI/VCI	Shows the values of the ATM VPI/VCI
Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
IGMP	Shows the state of the IGMP function
QoS	Shows if IGMP IP QoS is enabled or disabled
State	Shows the connection state of the WAN connection
Status	Lists the status of DSL link
IP Address	Shows IP address for WAN interface

5.2 Statistics

The Statistics submenu provides detailed information for LAN and WAN interfaces.

NOTE: These statistics refresh every 15 seconds.

5.2.1 LAN Statistics

This screen shows statistics for every LAN interface.

COMTREND O ADSL Rou	ter Statistics	LAN							
	Interface		Rece	ived		Т	ransn	nitteo	ł
Device Info		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Summary	Ethernet	20683	175	0	0	149205	248	0	0
WAN	Wireless	0	0	0	0	0	0	10	0
LAN WAN ATM ADSL Route ARP DHCP	Reset St	tatistics							

Heading	Description
Interface	LAN connections
Received/Transmitted - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in bytes Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) packets with errors Rx/TX (receive/transmit) packets dropped

5.2.2 WAN Statistics

This screen shows statistics for interfaces on the WAN.

COMMEND CADSL	Router												
N	Statistics WA	N											
	Service	VPI/VCI P	rotocol	Interf	ace		Rece	eived		Т	rans	mitte	ed
Device Info						Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Summary	pppoe_0_35_1	0/35	PPPoE	ppp_0_	35_1	1373	26	0	0	3096	48	0	0
WAN	br_0_33	0/33	Bridge	nas_0	_33	17448	49	0	0	1330	19	0	4
Statistics													
LAN		1											
WAN	Reset Statistics	S											
ATM													
ADSL													
Route													
ARP													
DHCP													

Heading	Description
Service	WAN service label
VPI/VCI	ATM Virtual Path/Channel Identifiers
Protocol	Connection type (e.g. PPPoE, IPoA, Bridge)
Interface	Connection interfaces are listed in the following format: ppp/nas_(VPI number_VCI number). These interface labels are auto-assigned.
Received/Transmitted - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in bytes Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) packets with errors Rx/TX (receive/transmit) packets dropped

5.2.3 ATM statistics

The following figure shows the ATM statistics screen.

ADSL RO	uter												
M	In	Out	In	In	In Hec	ATM Inter In Invalid Vpi Vci	face Sta In Po Not En	ntistics ort able	In PTI	In Idle	In Circuit Type	IN OAM RM CRC	In GFC
vice Info Summary	0	0	0	0	0	Errors 0	Erro 0	rs	0	Cells 0	Errors 0	Errors 0	0
/AN tatistics						AAL5 Inter	face St	atistics	5				
LAN		In Octet	s Out Oo	ctets In U	cast Pkts	Out Ucast I	kts In	Errors	Out Er	rors Ir	Discards	Out Discards	
WAN		0	0		0	0		0	0		0	0	
ATM ADSL		10				AAL5 VO	C Stati	stics					_
oute		VP		RC Errors	SAR Time	outs Overs	ized SD	Us Sho	ort Pack	et Erro	ors Length	Errors	
RP HCP ck Setup						Rese	t Clos	9					
ck Setup													

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

ATM AAL5 Layer Statistics over ADSL interface

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

ATM AAL5 Layer Statistics for each VCC over ADSL interface

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.
Over Sized SDUs	Number of PDUs discarded because the corresponding SDU was too large
Short Packet Errors	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer
Length Errors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer

5.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen in ADSL2+ mode.

ADSL	Router		
1V	Statistics ADSL		
	Mode:		ADSI 2+
	Line Coding:		Trellis On
evice Info	Status:		No Defect
Summary	Link Power State:		LO
WAN			
Statistics		Downstream	Upstream
LAN	SNR Margin (dB):	6.1	6.0
WAN	Attenuation (dB):	3.0	1.4
ATM	Output Power (dBm):	12.4	17.8
ADSI	Attainable Rate (Kbps):	20884	1
AUSL	Rate (Kbps):	20543	1199
Route	MSGc (number of bytes in overhead channel message	e): 75	11
ARP	B (number of bytes in Mux Data Frame):	254	36
OHCP	M (number of Mux Data Frames in FEC Data Frame):	1	1
lvanced Setup	T (Mux Data Frames over sync bytes):	2	4
ireless	R (number of check bytes in FEC Data Frame):	0	0
agnostics	S (ratio of FEC over PMD Data Frame length):	0.3964	0.9801
anagement	L (number of bits in PMD Data Frame):	5146	302
	D (interleaver depth):	1	1
	Delay (msec):	0	þ
	Super Frames:	28799	28876
	Super Frame Errors:	0	0
	RS Words:	0	0
	RS Correctable Errors:	0	0
	RS Uncorrectable Errors:	0	N/A
	HEC Errors:	0	0
	OCD Errors:	0	0
	LCD Errors:	0	0
	Total Cells:	22446469	0
	Data Cells:	612	0
	Bit Errors:	0	þ
	Total ES:	0	0
	Total SES:	0	0
	Total UAS:	16	0

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

Heading	Description
Mode	T1.413, G.lite, G.DMT, ADSL2/2+ or Re-ADSL
Туре	Channel type Interleave or Fast (not shown in all modes)
Line Coding	Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, Annex L and Annex M
Status	Lists the status of the DSL link
Link Power State	Link output power state.

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

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
В	Number of bytes in Mux Data Frame
М	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
Delay	The delay in milliseconds (msec)

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

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

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

🕙 http://192.168.1.1/berstart.tst?berState=0 - M 🔳	X
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	

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

🐴 http://192.168.1.1/berstop	.tst - Microsoft Inte (
ADSL BER Test - Result	:	~
The ADSL BER test compl	eted successfully.	
Test Time (sec):	20	
Total Transferred Bits:	0x000000000000000000000000000000000000	
Total Error Bits:	0x000000000000000000	
Error Ratio:	Not Applicable	
Clo	se	2
🙆 Done	🔮 Internet	

5.3 Route

Choose Route to display the routes the device has found.

COMPRESS OF	Router						
w	Device Info -	Route					
Device Info	Flags: U - up, ! D - dynamic (re	- reject, G edirect), M -	- gateway, H - h - modified (redire	ost, R ect).	- reinsta	te	
Summary 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	1			1			
ARP							
DHCP							
Quick Setup							
Advanced Setup							
Wireless							
Diagnostics							
Management							

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

5.4 ARP

This screens displays <u>Address Resolution Protocol</u> (ARP) related information.

COMMININD O ADSL R	Device Info	ARP		
	IP address	Flags	HW Address	Device
Summary WAN Statistics Route ARP DHCP	192.168.1.2	Complete	00:05:5D:A0:CD:E9	br0

Heading	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 the DHCP information.

COMPREND O ADSL	Router			
Device Info Summary WAN Statistics Route ARP DHCP	Device Info	DHCP Leases	IP Address	Expires In

Heading	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 advanced setup screens:

6.1 WAN	6.2 LAN
6.3 NAT	6.4 Security
6.5 Quality of Service	6.6 Routing
6.7 DNS	6.8 DSL
6.9 Port Mapping	6.10 Certificate

6.1 WAN

Follow these steps to configure the WAN interfaces.

STEP 1: To **Add** a new WAN connection, click the **Add** button. To edit an existing connection, click the **Edit** button next to the connection. To complete either an Add or **Edit**, go to STEP 2 in section 4.2.

A	Wide Area	Netwo	ork (WAN) s	Setup								
	Choose Add	. Edit. d	or Remove to	configure WAN	interfaces.							
e Info	Choose Sav	e/Rebo	ot to apply th	ne changes and r	eboot the syst	em.						
nced Setup		Con										
	a second s	COII.	Category	Service	Interface	Protocol	Igmp	QoS	VlanId	State	Remove	Edit
N	VPI/VCI	ID	cuccyory									
N I	VPI/VCI	ID	LIBR	nnnne 0 35 1	nnn 0 35 1	PPPoF	Disabled	Enabled	N/A	Enabled	Г	Edit
N I F	0/35	ID 1	UBR	pppoe_0_35_1	ppp_0_35_1	PPPoE	Disabled	Enabled	N/A	Enabled		Edit
N I r urity Ility of Service	0/35 0/33	ID 1 1	UBR	pppoe_0_35_1 br_0_33	ppp_0_35_1 nas_0_33	PPPoE Bridge	Disabled	Enabled Disabled	N/A N/A	Enabled Enabled		Edit Edit
N F rurity Jity of Service rting	0/35 0/33	ID 1	UBR	pppoe_0_35_1 br_0_33	ppp_0_35_1 nas_0_33	PPPoE Bridge	Disabled	Enabled Disabled	N/A N/A	Enabled Enabled		Edit

Heading	Description
VPI/VCI	ATM VPI (0-255) / VCI (32-65535)
Con. ID	WAN connection ID number
Category	ATM service category
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows the connection type
IGMP	Shows enable or disable IGMP proxy
QoS	Shows if IP QoS is enabled or disabled
VlanId	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
State	Shows the connection state of the WAN connection

Heading	Description
Remove	To remove a connection select the radio button in this column and click the Remove button under the table.
Edit	Used to edit connections

6.2 LAN

This screen allows the user to configure the LAN Interface on the device.

COMTREND O	Router
ADSL	Local Area Network (LAN) Setup
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping Certificate Wireless Diagnostics Management	Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective. IP Address: IP2.168.1.1 Subnet Mask: 255.255.255.0 Image: Image



Consult the field descriptions below for more details.

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

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

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

Enable IGMP Snooping: Enable by ticking the checkbox.

- <u>Standard Mode</u>: In standard mode, multicast traffic will flood all bridge ports when no client is subscribed to a multicast group.
- <u>Blocking Mode</u>: In blocking mode, the multicast data traffic will be blocked and not flood all bridge ports when no client is subscribed to a multicast group.
- **DHCP Server:** To enable DHCP, select **Enable DHCP server** and enter starting and ending IP addresses and the leased time. This setting configures the router to automatically assign IP, default gateway

and DNS server addresses to every PC on your LAN.

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

Configure the second IP address by ticking the checkbox shown below.

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

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

Configure the second IP Address and Subnet Mask for LAN interface					
IP Address:					
Subnet Mask:					
		Save	Save/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).

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.

GOMTREND O ADSL R	outer							
Device Info Advanced Setup WAN LAN	NAT Virta Virtual Serve with private port number	ual Servers Setup er allows you to direr IP address on the LA used by the server	ct incoming traffic fi N side. The Interna on the LAN side. A	rom WAN si al port is req maximum 3 Add	de (identified by Pr uired only if the ex 2 entries can be co Remove	rotocol and Externa kternal port needs t nfigured.	l port) to the Inte to be converted to	rnal server) a different
NAT Virtual Servers Port Triggering DMZ Host ALG	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove

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

Device Info Advanced Setup WAN LAN NAT Virtual Servers Portificate Wireless Dist Dist Management	COMPREND O ADSL	Router
Save/Apply	Device Info Advanced Setup WAN LAN NAT Virtual Servers Port Triggering DMZ Host ALG Security Quality of Service Routing DNS DSL Port Mapping Certificate Wireless Diagnostics Management	AT - Vrual Server Back provide name, and enter the server IP address and click "Save/Apply to forward IP ackets for this service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the specified click is the same as a "Actendent of the service to the servic

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

6.3.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by remote parties. Port Triggering dynamically opens the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Trigger 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 of 32 entries can be configured.

COMMEND O	Router										
- A	NAT Port Triggering S	etup									
Device Info Advanced Setup WAN LAN NAT	Some applications require dynamically opens up the 'C party using the 'Triggering application on the LAN side	that specific po Open Ports' in t Ports'. The Rou using the 'Ope	rts in the Ro he firewall v iter allows t n Ports'. A r	outer's fii when an the remo maximun Add	rewall applic ite par n 32 e Re	be opened ation on the ty from the ntries can t move	for acce e LAN ini WAN si oe config	ess by itiates de to e jured.	the remote a TCP/UDP establish ne	parties. Port Tr connection to a w connections l	rigger a remote back to the
Virtual Servers		Application	Tr	iaaer		0	pen		Remove		
Port Triggering		Hama	Duckson	Doub D		Ductored	Doub D				
DMZ Host		Name	Protocol	POPLK	ange	Protocol	POLLK	ange			
ALG				Start	End		Start	End			
Security		2									
Quality of Service											
Routing											
DNS											
DSL											
Port Mapping											
Certificate											
Wireless											
Diagnostics											
Management											

To add a Trigger Port, click the **Add** button. The following screen will display.

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

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

6.3.3 DMZ Host

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

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

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

COMBREND O ADSL	Router
- NV	NAT DMZ Host
Device Info	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.
Advanced Setup WAN	Enter the computer's IP address and click "Apply" to activate the DMZ host.
LAN	Clear the IP address field and click "Apply" to deactivate the DMZ host.
NAT	
Virtual Servers	DMZ Host IP Address:
Port Triggering	
DMZ Host	Save/Apply
ALG	
Security	
Quality of Service	
Routing	
DNS	
DSL	
Port Mapping	
Certificate	

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, enter an UDP port value (default is 5060) and click **Save/Apply**.

COMPREND O ADSL	Router	
M	ALG	
	Select the ALG below.	
Device Info		
Advanced Setup WAN	☑ SIP Enabled	
LAN		Savo/Apply
NAT		Save/Apply
Virtual Servers		
Port Triggering		
DMZ Host		
ALG		

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

6.4 Security

To display this option, the Firewall checkbox must be enabled in at least one PVC shown on the Advanced Setup - WAN screen.

NOTE: For a more technical discussion of this topic, see Appendix A.

6.4.1 MAC Filtering

NOTE: This function is only available when in bridge mode. Other connection modes use IP Filtering (pg. 47) which performs 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 ID. MAC filtering policy and rules can be set by following the procedure below.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the rules specified in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the rules specified in the following table. The default policy is **FORWARDED**. This can be changed by clicking the **Change Policy** button.

COMPREND O ADSL F	Router
w	MAC Filtering Setup
	MAC Filtering Global Policy: FORWARDED
Device Info Advanced Setup WAN LAN NAT Security IP Filtering MAC Filtering Parental Control Quality of Service Routing DNS DSL Port Mapping Certificate Wireless Diagnostics	Change Policy MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. Choose Add or Remove to configure MAC filtering rules. VPI/VCI Protocol Destination MAC Source MAC Frame Direction Remove Add Remove

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen 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.

COMUREND O	Router
	Add MAC Filter
Device Info Advanced Setup	Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.
LAN NAT	Protocol Type:
Security IP Filtering	Source MAC Address:
MAC Filtering Parental Control Quality of Somica	Frame Direction: LAN<=>WAN
Routing DNS	Select All
DSL Port Mapping	✓ br_0_33/nas_0_33
Certificate Wireless Diagnostics	Save/Apply
Management	

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 filter to selected PVCs (bridge mode only). Filter rules are arranged according to PVC, as shown under the VPI/VCI heading on the previous screen.

6.4.2 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead of IP Filtering, MAC Filtering (pg. 45) performs a similar function.

Outgoing IP Filter

The default setting for Outgoing traffic is **ACCEPTED**. Under this condition, all outgoing IP packets that match the filter rules will be **BLOCKED**.

COMTREND O ADSL	Router
Device Info Advanced Setup	Outgoing IP Filtering Setup By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Choose Add or Remove to configure outgoing IP filters.
WAN	Filter Name Protocol Source Address / Mask Source Port Dest. Address / Mask Dest. Port Remove
NAT Security IP Filtering MAC Filtering Parental Control	Add Remove

To add a filtering rule, click the **Add** button. The following screen will display.

COMMEND COMMEND	outer	
- A	Add IP Filter Outgoing The screen allows you to create a filter rule to identif	fy outgoing IP
Device Info Advanced Setup WAN	traffic by specifying a new filter name and at least on All of the specified conditions in this filter rule must b rule to take effect. Click 'Save/Apply' to save and acti	e condition below. e satisfied for the vate the filter.
LAN NAT	Filter Name:	
Security	Protocol:	-
IP Filtering	Source IP address:	
MAC Filtering	Source Subnet Mask:	
Parental Control	Source Port (port or port:port):	
Quality of Service	Destination IP address:	
DNS	Destination 1 duress.	
DSI	Desundtion Subnet Mask:	
Port Mapping	Destination Port (port or port:port):	
Certificate		
Wireless	Save/Apply	
Diagnostics		
Management		
100 - Contra 100 -		

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 port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or range.

Click **Save/Apply** to save and activate the filter.

Incoming IP Filter The default setting for all Incoming traffic is **BLOCKED**. Under this condition, only those incoming IP packets that match the filter rules will be **ACCEPTED**.



To add a filtering rule, click the **Add** button. The following screen will display.

COMTREMD O ADSL	Router
ADSL Device Info Advanced Setup WAN LAN NAT Security IP Filtering Outgoing Incoming MAC Filtering Parental Control Quality of Service Routing DNS DSL Port Mapping Certificate	Add IP Filter Incoming The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'save/Apply' to save and activate the filter. Filter Name:
Wireless Diagnostics Management	Select All pppoe_0_35_1/ppp_0_35_1 Save/Apply

For detailed field descriptions, please reference the previous table.

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

Click **Save/Apply** to save and activate the filter.

6.4.3 Parental Control

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

COMPLETED O ADSL R	Couter Time of Day	Restri	ctions	A r	naxim	um 1(5 ent	ries (can be	config	ured.	
Device Info Advanced Setup WAN LAN NAT Security IP Filtering MAC Filtering Parental Control	Username	MAC	Mon	Tue	Wed Add	Rer	Fri	Sat	Sun	Start	Stop	Remove

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

COMTREND O ADSL R	Router Time of Day Restriction	
Device Info Advanced Setup WAN LAN NAT Security	This page adds time of day re: to the Router. The 'Browser's I MAC address of the LAN device other LAN device, click the "Ot MAC address of the other LAN Windows based PC, go to com	striction to a special LAN device connected MAC Address' automatically displays the e where the browser is running. To restrict her MAC Address" button and enter the device. To find out the MAC address of a mand window and type "ipconfig /all".
IP Filtering MAC Filtering Parental Control Quality of Service Routing DNS DSL	User Name Browser's MAC Address Other MAC Address (xc:xc:xc:xc:xc:xc) Days of the week Click to colort	Mon Tue Wed Thu Fri Sat Sun
Port Mapping Certificate Wireless Diagnostics Management	Start Blocking Time (hh:mm) End Blocking Time (hh:mm)	Save/Apply

See below for instructions. Click **Save/Apply** to apply the settings. **User Name:** A user-defined label for this restriction. **Browser's MAC Address:** MAC address of the PC running the browser. **Other MAC Address:** MAC address of another LAN device. **Days of the Week:** The days the restrictions apply. **Start Blocking Time:** The time the restrictions start. **End Blocking Time:** The time the restrictions end.

6.5 Quality of Service

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

COMTREND O														
ADSL R	louter													
A	Quality	of Servi	e Setup											
	Choose	Add or Rei	nove to c	onfigure net	vork traffic das	ses.								
evice Info				MADI				т	DAFETC CLASS	TEICATION	111.55			
Ivanced Setup				PIAKK			SFT-1 SFT							
LAN	Class	Priorit	y IP Prece	dence Se	Type of W	AN La	n Protocol	Source Addr.	ce So /Mask Po	urce Dest	/Mask	Dest. Port	802.1P	Remov
Security								Federated						
uality of Service														
louting														
ONS .	Differe	ntiated S	ervice C	onfiguratio	n									
ISL Nort Manning		MAR	K				TRAFFIC CL	ASSIFI	CATION RULES	5				
Certificate	Class	Priority	DSCP La Mark P	n Protoc	ol Source	Source	Dest. Addr./Mask	Dest. Port	Source MAC	Destinatio MAC	n 802.1P	Enable/I	Disable	Remov
ireless			Sector S Los	663	- I second second		a second second second	Contrast.	Charles and a second	Addr./ Mas	K			

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

COMPREND CONTREND CONTREND CONTREND	outer	
- Al	Add Network Traffic Class Rule	
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing	The screen creates a traffic class rule to classify the upstream A rule consists of a class name and at least one condition be the rule to take effect. Click 'Save/Apply' to save and activate Traffic Class Name:	n traffic, assign queuing priority and optionally overwrite the IP header TOS byte. How. All of the specified conditions in this classification rule must be satisfied for a the rule. ype Of Service for the class r Mark IP Type Of Service', the correcponding TOS byte in the IP header of the
DNS DSL Port Mapping Certificate	Note: If Differentiated Service Configuration checkb will not be used for classification. IP TOS byte will b	ox is selected, you will only need to assign ATM priority. IP Precedence ie used for DSCP mark.
Wireless Diagnostics	Assign ATM Transmit Priority: Mark IP Precedence:	
Management	Mark IP Type Of Service: Mark 802.1p if 802.1q is enabled on WAN: Specify Traffic Classification Rules Enter the following conditions either for IP level, SE	T-1, or for IEEE 802.1p, SET-2.
	SET-1 Physical LAN Port: Protocol: Source IP Address: Source Subnet Mask UDP/TCP Source Port (port or portport): Destination IP Address: Destination Subnet Mask: UDP/TCP Destination Port (port or portport): SET-2 802.1p Priority:	
		Save/Apply

Field	Description
Traffic Class Name	Enter name for traffic class.
Assign ATM Transmit Priority	Select Low, Medium or High.
Mark IP Precedence	Select between 0-7. The lower the digit

	shows the higher the priority.
Mark IP Type Of Service	Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay
Mark 802.1p if 802.1q is enabled on WAN	Select between 0-7. The lower the digit shows the higher the priority.
SET-1	
Physical LAN Port	Select between eth0, Wireless and Wireless_Guest.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the subnet mask for the source IP address.
Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination Port (port or port:port)	Enter destination port number or port range.
SET-2	
802.1p Priority	Select between 0-7. The lower the digit shows the higher the priority

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

GOMMEND O ADSL	Router
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS	Add Network Traffic Class Rule The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule. Traffic Class Name: Net: Traffic Class Name:
DSL Print Server Port Mapping Certificate Wireless Diagnostics Management	Assign ATM Transmit Priority:
	Source IP Address: Source Subnet Mask: UDP/TCP Source Port (port or port:port): Destination IP Address: Destination Subnet Mask: UDP/TCP Destination Port (port or port:port): Source MAC Address: Source MAC Address: Destination MAC Address: Destination MAC Address: Destination MAC Address: Destination MAC Mask:
	Save/Apply

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

6.6 Routing

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

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

6.6.1 Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is selected, this device will accept the first received default gateway assignment from one of the enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply** button to save it.



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

6.6.2 Static Route

The Static Route screen lists the configured static routes. Click the **Add** or **Remove** buttons to change settings.

COMUREND O ADSL R	outer				
- And	Routing Sta be configured	atic Route I)	e (A maxim	um 32 entri	es can
Device Info Advanced Setup	Destination	Subnet Mask	Gateway	Interface	Remove
WAN LAN NAT		Add	d Remove	•	
Security Quality of Service Routing					
Default Gateway Static Route RIP					

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

COMULIEND O ADSL	Router	
w	Routing Static Route Add	
Device Info Advanced Setup	Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.	
WAN LAN NAT	Destination Network Address: Subnet Mask:	
Security Quality of Service Routing	Use Gateway IP Address	
Default Gateway Static Route RIP	Save/Apply	

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

6.6.3 RIP

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

COMPREND C ADSL	Router		
N	Routing RIP Configuration		
Device Info Advanced Setup WAN LAN NAT	To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected. Global RIP Mode C Disabled C Enabled		
Security	Interface VPI/VCI Version Operation Enabled		
Quality of Service	br0 (LAN) 2 🖌 Active 🔽 🗖		
Routing	ppp_0_35_1 0/35 2 💌 Passive 🕶 🗖		
Default Gateway			
Static Route	Save/Apply		
RIP			

6.7 **DNS**

6.7.1 DNS Server

If the **Enable Automatic Assigned DNS** checkbox is selected, this device will accept the first received DNS assignment from one of the DHCP enabled PVC(s) – (PPPoA, PPPoE, or MER) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.

COMPRESSION OF ADSL	Router
N	DNS Server Configuration
Device Info Advanced Setup WAN LAN NAT Security Quality of Service	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.
Routing DNS DNS Server Dynamic DNS DSL Port Mapping Certificate	Primary DNS server: Secondary DNS server: Save

NOTE: Click the **Save** button to save the new configuration. Remember, the device must be rebooted to make the new configuration effective.

6.7.2 Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of many domains, allowing the CT-5365 to be more easily accessed from various locations on the Internet.

GOMHRENDO	Route	,				
N	Dyna	mic DNS				
Device Info Advanced Setup WAN LAN	The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet. Choose Add or Remove to configure Dynamic DNS.					
NAT		Hostname	Username	Service	Interface	Remove
Security Quality of Service Routing DNS DNS Server Dynamic DNS			Add	Remove	e	

To add a dynamic DNS service, click the **Add** button and this screen will display.

COMMEREND O	Router	
A	Add dynamic DDNS	
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DNS Server Dynamic DNS DSL Port Mapping Certificate Wireless Diagnostics Management	This page allows you to D-DNS provider Hostname Interface DynDNS Settings Username Password	add a Dynamic DNS address from DynDNS.org or TZO. DynDNS.org pppoe_0_35_1/ppp_0_35_1 Save/Apply

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

6.8 DSL

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

GOMTREND	
ADSL	Router
N	DSL Settings
	Select the modulation below.
Device Info	G.Dmt Enabled
Advanced Setup WAN	G.lite Enabled
LAN	▼ T1.413 Enabled
NAT	ADSL2 Enabled
Security	AnnexL Enabled
Routing	ADSI 2+ Enabled
DNS	
DSL	AnnexM Enabled
Port Mapping	Select the phone line pair below.
Certificate	 Inner pair
Diagnostics	C Outer pair
Management	
	Capability
	Bitswap Enable
	SRA Enable
	Apply

Modulation	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	

Modulation	Data Transmission Rate	- Mbit/s (Megabits per second)
ADSL2+	Downstream: 24 Mbit/s	Upstream: 1.0 Mbit/s
AnnexM	Downstream: 24 Mbit/s	Upstream: 3.5 Mbit/s

Options	Description
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)

6.9 Port Mapping

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group. As shown below, when you tick the **Enable virtual ports on**, the LAN interfaces (eth0) in the default group will separate.

GOMTREND O	11				
ADSL KO	Juter				
- AN	Port Mapping	A maximum 16 entries can be configured			
Device Info Advanced Setup WAN LAN NAT	ice Info Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To supp ranced Setup The move the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface. AN Enable virtual ports on AT Enable virtual ports on) as an independent network. To support ising the Add button. The Remove button default group has IP interface.	
Security	Group Name	Interfaces	Remove	Edit	
Routing	Default	eth0, Wireless, Wireless_Guest			
DNS	Add Romo	- 1			
DSL Doub Mapping	Add	le			
Certificate					
	↓ uter				
Device Info	Port Mapping	A maximum 16 entries can be configured pports multiple ports to PVC and bridging groups, must create mapping groups with appropriate Li	Each grou	p will perform N interfaces u	as an independent network. To support sing the Add button. The Remove button
Advanced Setup WAN LAN NAT	Enable virtu	all ports on etho	Peradit gr	oup. Only the	oerduit group nas ir internate.
Security	Group Name	Interfaces		Remove	Edit
DNS	Default	eth0.1, eth0.2, eth0.3, eth0.4, Wireless, Wireless	_Guest		
DSL Port Mapping Certificate	Add Remove				

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

CONVERIDO ADSL RC	uter
ADSL Re Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping Certificate Wireless Diagnostics Management	Port Mapping Configuration To create a new mapping group: 1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique. 2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. Note that these clients may obtain public IP addresses 3. Click Save/Apply button to make the changes effective immediately Note that the selected interfaces will be removed from their existing groups and added to the new group. IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. Grouped Available Interfaces Interfaces eth0.2 eth0.2
	Automatically Add Clients With the following DHCP Vendor IDs

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

Automatically Add Clients With the Following DHCP Vendor IDs:

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

There are four PVCs (0/33, 0/36, 0/37, and 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video). The LAN interfaces are eth0.1, eth0.2, eth0.3, eth0.4 and Wireless. Port mapping configuration is:

- 1. Default: eth0.1, eth0.2, eth0.3, eth0.4, Wireless, and Wireless_Guest.
- 2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

The CPE's DHCP server is now running on "Default". In addition, ISP's DHCP server is running on PVC 0/36. It is for setup-box use only.

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

If the setup-box was connected with interface "eth0.1" and sent a DHCP request with vendor id "Video", CPE's DHCP server will forward this request to ISP's DHCP server; and CPE will change the port-mapping configuration automatically. The port-mapping configuration will become:

- 1. Default: eth0.2, eth0.3, eth0.4, Wireless, and Wireless_Guest.
- 2. Video: nas_0_36, nas_0_37, nas_0_38, and eth0.1.

6.10 Certificate

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

6.10.1 Local

GOMMEND O ADSL	Router
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping Certificate	Local Certificates Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored. Name In Use Subject Type Action Create Certificate Request Import Certificate
Local Trusted CA	

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 for information about when they need.

COMPRESSION OF ADSL	Router
A	Create new certificate request
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping Certificate Local Trusted CA	To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate. Certificate Name: Common Name: State/Province Name: Country/Region Name: US (United States) Apply

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

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

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name of 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.

COMMEND O	toùter		
- w	Import certificate		
Device Info	Enter certificate name,	paste certificate content and private key.	
Advanced Setup WAN	Certificate Name:	BEGIN CERTIFICATE <inset certificate="" here=""></inset>	*
NAT Security Quality of Service Routing		END CERTIFICATE	
DNS DSL Port Mapping Certificate Local Trusted CA Wireless	Certificate:		
Diagnostics Management		BEGIN RSA PRIVATE KEY <insert here="" key="" private=""> END RBA PRIVATE KEY</insert>	×
	Private Key:		Ŧ
		Apply	

6.10.2 Trusted CA

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

COMPRESSION OF ADSL	Router
w	Trusted CA (Certificate Authority) Certificates
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping Certificate Local	Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored. Name Subject Type Action Import Certificate

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

COMPRESS COM	Router		
Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DHS DSL Port Mapping Certificate Local Trusted CA Wireless Diagnostics Management	Import CA cer Enter certificate Certificate Name:	rtificate e name and paste certificate content. BEGIN CERTIFICATE <insert certificate="" here="">END CERTIFICATE</insert>	4
		Apply	

Chapter 7 Wireless

The Wireless submenu provides access to WLAN configuration settings including wireless network name, channel restrictions (based on country), security, and quality of services features, access point or bridging behavior and station info.

7.1 Basic

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

COMPRESS OF ADSL	Router
N	Wireless Basic
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service Station Info	This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options. Enable Wireless Hide Access Point SSID: Comtrend BSSID: 00:1D:20:20:77:5D Country: [UNITED STATES
Diagnostics Management	
g	Enable Wireless Guest Network
	Guest SSID: Guest Save/Apply

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

Field	Description
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, BSSID and Country settings.
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.
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.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.

Field	Description
Country	 A drop-down menu that permits worldwide and specific national settings. Each country listed below enforces specific regulations limiting channel range: US= worldwide Japan=1-14 Jordan= 10-13 Israel= 1-13
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

7.2 Security

WIRELESS SECURITY

The wireless security screen (shown below) allows for configuration of wireless security settings according to WiFi Simple Configuration (WSC) or Manual Setup AP methods. The WSC method automatically configures security settings using Wi-Fi Protected Setup (WPS). In comparison, the Manual method requires the user to select and enter all these settings for every device on the network.

COMPRESS OF ADSL	Router	
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service Station Info Diagnostics Management	Wireless Security This page allows you to configure You may choose either Wiff Sim WSC Setup AP Configure all security settings of This will overwrite existing setting Setup AP: Manual Setup AP Mageoff yn eenrybton stre Click "Save/Apply" when done. Select SSID: Network Authentication: WEP Encryption:	are security features of the wireless LAN interface. pie Configuration (WSC) or manual configuration. with an external registar. ings. C Push-Button PIN Configure Help ntication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network negth. Comtrend T Open Disabled T Save/Apply

Manual Setup AP settings are described in the table below.

Select SSID

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. 802.11 protocols support two types of network authentication services: open system and shared key.

Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

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.

Select SSID:	Comtrend -
Network Authentication:	802.1×
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled 💌
Encryption Strength:	128-bit 💌
Current Network Key:	2 💌
Network Key 1:	
Network Key 2:	
Network Key 3:	
Network Key 4:	
	Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption key Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
	Save/Annly

The settings for WPA authentication are shown below.

Network Authentication:		-
Network Addicitication.	1 11 1	
WPA Group Rekey Interval:	0	
RADIUS Server IP Address:	0.0.0.0	
RADIUS Port:	1812	
RADIUS Key:		
WPA Encryption:		
WEP Encryption:	Disabled 💌	
		Save/Apply
		Save/Apply

The settings for WPA-PSK authentication	n are shown below.
---	--------------------

Select SSID:	Comtrend -	
Network Authentication:	WPA-PSK	
WPA Pre-Shared Key: WPA Group Rekey Interval: WPA Encryption: WEP Encryption:	0 TKIP	<u>Click here to display</u>
		Save/Apply

WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

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. FYI: Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

WPS

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. This router has both a WPS button on the front panel and a virtual button accessed from the web user interface (WUI).

Devices with the WPS logo (shown here) support WPS. However, the WPS logo might not be present on your device. In this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



NOTE: WPS is only available in WPA-PSK, WPA2-PSK or 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 procedure below. <u>You must</u> choose either the Push-Button or PIN configuration method for Steps 4 and 5.

I. SELECT NETWORK AUTHENTICATION MODE

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 example below shows WPA2-PSK mode.

Manual Setup AP	
You can set the network auth specify whether a network ke network and specify the encry Click "Save/Apply" when done	entication method, selecting data encryption, y is required to authenticate to this wireless yption strength. e.
Select SSID:	Comtrend -
Network Authentication:	WPA2 -PSK
WPA Pre-Shared Key:	•••••
WPA Group Rekey Interval:	
WPA Encryption:	AES 1 & 2
WEP Encryption:	Disabled 🔽
	Save/Apply

Step 2: Enter a WPA Pre-Shared Key and click the **Save/Apply** button. You will see the following dialog box if the Key is too short or too long.



Step 3: The WSC Add Client section should now appear, as shown below.

WSC Add Client		
This feature is available only	when WPA PSK or WPA2 P	SK is configured.
Add a client:	C Push-Button © PIN	Add Click here to display

IIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the front 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 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 4: 1st method: WPS button

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

2nd method: WUI virtual button

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

WSC Add Client	
This feature is available only w	hen WPA PSK or WPA2 PSK is configured.
Add a client:	⊙ Push-Button ○ PIN Add

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

WL5364 11n US	8 Dongle Utilit	ty							
Profile I	Letwork	Advanced	Statistics		Ø WPS				()
			۱	WPS AP List					
ID :		12345678901	123456	00-19-1	5-32-F9-16	11	0	Rescan	
ID : 0×000	4	Comtrend 53	65	00-19-1	5-32-E9-07	11	•	Information	
							U	Pin Code	1
								00021838	
			WPS Profile Lis	t				Config Mode	
								Enrollee 🔻	
								Deteil	
								Decali	1
								Connect	1
								Rotate	
								Disconnect	
<u>P</u> IN	🖸 🛛	PS Associate IE		Pro	gress >> 25%			Delete	
PBC	W	PS Probe IE	PBC - Sending	gEAPOL-Start					
Status	>> Comtrend 5	365 <> 00-19-15	-32-F9-07			Link Qualit	y >> 10()%	
Extra Info >> Link is Up [TxPower:100%]					Signal Streng	th 1 >> 1	100%		
Channel >> 11 <> 2462 MHz					Signal Streng	th 2 >> 1	100%		
Authentication	>> WPA2-PSK					Noise Stren	gth >> 2	6%	
Encryption	>> AES								
Network Type	>> Infrastructi	ure			Transmit			U.S.Y.	-
IP Address >> 0.0.0.0		Link Speed >> 24.0 Mbps		MdX					
Default Gateway	>> 0.0.0.0				Throughput	>> 0.000 Kbps		493.472	
,	НТ	·			Deserves			Kbps	
BW(>> p/a		SMD0 v	x D/a		Link Speed	>> 1.0 Mbps		Max	
GI >> n/a	MCS >> n.	/a SNR1>	»> n/a		Throughput	>> 221.472 Kbj	ps	95.197	

You can now proceed to Step 6 to check your connection.
IIb. WPS – PIN CONFIGURATION

Using this method, a client is configured by the router AP using a personal identification number (PIN). The PIN can be found on the device itself or within the client software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check 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 4:** Select the PIN radio button in the WSC Add Client section of the Wireless Security screen. Enter the client PIN in the box provided and click Add.

WSC Add Client		
This feature is available only	when WPA PSK or WPA2 P	SK is configured.
Add a client:	○ Push-Button ⊙ PIN	Add Click here to display

Step 4: 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.

WL5364 11n	USB Dongle Uti	lity								×
Profile	Left Network	کی Advanced	Statistics	www.	Ø WPS				?	P WiPi 11u
				WPS AP List					_	
ID :		CT5365 TEST		00-19-1	5-32-F9-16	11	0	Rescan		
ID : 0;	:0004	Comtrend 53	55	00-19-1!	5-32-F9-07	11		Information Pin Code 00021838		
			WPS Profile L	ist				Config Mode		
								Enrollee]	
								Detail		
								Connect		
								Rotate		
								Disconnect		
P	IN 💽	WPS Associate IE		Prog	gress >> 15%			Delete		
PĮ	<u>3</u> C	WPS Probe IE	PIN - Begin	associating to WP	S AP					

You can now proceed to Step 6 to check your connection.

III. CHECK CONNECTION

Step 6: 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 example below shows that the connection established successfully.

WIT WL	5364 11n USB D	ongle Utilit	¥ .							×
Pr	ofile Ne	twork	Advanced	Statistics	www.	Ø WPS				P Wiri 11u
				۱	MPS AP List					
	ID : 0x0004		Comtrend 53	55	00-19-15	-32-F9-07	11	Rescan	on 9	
				WPS Profile Lis	t			Config Mode	•	
	Comtrend 53	5	00-	19-15-32-F9-07	Q			Enrollee Detail Connec Rotate Disconne	t ct	
	<u>P</u> IN	🖉 🗹 W	PS Associate IE		Progr	ess >> 100%		Delete		
	PBC	v	PS Probe IE	WPS status is	s connected succe	essfully - Comtren	id 5363			

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.

⁽⁽ † ⁾⁾ Wireless Network	Connection	5 Status	? ×
General Support			
Connection			
Status:		C	Connected
Network:		Comt	rend 5365
Duration:			00:06:14
Speed:		!	54.0 Mbps
Signal Strength:			atili
Activity			
	Sent —		Received
Packets:	121		71
	Disable	<u>V</u> iew Wireless t	Networks
			<u>C</u> lose

7.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. Every network device has a unique 48-bit MAC address. When MAC address filtering is enabled, it restricts the devices that can connect to your access point.

To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the table below and click the **Remove** button.

COMTREND CONTREND CONTRENTCO CONTREND C	outer
- AN	Wireless MAC Filter
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service Station Info	MAC Restrict Mode: Disabled C Allow C Deny MAC Address Remove Add Remove

Option	Description
MAC Restrict Mode	Off – Disables MAC filtering 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. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.

Enter the MAC address on the screen below and click **Save/Apply**.

COMTRAND CADSL	Router
- A	Wireless MAC Filter
Device Info	Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.
Advanced Setup Wireless	MAC Address:
Basic Security MAC Filter	Save/Apply

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.

COMMEND O ADSL	Router
AV	Wireless Bridge
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service	This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.
Station Info	
Diagnostics	Bridge Restrict: Enabled
Management	Remote Bridges MAC Address: Refresh Save/Apply

AP Mode	Description
Access Point	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.
Bridge Restrict	Selecting Disabled in Bridge Restrict 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 Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

7.5 Advanced

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

COMMEREND O	Router	
Device Info Advanced Setup Wireless Basic Security MAC filter Wireless Bridge Advanced Quality of Service Station Info Diagnostics Management	Wireless Advanced This page allows you to configu operate, force the transmission interval for clients in power-sau preambles are used. Click "Apply" to configure the a AP Isolation: Band: Channel: Auto Channel Timer(min) 54g" Rate: Multicast Rate: Basic Rate: Fragmentation Threshold: RTS Threshold: DTIM Interval: Beacon Interval: Beacon Interval: Maximum Associated Clients: XPress" Technology: 54g" Mode: 54g" Mode: 54g" Protection: Preamble Type: Transmit Power:	ure advanced features of the wireless LAN interface. You can select a particular channel on which to n rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup we mode, set the beacon interval for the access point, set XPress mode and set whether short or long dvanced wireless options. Off 24GHz 11 1062731266 Auto 2346 2347 1 100 128 Disabled 54g Auto Auto Save/Apply

Click **Save/Apply** to set new advanced wireless options.

Field	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point can be linked.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices

Field	Description
	can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. 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	Allows selection of a specific channel (1-11) or Auto mode. Current channel shown to the right.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable).
54g Rate	Specifies a data transmission rate. In Auto mode (default) it uses the maximum rate if possible but drops to lower rates when necessary. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.
Multicast Rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Setting 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 split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented.
	Values between 256 and 2346 can be entered. The value should remain at its default setting of 2346, if possible, since setting the Fragmentation Threshold too low may result in poor performance. If you experience a high packet error rate, try to slightly increase the Fragmentation Threshold.
RTS Threshold	Request to Send, 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. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold altogether.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon 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.
Beacon 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. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

Field	Description
Maximum Associated Clients	The maximum number of clients allowed to connect to the router.
Xpress [™] Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards. Default is disabled .
54g [™] Mode	Select Auto mode for greatest compatibility. Select Performance mode for the fastest performance among 54g certified equipment. Select LRS mode if you are experiencing difficulty with legacy 802.11b equipment. If this does not work, you may also try 802.11b only mode.
54g Protection	In Auto mode, the router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turning protection Off will maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for applications where maximum throughput is desired but it does not work with legacy equipment. Long preamble works with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	Set the power output (by percentage) as desired.

7.6 Quality of Service

WMM provides advanced quality of service (QoS) features for Wi-Fi networks to improve the end-user experience by prioritizing audio, video and voice traffic and optimizing the way shared network resources are allocated among competing applications. To enable WMM, select **Enabled** in the WMM (Wi-Fi Multimedia) drop down list box. The screen will display as shown below.

GOMMEND O	louter
- A	WMM(Wi-Fi Multimedia) Settings
Device Info Advanced Setup	WMM(Wi-Fi Multimedia): Enabled WMM No Acknowledgement: Disabled
Wireless Basic Security	Default Wireless QoS Classification: DSCP Network traffic class is automatically assigned according to DSCP in TCP/IP header.
Wireless Bridge Advanced	Extended Wireless QoS Classification: Choose Add or Remove to configure network traffic classes.
Station Info Diagnostics	Class Name Priority TRAFFIC CLASSIFICATION RULES Protocol Source Addr./Mask Source Port Dest. Addr./Mask Dest. Port
Management	Add QoS Entry Save/Apply WME Settings

Field	Description
WMM (Wi-Fi Multimedia)	This technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It ensures that multimedia services get higher priority.

Field	Description
WMM No	Refers to the acknowledge policy used at the MAC level. Enabling
Acknowledge	no Acknowledgement can result in more efficient throughput but
ment	higher error rates in a noisy Radio Frequency (RF) environment.

To add an **Extended Wireless QoS Classification**, click **Add QoS Entry**. The following screen will display.

COMBREND O ADSL	Router
ADSL Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service Station Info Diagnostics Management	Add/Edit Wireless Quality of Service Rule Add/Edit Wireless Quality of Service Rule The screen controls a wireless traffic QoS rule. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule. Traffic Class Name: Assign Wireless Priority Wireless Transmit Priority: O • WMM Best Effort (default) • Specify Traffic Classification Rules Protocol: Source IP Address: Source Subnet Mask:
	UDP/TCP Source Port (port or port:port): Destination IP Address: Destination Subnet Mask: UDP/TCP Destination Port (port or port:port): Save/Apply

Enter a **Traffic Class Name** and assign the **Wireless Transmit Priority** from the drop-down list box. **Specify Traffic Classification Rules** by choosing the desired parameters under this heading. Click **Save/Apply** to add the Wireless QoS rule.

When finished adding rules, click **Save/Apply WME Settings** on the main screen.

7.7 Station Info

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

COMPREND O ADSL R	outer
- A	Wireless Authenticated Stations
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Quality of Service Station Info Diagnostics Management	This page shows authenticated wireless stations and their status. BSSID Associated Authorized Refresh

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

Chapter 8 Diagnostics

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

COMMEND O ADSL	Router		
Powice Infe	br_0_33 Diagnostics Your modem is capable of testing your DSL	. connectio	tion. The individual tests are listed below. If a test displays a fail status, click
Advanced Setup Wireless	and follow the troubleshooting procedures.	work	I to make some the rail status is consistent, a the test continues to rail, they may
Management	Test your ENET(1-4) Connection:	PASS	S Help
	Test your Wireless Connection:	PASS	S Help
	Test the connection to your DSL servi Test ADSL Synchronization:	ce provid	rider S <u>Help</u>
	Test ATM OAM F5 segment ping:	PASS	S Help
	Test ATM OAM F5 end-to-end ping:	PASS	S Help
		Tes	Previous Connection Test With OAM F4

The figure above shows the Diagnostics screen in bridge mode.

COMPREND O	outer		
Device Info Advanced Setup Wireless Diagnostics Management	pppoe_0_35_1 Diagnostics Your modem is capable of testing your DSI "Rerun Diagnostic Tests" at the bottom of and follow the troubleshooting procedures Test the connection to your local net Test your ENET(1-4) Connection: Test your Wireless Connection:	work PASS PASS	on. The individual tests are listed below. If a test displays a fail status, click o make sure the fail status is consistent. If the test continues to fail, click "Help" Help Help
	Test the connection to your DSL serv Test ADSL Synchronization: Test ATM 0AM F5 segment ping: Test ATM 0AM F5 end-to-end ping:	PASS PASS PASS	ter Help Help
	Test the connection to your Internet Test PPP server connection: Test authentication with ISP: Test the assigned IP address:	service pr PASS PASS PASS	rovider Help Help Help
	Ping default gateway: Ping primary Domain Name Server:	PASS PASS Tes	Help Help Next Connection st Test With OAM F4

The figure above shows the Diagnostics screen in PPPoE mode.

Consult the table below for field descriptions.

Test	Condition
ENET Connection	Pass: Indicates that the Ethernet interface on your computer is connected to the LAN port of this device. Fail: Indicates that the device does not detect the Ethernet interface on your computer.
Wireless connection	Pass: Indicates the wireless card on the device is ON. Down: Indicates that the wireless card is OFF.
ADSL Synchronization	Pass: Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid ADSL LED on the device also indicates the detection of a DSL signal from the telephone company Fail: Indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The ADSL LED will turn off.
Ping Default Gateway	Pass: Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router.Fail: Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the device can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore, if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

NOTE: This table describes the basic test set (i.e. no PVC configured). For help with other tests click on the <u>Help</u> link next to each test condition.

Chapter 9 Management

The Management menu has the following maintenance functions and processes:

9.1 Settings	9.2 System Log
9.3 SNMP Agent	9.4 TR-069 Client
9.5 Internet Time	9.6 Access Control
9.7 Update Software	9.8 Save and Reboot

9.1 Settings

The Settings screen allows for the backup, retrieval, and restoration of settings.

9.1.1 Backup

Select **Backup** from the **Settings** submenu to access the screen shown below. Click the **Backup Settings** button to save the current configuration settings. You will be prompted to define the location of a backup file to save to your PC.

COMPRESS OF ADSL	Router
M	Settings - Backup
Dovico Info	Backup DSL router configurations. You may save your router configurations to a file on your PC.
Advanced Setun	
Wireless	Backup Settings
Diagnostics	
Management	
Settings	
Backup	
Update	
Restore Default	
System Log	
Internet Time	
Access Control	
Update Software	
Save/Reboot	

9.1.2 Update Settings

Select **Update** from the **Settings** submenu to access the screen shown below. Enter a previously saved configuration backup file in the **Settings File Name** field and click the **Update Settings** button to load it. If you forget the filename and path, you can search your PC by clicking on the **Browse** button.

COMPREND O ADSL	Router
Device Info Advanced Setup Wireless Diagnostics Management Settings Backup Update Restore Default System Log SIMP Agent Internet Time Access Control Update Software	Tools Update Settings Update DSL router settings. You may update your router settings using your saved files. Settings File Name: Browse Update Settings
Save/Reboot	

9.1.3 Restore Default

Select **Restore Default** from the **Settings** submenu to access the screen shown below. Click the **Restore Default Settings** button to restore the device to the <u>default firmware settings</u>. Restoring system settings require a device reboot.

COMTREND		
ADSL R	outer	
and a	Tools Restore Default Settings	
	Pactora DSL router settings to the factory def	aulto
Device Info	Restore DSL router settings to the ractory den	auits.
Advanced Setup		
Wireless		Restore Default Settings
Diagnostics		
Management		
Settings		
Backup		
Update		
Restore Default		
System Log		
SNMP Agent		
Internet Time		
Access Control		
Update Software		
Save/Reboot		

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

After the Restore Default Configuration button is selected, the following screen appears. Close the device Configuration window and wait for 2 minutes before reopening the browser. If necessary, reconfigure your PC IP address to match your new configuration (see section 3.2 for details).

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

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

9.2 System Log

The **System Log** option under **Management** allows for the viewing of system events and configuration of related options. The default setting for the System Log is enabled. Follow the steps below to enable and view the System Log.

	STEP 1:	Click Configure	System	Log to	begin.
--	---------	-----------------	--------	--------	--------

COMPREND O	outer
Device Info Advanced Setup Wireless Diagnostics Management Settings	System Log The System Log dialog allows you to view the System Log and configure the System Log options. Click "View System Log" to view the System Log. Click "Configure System Log" to configure the System Log options. View System Log Configure System Log
System Log SNMP Agent Internet Time Access Control Update Software Save/Reboot	

Step 2: Select the system log options (see table below) and click Save/Apply.

NOTE: The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

COMPREND O ADSL	Router
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log SIMP Agent Internet Time Access Control Update Software Save/Reboot	System Log Configuration If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Local' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory. Select the desired values and click 'Save/Apply' to configure the system log options. Log:
	Save/Apply

Field	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled.
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. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging" which is the lowest critical level. The log levels are defined as follows:
	 Emergency = system is unusable Alert = action must be taken immediately Critical = critical conditions Error = Error conditions Warning = normal but significant condition Notice= normal but insignificant condition Informational= provides information for reference Debugging = debug-level messages
	Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both modes are configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

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.
			Refiresh 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 the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.

	Router	
N	SNMP - Configurat	äon
	Simple Network Man	nagement Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP
Device Info	agent in this device.	
Advanced Setup	Select the desired va	alues and click "Apply" to configure the SNMP options.
Wireless		
Diagnostics	SNMP Agent C Dis	sable 💿 Enable
Management		
Settings	Read Community:	public
System Log	Set Community:	private
SNMP Agent	System Name:	Comtrend
TR-069 Client	System Location:	unknown
Internet Time	System Eocadon.	
Access Control	System Contact:	unknown
Update Software	Trap Manager IP:	0.0.0.0
Save/Reboot		
		Save/Apply

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 router.

GOMBREND O ADSL	Router	
SI	TR-069 client - Configuration	
Device Info	WAN Management Protocol (TR-0 and diagnostics to this device.	69) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection,
Advanced Setup Wireless	Select the desired values and clic	k "Apply" to configure the TR-069 client options.
Diagnostics Management	Inform ⓒ Disable 〇 Enabl	le
Settings	Inform Interval:	300
SNMP Agent	ACS URL: ACS User Name:	admin
TR-069 Client Internet Time	ACS Password:	0000
Access Control Update Software	Connection Request User Name: Connection Request Password:	
Save/Reboot		Save/Apply GetRPCMethods

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

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet timeservers, tick the corresponding box displayed on this screen shown below.

COMTREMD O ADSL	louter
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log SIMP Agent Internet Time Access Control	Time settings This page allows you to the modem's time configuration. Image: Automatically synchronize with Internet time servers First NTP time server: clock.fmt.he.net Second NTP time server: None Time zone offset: (GMT-12:00) International Date Line West Save/Apply
Update Software Save/Reboot	

First NTP timeserver:Select the required server.Second NTP timeserver:Select second timeserver, if required.Time zone offset:Select the local time zone.

Configure these options and then click **Save/Apply** to activate.

NOTE: Internet Time must be activated to use Parental Control (page 50). In addition, this menu item is not displayed when in bridge mode since the router would not be able to connect to the NTP timeserver.

9.6 Access Control

The Access Control option under the Management menu bar configures access related parameters in three areas: Services, IP Addresses, and Passwords. Use Access Control to control local and remote management settings for the device.

9.6.1 Services

The Services option limits or opens the access services over the LAN or WAN. These access services are available: FTP, HTTP, ICMP, SNMP, SSH, TELNET and TFTP. Enable a service by ticking its checkbox. Click **Save/Apply** to activate.

COMTREND					
ADSL R	outer				
	Access Control	Services			
Device Info	A Service Control Lis	t ("SCL") enables or disabl	les services	from being u	sed.
Advanced Setun					
Wireless					
Diagnostics			Services	LAN	WAN
Management			FTP	🗖 Enable	🗖 Enable
Settings			HTTP	Enable	Enable
System Log			TOMP	Enablo	. Enable
SNMP Agent			ICIMP	Elidble	I Enable
Internet Time			SNMP	Enable	🗖 Enable
Access Control			SSH	🗹 Enable	🗖 Enable
Services			TELNET	Enable	Enable
IP Addresses			TETO		
Passwords			TELE	L Enable	L Enable
update Software					-

NOTE: The WAN column is present if the WAN interface is active. Only the LAN side will be displayed if the WAN interface is down.

Appendix D contains a quick introduction to SSH clients.

9.6.2 IP Addresses

The IP Addresses option limits local access by IP address. When the **Access Control Mode** is enabled, only the IP addresses listed here can access the device. Before enabling **Access Control Mode**, add IP addresses with the **Add** button.

COMPREND CO ADSL R	outer
- A	Access Control IP Address
Device Info Advanced Setup	The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Wireless Diagnostics Management	Access Control Mode: O Disable C Enable
Settings System Log	IP Address Remove
TR-069 Client Internet Time	Add Remove
Access Control Services IP Addresses	
Passwords Update Software Save/Reboot	

On this screen, enter the IP address, subnet mask, and interface to which you wish to give management permissions. Click **Save/Apply** to continue.

COMPREND O ADSL	Router
- A	Access Control
Device Info	
Advanced Setun	IP Address:
Wireless	
Diagnostics	Save/Apply
Management	
Settings	
System Log	
SNMD Agent	
TR-060 Client	
Internet Time	
Access Control	
Services	
TP Addresses	
Passwords	
Update Software	
Save/Reboot	

9.6.3 Passwords

The Passwords option configures the user account access passwords for the device. Access to the device is limited to the following three user accounts:

- **root** is to be used for local unrestricted access control.
- **support** is to be used for remote maintenance of the device
- **user** is to be used to view information and update device firmware.

NOTE: Passwords for these three user accounts can be found in section 3.1.

Use the fields in the screen below to select a username and change its password. Passwords must be 16 characters or less. Click **Save/Apply** to continue.

GOMUREND O ADSL 1	Router		
- A	Access Control Passwords		
	Access to your DSL router is controlled through three user accounts: root, support, and user.		
Device Info			
Advanced Setup	The user name "root" has unrestricted access to change and view configuration of your DSL Router.		
Wireless	The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.		
Diagnostics	,,,.,		
Management Settings	The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.		
System Log	Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cappot contain a		
SNMP Agent	space.		
TR-069 Client			
Internet Time	Username:		
Access Control	Old Password:		
Services	New Password:		
IP Addresses Passwords	Confirm Password:		
Update Software Save/Reboot	Save/Apply		

9.7 Update Software

The **Update Software** screen allows for firmware updates. Manual device upgrades from a locally stored file can be performed using the following screen.

COMPRESS OF ADSL	Router		
N	Tools Update Software		
	Step 1: Obtain an updated software image file from your ISP.		
Device Info			
Advanced Setup	Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.		
Wireless	Step 3: Click the "Update Software" button once to upload the new image file.		
Diagnostics			
Management	NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.		
Settings	Cofficient File Manage		
System Log	Soluvate File Name: Drowse		
SNMP Agent	Under Collinson		
TR-069 Client	Update Software		
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 **Browse** button to locate the image file.

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

NOTE 1: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation.

It is recommended that you compare the **Software Version** at the top of the **Device Info** Summary screen (see graphic below) with the firmware version installed, to confirm the installation was successful.

9.8 Save and Reboot

This function saves the current configuration settings and reboots the device.

GOMHEND ADSL	Router
N	Click the button below to save and reboot the router.
Device Info	Save/Reboot
Advanced Setup	
Wireless	
Diagnostics	
Management	
Settings	
System Log	
SNMP Agent	
TR-069 Client	
Internet Time	
Access Control	
Update Software	
Save/Reboot	

- **NOTE:** You may need to reconfigure the TCP/IP settings after rebooting. For example, if the DHCP server is disabled Static IP settings must be configured. See section 3.2 IP Configuration for instructions.
- **NOTE:** If you lose all access to the web user interface (WUI), you may need to close the browser, wait for two minutes, and then restart the WUI. If this does not work, then press the reset button on the rear panel of the device for 5-7 seconds to restore to default settings.

Appendix A - Security

Stateful Packet Inspection

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

Denial of Service Attack

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

TCP/IP/Port/Interface Filter

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

Outgoing IP Filter

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

Filter Name: User defined Filter Name.

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

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

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

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

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

Example 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Destination Address	: NA
Destination Subnet Mask	: NA
Destination Port	: NA

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

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Destination Address	: 172.16.13.4
Destination Subnet Mask	: 255.255.255.0
Destination Port	: 6060:7070

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

Incoming IP Filtering:

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

Filter Name: User defined Filter Name.

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

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

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

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

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

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

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Destination Address	: NA
Destination Submask	: NA
Destination Port	: NA

Selected WAN interface: mer_0_35/nas_0_35

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

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Source Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Destination Address	: 192.168.1.45
Destination Subnet Mask	: 255.255.255.0
Destination Port	: 6060:7070

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

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

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

Protocol Type: Either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

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

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

Frame Direction: (User must select interface on which this rule is applied)

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

Example 1:

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

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

Example 2:

Global Policy: Blocked Protocol Type: PPPoE Destination MAC Addr: 00:12:34:56:78:90 Source MAC Addr: 00:34:12:78:90:56 Frame Direction: WAN => LAN WAN Interface Selected: br_0_34/nas_0_34

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

Daytime Parental Control

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

User Name: Name of the Filter.

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

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

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

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

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

Example:

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

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

Appendix B - Pin Assignments

Line Port (RJ11)

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

LAN Port (RJ45)

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

Appendix C - Specifications

Rear Panel

RJ-11 X1 for ADSL2+, RJ-45 X 4 for LAN, Reset Button X 1, Power Jack X 1, Power button X 1, Wi-Fi Antenna X 1, WPS Button X 1, Wi-Fi Button X 1

ADSL

Standard ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2G.992.5 (ADSL2+)Downstream: 24 MbpsUpstream: 1.3 MbpsG.992.3 (ADSL2)Downstream: 12 MbpsUpstream: 1.3 MbpsG.DMTDownstream: 8 MbpsUpstream: 0.8 MbpsAnnexMAnnexMAnnexM

Ethernet

StandardIEEE 802.3, IEEE 802.3u 10/100 BaseTAuto-sense MDI/MDX supportYes

Wireless

IEEE802.11b/g
64/128-bit WEP
11 (US, Canada), 13 (Europe), 14 (Japan)
.Up to 54Mbps
Yes
Optional

ATM Attributes

RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC 1577 (IPoA), Annex M Support PVCs16 AAL type......AAL5 ATM service classUBR/CBR/VBR ATM UNI support.....UNI3.1/4.0 OAM F4/F5......Yes

Management

SNMP, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP, TFTP, or FTP server, Supports TR-069/TR-098/TR-111 for Remote Management

Bridge Functions

Routing Functions

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

Security Functions

Authentication protocols...... PAP, CHAP TCP/IP/Port filtering rules, Port triggering/Forwarding, Packet and MAC address filtering, Access Control, SSH

QoS

L3 policy-based QoS, IP QoS, ToS

Application Passthrough

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

Power Supply

External power adapter..... Input 110 Vac or 240 Vac

Environment Condition

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

Kit Weight

1 X (CT-5365, RJ11 and RJ45 cables, Power Adapter, CD-ROM) = 0.97 kg

Dimensions205 mm (W) x 47 mm (H) x 145 mm (D)

CertificationsFCC Part 15 class B

NOTE: Specifications are subject to change without notice.

Appendix D - SSH Client

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

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

To access the router using Linux ssh client: From LAN: Use the router WEB UI to enable SSH access from LAN. (default is enabled) type: ssh -l root 192.168.1.1

From WAN: Use WEB UI to enable SSH access from WAN. type: ssh -l support router-WAN-ip-address To access the router using the Windows "putty" ssh client: From LAN: Use the router WEB UI to enable SSH access from LAN (default is enabled) type: putty -ssh -l admin 192.168.1.1

From WAN: In the router, use WEB UI to enable SSH access from WAN. type: putty -ssh -l support router-WAN-ip-address