

AR-5312u

ADSL2+ WLAN Router

User Manual

Version A1.0, November 3, 2014



Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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



WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in [Appendix C – Specifications](#).

Copyright

Copyright©2014 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

NOTE: This document is subject to change without notice.

Protect Our Environment



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



separate from domestic waste.

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

Table of Contents

CHAPTER 1 INTRODUCTION.....	6
1.1 FEATURES LIST	6
CHAPTER 2 INSTALLATION.....	7
2.1 HARDWARE SETUP.....	7
2.2 FRONT PANEL	9
CHAPTER 3 WEB USER INTERFACE.....	11
3.1 DEFAULT SETTINGS	11
3.2 IP CONFIGURATION.....	11
3.3 LOGIN PROCEDURE.....	14
CHAPTER 4 DEVICE INFORMATION.....	16
4.1 WAN	17
4.2 STATISTICS.....	18
4.2.1 LAN Statistics.....	18
4.2.2 WAN Service	19
4.2.3 XTM Statistics.....	20
4.2.4 xDSL Statistics	21
4.3 ROUTE	26
4.4 ARP.....	27
4.5 DHCP.....	27
4.6 NAT SESSION	29
4.7 IGMP PROXY	30
4.8 IPV6	31
4.8.1 IPv6 Info.....	31
4.8.2 IPv6 Neighbor	32
4.8.3 IPv6 Route	33
4.9 NETWORK MAP	34
4.10 WIRELESS	35
4.10.1 Station Info	35
4.10.2 Site Survey	36
CHAPTER 5 BASIC SETUP.....	37
5.1 LAYER 2 INTERFACE	37
5.1.1 WAN Service Setup	38
5.2 NAT	39
5.2.1 Virtual Servers	39
5.2.2 Port Triggering.....	40
5.2.3 DMZ Host	42
5.2.4 IP Address Map	43
5.2.5 IPSEC ALG.....	45
5.2.6 SIP ALG.....	46
5.3 LAN.....	47
5.3.1 LAN IPv6 Autoconfig.....	50
5.3.2 Static IP Neighbor	53
5.3.3 UPnP	54
5.4 WIRELESS	55
5.4.1 Basic	55
5.4.2 Security.....	57
5.5 PARENTAL CONTROL.....	60
5.5.1 Time Restriction.....	60
5.5.2 URL Filter.....	61
5.6 HOME NETWORKING.....	63
5.6.1 Print Server	63
5.6.2 DLNA.....	64
5.6.3 Storage Service.....	65

CHAPTER 6 ADVANCED SETUP	66
6.1 AUTO-DETECTION SETUP	66
6.2 SECURITY	71
6.2.1 IP Filtering	71
6.2.2 MAC Filtering.....	74
6.3 QUALITY OF SERVICE (QoS).....	76
6.3.1 QoS Queue Setup.....	77
6.3.2 QoS Policer	79
6.3.3 QoS Classification.....	81
6.4 ROUTING	83
6.4.1 Default Gateway.....	83
6.4.2 Static Route.....	84
6.4.3 Policy Routing	85
6.4.4 RIP.....	86
6.5 DNS.....	87
6.5.1 DNS Server.....	87
6.5.2 Dynamic DNS.....	88
6.5.3 DNS Entries.....	89
6.5.4 DNS Proxy/Relay.....	90
6.6 DSL.....	91
6.7 INTERFACE GROUPING	93
6.8 IP TUNNEL.....	96
6.8.1 IPv6inIPv4.....	96
6.8.2 IPv4inIPv6.....	97
6.9 CERTIFICATE.....	98
6.9.1 Local.....	98
6.9.2 Trusted CA.....	100
6.10 POWER MANAGEMENT	101
6.11 MULTICAST.....	102
6.12 WIRELESS	104
6.12.1 Basic.....	104
6.12.2 Security.....	106
6.12.3 WPS.....	109
6.12.4 MAC Filter.....	113
6.12.5 Wireless Bridge.....	115
6.12.6 Advanced.....	116
CHAPTER 7 DIAGNOSTICS	119
7.1 DIAGNOSTICS – INDIVIDUAL TESTS	119
7.2 FAULT MANAGEMENT.....	120
7.3 UPTIME STATUS	121
7.4 PING	122
7.5 TRACE ROUTE	123
7.6 SYSTEM UTILIZATION	124
CHAPTER 8 MANAGEMENT	125
8.1 SETTINGS.....	125
8.1.1 Backup Settings.....	125
8.1.2 Update Settings.....	126
8.1.3 Restore Default.....	126
8.2 SYSTEM LOG	127
8.3 SNMP AGENT	129
8.4 TR-069 CLIENT	130
8.5 INTERNET TIME	132
8.6 ACCESS CONTROL	133
8.6.1 Passwords.....	133
8.6.2 Service Access.....	135
8.6.3 IP Address.....	136
8.7 UPDATE SOFTWARE	137
8.8 REBOOT.....	138
CHAPTER 9 LOGOUT	139

APPENDIX A - FIREWALL	140
APPENDIX B - PIN ASSIGNMENTS	143
APPENDIX C – SPECIFICATIONS	144
APPENDIX D - SSH CLIENT	146
APPENDIX E - CONNECTION SETUP	147
APPENDIX F - WPS OPERATION	179
APPENDIX G - PRINTER SERVER	184

Chapter 1 Introduction

AR-5312u is an 802.11n (300Mbps) Wireless ADSL2+ router comprising four 10/100 Base-T Ethernet ports, a Wi-Fi Protected Setup (WPS)/ Wi-Fi switch button, a USB Host, and is backward compatible with existing 802.11b (11Mbps) and 11g (54bps) equipment.

The AR-5312u ADSL2+ router provides state of the art security features such as 64/128 bit WEP encryption and WPA/WPA2 encryption, Firewall, and VPN pass through.

1.1 Features List

- Annex A/L/M
- PhyR and G.INP
- Up to 16 PVCs and Up to 8 PTM flows
- Auto PVC configuration
- Integrated 802.11b/g/n AP
- WPA/WPA2, 802.1x and RADIUS client
- Wi-Fi Protected Setup (WPS) 2.0
- Wireless Distribution System (WDS)
- WMM
- IPv6 compliant
- UPnP
- IGMP Snooping/Proxy and Fast Leave
- DNS Proxy/Relay
- DHCP Server/Client
- Dynamic IP assignment
- NAT/PAT
- IP/MAC address filtering
- Embedded SNMPv2 agent
- Per-PVC packet level QoS
- Static route and RIP/RIP v2 routing function
- FTP/TFTP server
- TR-064/TR-069/TR-098/TR-111
- Configuration backup and restoration
- Web-based management
- HTTPS/HTTP server
- Remote administration, automatic firmware upgrade and configuration

Chapter 2 Installation

2.1 Hardware Setup



DO NOT STACK

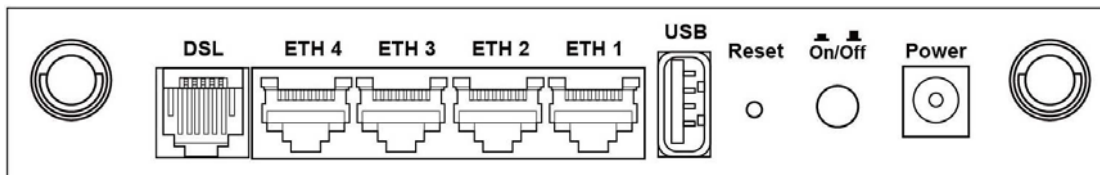
Non-stackable

This device is not stackable – do not place units on top of each other, otherwise damage could occur.

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



DSL

Connect to the DSL port with the DSL RJ11 cable.

LAN (Ethernet) Ports

You can connect the router to up to four LAN devices using RJ45 cables. The ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

USB HOST PORT

A USB 2.0 host port supports compatible printers. See [Appendix G](#) for setup instructions. Support for other devices may be added in future firmware upgrades.

Reset Button

Restore the default parameters of the device by pressing the Reset button for 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section [2.2 Front Panel](#) for details).

NOTE: If pressed down for more than 60 seconds, the AR-5312u will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

Power ON

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

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

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

2.2 Front Panel

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



LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
ETH 1X-4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
WPS	Green	On	WPS function is OK.
		Off	WPS function is closed or failure.
WiFi	Green	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WIFI.
USB	Green	On	USB equipment is connected.
		Off	USB equipment is not connected.
		Blink	Data transmission.
DSL	Green	On	xDSL Link is established.
		Off	Modem power off.
		Blink	fast: xDSL Link is training or data transmitting. slow: xDSL training failed.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
		Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing through the device (either direction)

Note:

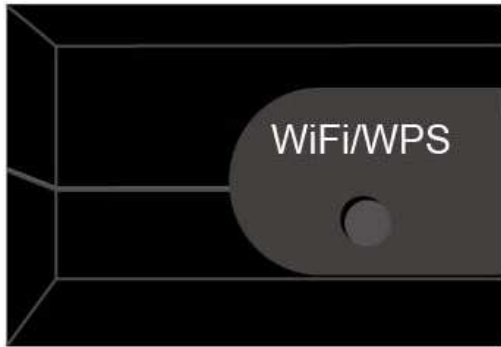
A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL is up) and no traffic detected. If the IP or PPPoE session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.

WiFi/WPS Button

Press and release WiFi-WPS button to activate WPS (make sure the WPS is enabled in Wireless->Security page).

Press and hold WiFi-WPS button more than 5 seconds to enable/disable WiFi.



Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- WIFI access: **enabled**

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the AR-5312u powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

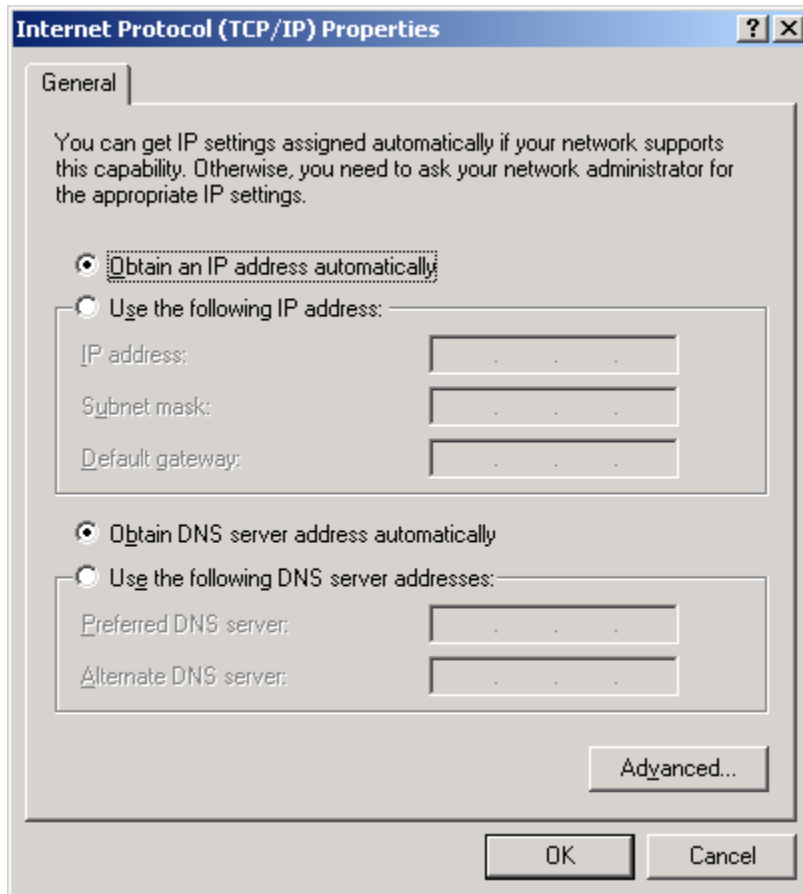
To obtain an IP address from the DHCP server, follow the steps provided below.

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

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

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

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



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

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

STATIC IP MODE

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

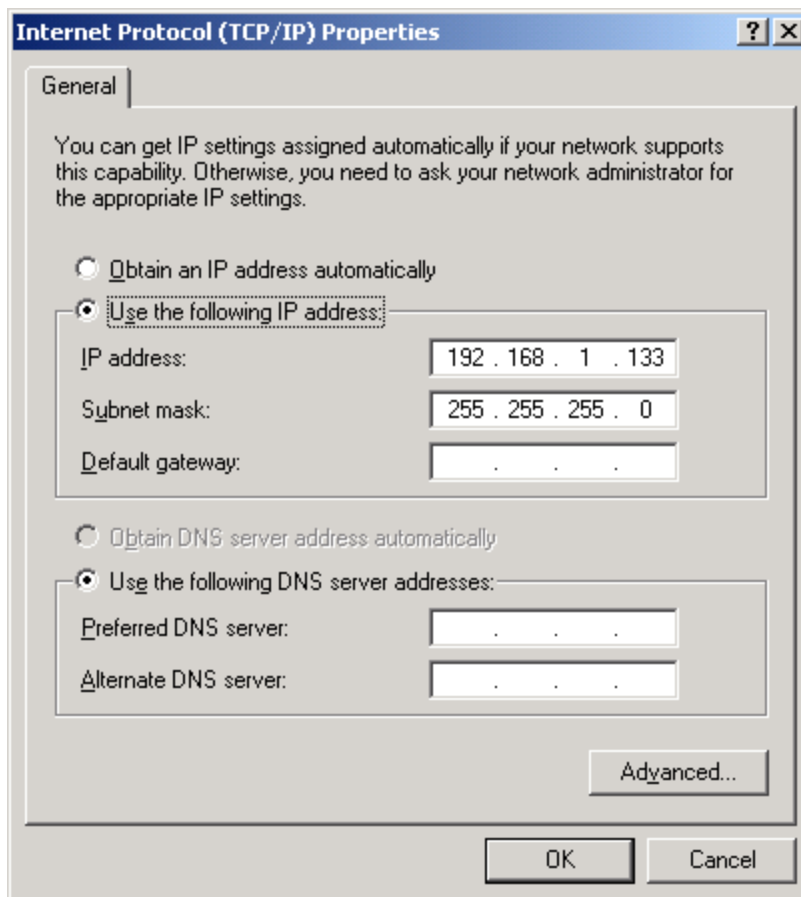
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



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

3.3 Login Procedure

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

NOTE: The default settings can be found in [3.1 Default Settings](#).

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

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the [Chapter 4 Device Information](#) screen and login with remote username and password.

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



Click **OK** to continue.

NOTE: The login password can be changed later (see [8.6.1 Passwords](#)).

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

The screenshot displays the Comtrend web management interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different sections: Device Info (a line graph), Basic Setup (a floppy disk), Advanced Setup (a gear), Diagnostics (a stethoscope), Management (a person), and Logout (a person walking). Below the navigation bar, the main content area is divided into three sections: Device, LAN, and Wireless. On the left side, there is a sidebar menu with options like Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, Network Map, and Wireless.

Device

Model	AR-5312u
Board ID	96318AT-1341N5
Serial Number	1465312U02F-AA000251
Firmware Version	JC31-412CTU-C03_R01.A2pG039k.d25f
Bootloader (CFE) Version	1.0.38-112.118-46
Up Time	1 hours:3 mins:36 secs

Wireless

Driver Version	6.30.102.7.cpe4.12L06B.1
Primary SSID	Comtrend9A24
Status	Enabled
Channel	1
Security	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	•••••••• <input type="button" value="Show"/>

LAN

ETH1 ETH2 ETH3 ETH4

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:f5:9a:24
DHCP Server	Enabled
LAN IPv6 ULA Address	

WAN

DOWN

Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway	

You can also reach this page by clicking on the following icon located at the top of the screen.



Chapter 4 Device Information

You can reach this page by clicking on the following icon located at the top of the screen.



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

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

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

The Device Info Summary screen displays at startup.

Device

Model	AR-5312u
Board ID	96318AT-1341N5
Serial Number	1465312UXXF-AA000251
Firmware Version	JC31-412CTU-C03_R01.A2pG039k.d25f
Bootloader (CFE) Version	1.0.38-112.118-46
Up Time	1 hours:3 mins:36 secs

Wireless

Driver Version	6.30.102.7.cpe4.12L06B.1
Primary SSID	Comtrend9A24
Status	Enabled
Channel	1
Secure	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	•••••••• <input type="button" value="Show"/>

LAN

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	f8:8e:85:f5:9a:24
DHCP Server	Enabled
LAN IPv6 ULA Address	

WAN

Default Gateway	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway	

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

4.1 WAN

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with options: Summary, WAN (highlighted), Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, and IPv6. The main content area is titled 'WAN Info' and contains a table with the following columns: Interface, Description, Type, VlanMuxId, IPv6, Icmp, MLD, NAT, Firewall, Status, IPv4 Address, and IPv6 Address.

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

4.2 Statistics

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

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

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ETH1	0	0	0	0	0	0	0	0
ETH2	0	0	0	0	0	0	0	0
ETH3	0	0	0	0	0	0	0	0
ETH4	326426	3417	0	0	747880	1753	0	0
wlan0	0	0	0	0	0	0	0	0

Reset Statistics

Heading	Description
Interface	LAN interface(s)
Received/Transmitted:	<ul style="list-style-type: none"> - Bytes - Pkts - Errs - Drops
	<ul style="list-style-type: none"> Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.

Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Statistics -- WAN

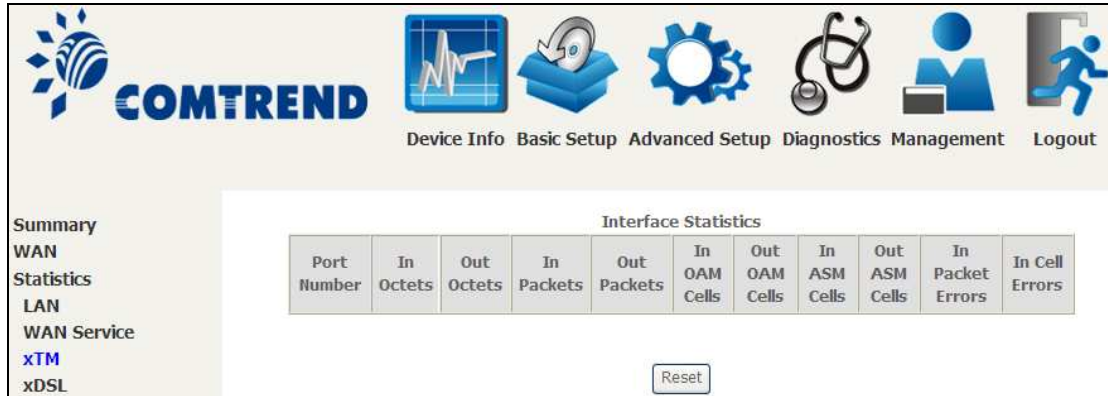
Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Reset Statistics

Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted	<ul style="list-style-type: none"> - Bytes - Pkts - Errs - Drops
	<ul style="list-style-type: none"> Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.3 XTM Statistics

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



XTM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface.
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error

4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type. The two examples below (ADSL2 & ADSL2+) show this variation.

ADSL2

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout


Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6
Wireless

Statistics -- xDSL

Mode:	ADSL_G_dmt.bis			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	L0			
	Downstream	Upstream		
PhyR Status:	Off	Off		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	98	67		
Attenuation (0.1 dB):	40	25		
Output Power (0.1 dBm):	131	120		
Attainable Rate (Kbps):	12764	1219		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	12767	1219	0	0
MSGc (# of bytes in overhead channel message):	51	11	0	0
B (# of bytes in Mux Data Frame):	227	75	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	1	0	0
T (Mux Data Frames over sync bytes):	2	2	0	0
R (# of check bytes in FEC Data Frame):	0	0	0	0
S (ratio of FEC over PMD Data Frame length):	0.5701	1.9804	0.0	0.0
L (# of bits in PMD Data Frame):	3199	307	0	0
D (interleaver depth):	1	1	0	0
Delay (msec):	0	0	0.0	0.0
IHP (DMT symbol):	0.00	0.00	0.0	0.0
Super Frames:	0	0	0	0
Super Frame Errors:	929	0	0	0
RS Words:	0	3459590	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	23	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	51557064	4916868	0	0
Data Cells:	460	0	0	0
Bit Errors:	0	0	0	0
Total ES:	21	0		
Total SES:	21	0		
Total UAS:	137	116		

xDSL BER Test Reset Statistics Draw Graph

ADSL2+



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6
Wireless

Statistics -- xDSL

Mode:	ADSL2+			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	L0			
	Downstream	Upstream		
PhyR Status:	Off	Off		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	63	73		
Attenuation (0.1 dB):	55	25		
Output Power (0.1 dBm):	60	120		
Attainable Rate (Kbps):	26956	1211		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	26438	1207	0	0
MSGc (# of bytes in overhead channel message):	55	11	0	0
B (# of bytes in Mux Data Frame):	124	74	0	0
M (# of Mux Data Frames in FEC Data Frame):	2	1	0	0
T (Mux Data Frames over sync bytes):	7	2	0	0
R (# of check bytes in FEC Data Frame):	4	0	0	0
S (ratio of FEC over PMD Data Frame length):	0.3022	1.9736	0.0	0.0
L (# of bits in PMD Data Frame):	6723	304	0	0
D (interleaver depth):	32	1	0	0
Delay (msec):	2	0	0.0	0.0
INP (DMT symbol):	0.00	0.00	0.0	0.0
Super Frames:	185303	176369	0	0
Super Frame Errors:	831	10288	0	0
RS Words:	39561768	1768879	0	0
RS Correctable Errors:	18	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	16	3635	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	186400453	8507172	0	0
Data Cells:	1474	3	0	0
Bit Errors:	0	0	0	0
Total ES:	20	0		
Total SES:	20	0		
Total UAS:	1213	1193		

xDSL BER Test Reset Statistics Draw Graph

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

Field	Description
Mode	ADSL2, ADSL2+
Traffic Type	ATM, PTM
Status	Lists the status of the DSL link
Link Power State	Link output power state.
Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin

Field	Description
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

In VDSL mode, the following section is inserted.

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

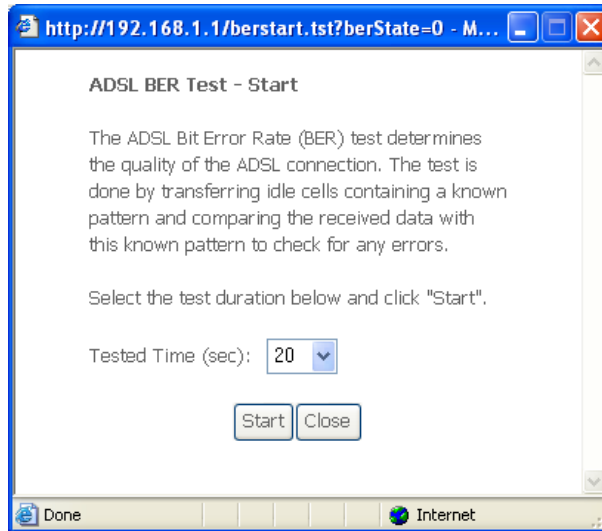
OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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

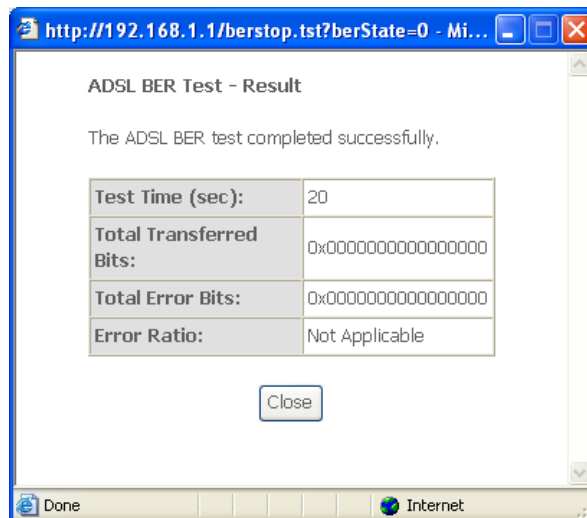
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

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

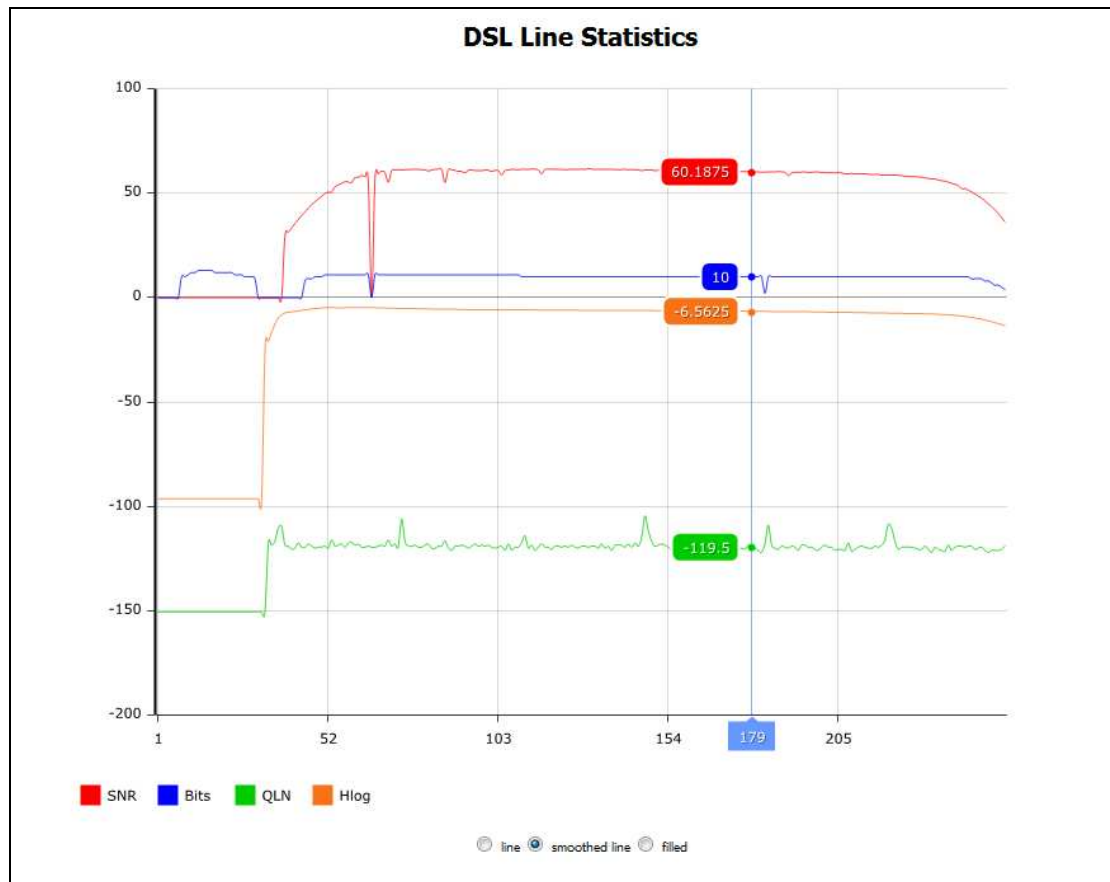


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



xDSL TONE GRAPH

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



4.3 Route

Choose **Route** to display the routes that the AR-5312u has found.

Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6

Device Info -- Route

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

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

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

4.4 ARP

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area displays the ARP table under the heading "Device Info -- ARP". On the left side, there is a sidebar menu with options: Summary, WAN, Statistics, Route, ARP (highlighted), and DHCP.

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:25:11:af:fd:f8	br0

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


4.5 DHCP






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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area displays the DHCP Leases table under the heading "Device Info -- DHCP Leases". On the left side, there is a sidebar menu with options: Summary, WAN, Statistics, Route, ARP, DHCP (highlighted), DHCPv4, and DHCPv6.

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

Field	Description
IPv6 Address	Shows IP address of device/host/PC
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



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
DHCPv4
DHCPv6

Device Info -- DHCPv6 Leases

IPv6 Address	MAC Address	Duration	Expires In
--------------	-------------	----------	------------

Field	Description
IPv6 Address	Shows IP address of device/host/PC
MAC Address	Shows the Ethernet MAC address of the device/host/PC
Duration	Shows leased time in hours
Expires In	Shows how much time is left for each DHCP Lease

4.6 NAT Session

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session

NAT Session

Press "Show All" will show all NAT session information.

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
-----------	-------------	----------------	------------------	----------	---------

Refresh Show All

Click the "Show All" button to display the following.

NAT Session

Press "Show Less" will show NAT session information on WAN side only.

Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.3	4233	192.168.1.1	80	tcp	73
192.168.1.3	4211	192.168.1.1	80	tcp	25
192.168.1.3	4230	192.168.1.1	80	tcp	53
192.168.1.3	4251	192.168.1.1	80	tcp	103
192.168.1.3	4260	192.168.1.1	80	tcp	104
192.168.1.3	17500	255.255.255.255	17500	udp	29
192.168.1.3	4241	192.168.1.1	80	tcp	83
192.168.1.3	4225	192.168.1.1	80	tcp	48
192.168.1.3	4255	192.168.1.1	80	tcp	103
192.168.1.3	17500	192.168.1.255	17500	udp	29
192.168.1.3	4239	192.168.1.1	80	tcp	83
192.168.1.3	4221	192.168.1.1	80	tcp	48
192.168.1.3	4261	192.168.1.1	80	tcp	104
192.168.1.3	4263	192.168.1.1	80	tcp	431999

Refresh Show Less

Field	Description
Source IP	The source IP from which the NAT session is established
Source Port	The source port from which the NAT session is established
Destination IP	The IP which the NAT session was connected to
Destination Port	The port which the NAT session was connected to
Protocol	The Protocol used in establishing the particular NAT session
Timeout	The time remaining for the TCP/UDP connection to be active

4.7 IGMP Proxy

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of menu items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, and IGMP Proxy. The main content area displays a 'List of IGMP Proxy Entries' table with columns for Interface, WAN, Groups, Member, and Timeout.

Field	Description
Interface	The Source interface from which the IGMP report was received
WAN	The WAN interface from which the multicast traffic is received
Groups	The destination IGMP group address
Member	The Source IP from which the IGMP report was received
Timeout	The time remaining before the IGMP report expires

4.8 IPv6

4.8.1 IPv6 Info

The screenshot shows the Comtrend web interface. The navigation menu includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The IPv6 Info section is active, displaying the following information:

IPv6 WAN Connection Info

Interface	Status	Address	Prefix

General Info

Device Link-local Address	fe80::fa8e:85ff:fef5:9a24/64
Default IPv6 Gateway	
IPv6 DNS Server	

The left sidebar menu includes: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, **IPv6 Info**, IPv6 Neighbor, and IPv6 Route.

Field	Description
Interface	WAN interface with IPv6 enabled
Status	Connection status of the WAN interface
Address	IPv6 Address of the WAN interface
Prefix	Prefix received/configured on the WAN interface
Device Link-local Address	The CPE's LAN Address
Default IPv6 Gateway	The default WAN IPv6 gateway
IPv6 DNS Server	The IPv6 DNS servers received from the WAN interface / configured manually

4.8.2 IPv6 Neighbor

The screenshot shows the Comtrend web interface. At the top left is the Comtrend logo. To its right is a navigation menu with icons and labels: Device Info (line graph), Basic Setup (floppy disk), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). Below the navigation menu is a sidebar on the left with a list of menu items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, IPv6 Info, **IPv6 Neighbor** (highlighted in blue), and IPv6 Route. The main content area is titled "Device Info -- IPv6 Neighbor Discovery table" and contains a table with four columns: IPv6 address, Flags, HW Address, and Device.

Field	Description
IPv6 Address	Ipv6 address of the device(s) found
Flags	Status of the neighbor device
HW Address	MAC address of the neighbor device
Device	Interface from which the device is located

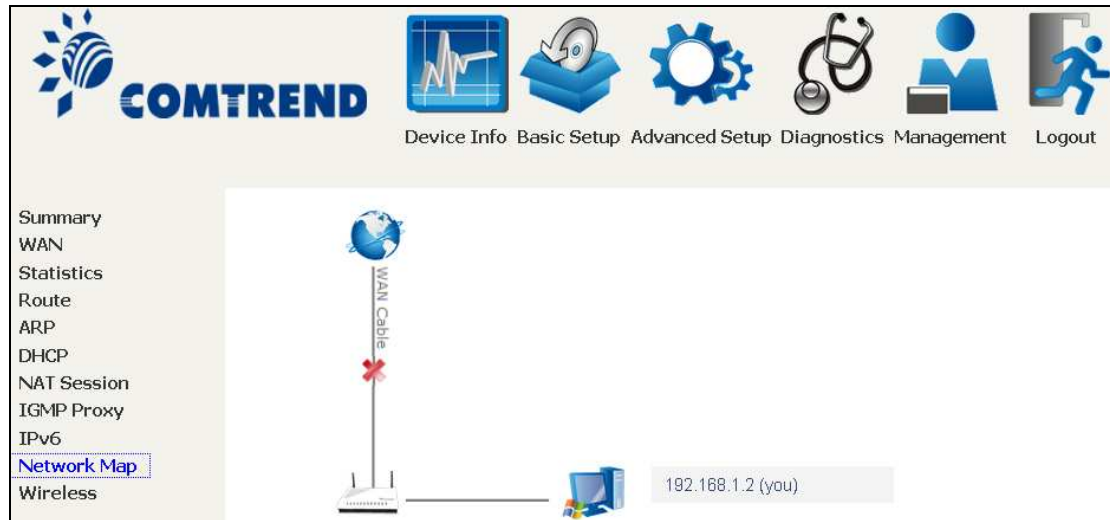
4.8.3 IPv6 Route

The screenshot shows the COMTREND web interface. At the top left is the COMTREND logo. To the right are navigation icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation is a sidebar menu with options: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, IPv6 Info, IPv6 Neighbor, and IPv6 Route (highlighted). The main content area is titled "Device Info -- IPv6 Route" and contains a table with the following columns: Destination, Gateway, Metric, and Interface.

Field	Description
Destination	Destination IP Address
Gateway	Gateway address used for destination IP
Metric	Metric specified for gateway
Interface	Interface used for destination IP

4.9 Network Map

The network map is a graphical representation of router's wan status and LAN devices. The feature is only available using a non-IE browser.



The screenshot displays the Comtrend router's web interface. At the top left is the Comtrend logo. To its right is a navigation bar with icons and labels for: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists various system status pages: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, **Network Map** (highlighted with a blue border), and Wireless. The main content area shows a network diagram. On the left, a router icon is connected to a globe icon labeled 'WAN Cable', with a red 'X' indicating a disconnected or failed connection. A horizontal line connects the router to a computer icon on the right, which is labeled with the IP address '192.168.1.2 (you)'.

4.10 Wireless

4.10.1 Station Info

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


The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with options: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, Network Map, Wireless, Station Info (highlighted), and Site Survey. The main content area is titled 'Wireless -- Authenticated Stations' and contains the text 'This page shows authenticated wireless stations and their status.' Below this text is a table with five columns: MAC, Associated, Authorized, SSID, and Interface. A 'Refresh' button is located to the right of the table.







Consult the table below for descriptions of each column heading.

Field	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

4.10.2 Site Survey

The graph displays wireless APs found in your neighborhood by channel.



Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary

WAN

Statistics

Route

ARP

DHCP

NAT Session

IGMP Proxy

IPv6

Network Map

Wireless

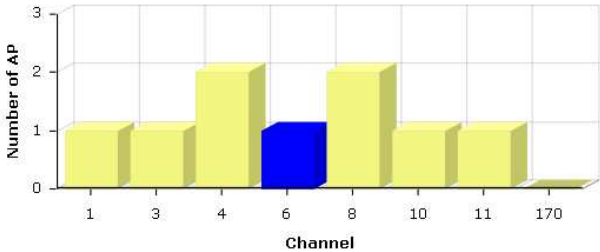
Station Info

Site Survey

Wireless -- Channel Graph

The following graph displays wireless APs found in your neighborhood by channel.

Your broadband router is transmitting on channel 6.











Channel	Number of AP
1	1
3	1
4	2
6	1
8	2
10	1
11	1
170	0

■ Your Broadband Router
■ Neighboring APs

Wireless -- Site Survey

List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
	NETT_FEED96	3A:72:C0:FE:ED:97	8
	TB-Mini	38:72:C0:FE:ED:97	8
	oran	F8:8E:85:11:22:33	10
	CTMIS-INT	80:1F:02:FF:7E:C8	11
	don	80:1F:02:57:22:34	1
	CTMIS-INT	02:1D:20:FF:C8:E9	3
	CT_WAP175	80:1F:02:E6:D4:B0	4
	ACSTest	02:1F:02:E6:D4:B0	4

[Refresh](#)

36

Chapter 5 Basic Setup

You can reach this page by clicking on the following icon located at the top of the screen.



5.1 Layer 2 Interface

Add or remove ATM, PTM and ETH WAN interface connections here.

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. The main content area is titled 'Step 1: Layer 2 Interface'. It features a dropdown menu to 'Select new interface to add:' with 'ATM Interface' selected and an 'Add' button. Below this are three configuration sections: 'DSL ATM Interface Configuration' with a table of columns (Interface, Vpi, Vci, DSL Latency, Category, Peak Cell Rate, Sustainable Cell Rate, Max Burst Size, Link Type, Conn Mode, IP QoS, MPAAL Prec./Alg./Wght, Remove), 'DSL PTM Interface Configuration' with a table (Interface, DSL Latency, PTM Priority, Conn Mode, IP QoS, Remove), and 'ETH WAN Interface Configuration' with a table (Interface/(Name), Connection Mode, Remove). At the bottom, 'Step 2: Wide Area Network (WAN) Service Setup' includes a 'PPP Redirect' section with 'Disable' selected and 'Enable' as an option, and a table with columns (Interface, Description, Type, Vlan8021p, VlanMuxId, Igmp, NAT, Firewall, IPv6, Mld, Remove, Edit) and 'Add'/'Remove' buttons.

Click **Add** to create a new ATM interface (see [Appendix E - Connection Setup](#)).

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

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

5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: Disable Enable

Interface	Description	Type	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Mld	Remove	Edit

Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see [Appendix E - Connection Setup](#).

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

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

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

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

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

5.2 NAT

To display this option, NAT must be enabled in at least one PVC. *NAT is not an available option in Bridge mode.*

5.2.1 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.



COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
 Virtual Servers
 Port Triggering
 DMZ Host
 IP Address Map
 IPSEC ALG
 SIP ALG
 LAN

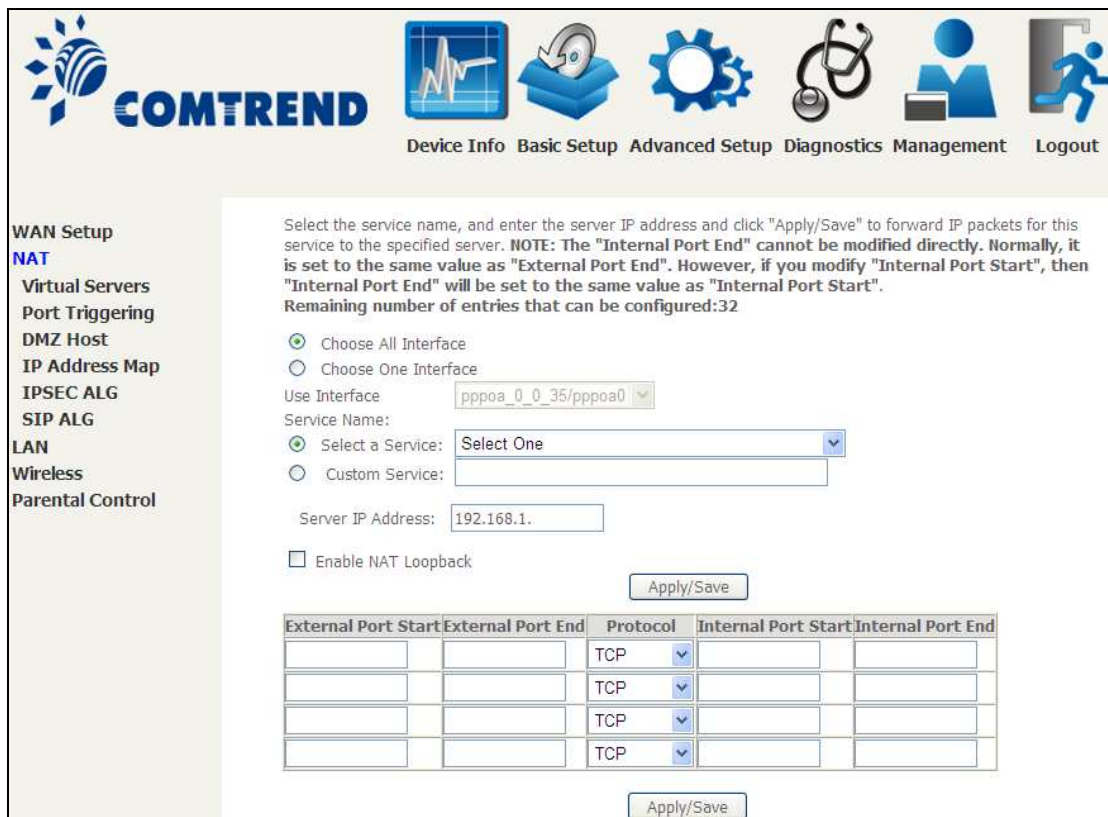
NAT -- Virtual Servers Setup

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

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	NAT Loopback	Remove

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



COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
 Virtual Servers
 Port Triggering
 DMZ Host
 IP Address Map
 IPSEC ALG
 SIP ALG
 LAN
 Wireless
 Parental Control

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**
 Remaining number of entries that can be configured:32

Choose All Interface
 Choose One Interface

Use Interface:

Service Name:

Select a Service:
 Custom Service:

Server IP Address:

Enable NAT Loopback

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		

Apply/Save

Consult the table below for field and header descriptions.

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

5.2.2 Port Triggering

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

The screenshot shows the COMTREND router web interface. The main content area is titled "NAT -- Port Triggering Setup". It contains a descriptive paragraph: "Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured." Below the text are "Add" and "Remove" buttons. A table is displayed with the following structure:

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

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
LAN

NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Click Save/Apply to save and apply the settings.

Consult the table below for field and header descriptions.

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

5.2.3 DMZ Host

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



The screenshot shows the COMTREND router's web management interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host (highlighted), IP Address Map, IPSEC ALG, SIP ALG, and LAN. The main content area is titled "NAT -- DMZ Host" and contains the following text: "The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer." Below this, it says: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." There is a text input field labeled "DMZ Host IP Address:" and a checkbox labeled "Enable NAT Loopback". A "Save/Apply" button is located at the bottom right of the form.

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

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

Enable NAT Loopback allows PC on the LAN side to access servers in the LAN network via the router's WAN IP.

5.2.4 IP Address Map

Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).

Field/Header	Description
Rule	The number of the rule
Type	Mapping type from local to public.
Local Start IP	The beginning of the local IP
Local End IP	The ending of the local IP
Public Start IP	The beginning of the public IP
Public End IP	The ending of the public IP
Remove	Remove this rule

Click the Add button to display the following.

Select a Service, then click the **Save/Apply** button.

One to One: mapping one local IP to a specific public IP

Many to one: mapping a range of local IP to a specific public IP

Many to many(Overload): mapping a range of local IP to a different range of public IP

Many to many(No Overload): mapping a range of local IP to a same range of public IP

5.2.5 IPSEC ALG

IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.



The screenshot displays the Comtrend router's web management interface. At the top, the Comtrend logo is on the left, and a navigation menu includes Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left side of the main content area, a sidebar menu lists WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG (highlighted), and SIP ALG. The main content area is titled 'IPSEC ALG settings' and contains the following text: 'This page allows you to enable / disable IPSEC ALG.' followed by a note: 'NOTE: This configuration doesn't take effect until router is rebooted.' Below this, there is a checked checkbox labeled 'Enable IPSEC ALG.' and a 'Save' button.

To enable IPSEC ALG, tick the checkbox and click the **Save** button.

5.2.6 SIP ALG

This page allows you to enable / disable SIP ALG.



The screenshot displays the Comtrend web management interface. At the top left is the Comtrend logo. A navigation bar contains icons and labels for: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG, SIP ALG (highlighted in blue), and LAN. The main content area is titled "SIP ALG settings" and contains the following text: "This page allows you to enable / disable SIP ALG." followed by a bolded note: "NOTE: This configuration doesn't take effect until router is rebooted." Below this is a checked checkbox labeled "Enable SIP ALG." and a "Save" button.

5.3 LAN

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

The screenshot displays the Comtrend web interface for LAN configuration. The top navigation bar includes icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various setup options: WAN Setup, NAT, LAN (selected), IPv6 Autoconfig, Static IP Neighbor, UPnP, Wireless, Parental Control, and Home Networking. The main content area is titled 'Local Area Network (LAN) Setup' and includes a 'GroupName' dropdown set to 'Default'. The 'IP Address' field is set to 192.168.1.1 and the 'Subnet Mask' is 255.255.255.0. Under 'IGMP Snooping mode', 'Blocking Mode' is selected, and 'Enable Enhanced IGMP' is checked. There are checkboxes for 'Enable LAN side firewall' and 'Setting TFTP Server'. The 'DHCP Server' section has 'Enable DHCP Server' selected, with 'Start IP Address' at 192.168.1.2, 'End IP Address' at 192.168.1.254, and 'Leased Time (hour)' set to 24. A table for 'Static IP Lease List' has columns for MAC Address, IP Address, Remove, and WDL, with 'Add Entries' and 'Remove Entries' buttons below it. An unchecked checkbox is for 'Configure the second IP Address and Subnet Mask for LAN interface'. The 'Ethernet Media Type' section shows four ports (ETH1-ETH4) all set to 'Auto'. An 'Apply/Save' button is at the bottom right.

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

IGMP Snooping:

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

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

Enable Enhanced IGMP: Enable by ticking the checkbox . IGMP packets between LAN ports will be blocked.

Enable LAN side firewall: Enable by ticking the checkbox .

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

Setting TFTP Server: Enable by ticking the checkbox . Then, input the TFTP server address or an IP address.

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

MAC Address	IP Address	Remove	WOL
<input type="button" value="Add Entries"/>		<input type="button" value="Remove Entries"/>	

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

DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

Enable Wake On Lan.

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

MAC Address	IP Address	Remove	WOL
12:34:56:78:90:12	192.168.1.33	<input checked="" type="checkbox"/>	Disable
<input type="button" value="Add Entries"/>		<input type="button" value="Remove Entries"/>	

2ND LAN INTERFACE

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

<input checked="" type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN interface
IP Address: <input type="text"/>
Subnet Mask: <input type="text"/>

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

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

Ethernet Media Type:

Configure auto negotiation, or enforce selected speed and duplex mode for the Ethernet ports.

Auto	▼
Auto	
10Mbps-Half	
10Mbps-Full	
100Mbps-Half	
100Mbps-Full	

5.3.1 LAN IPv6 Autoconfig

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

The screenshot shows the COMTREND web interface for IPv6 LAN Auto Configuration. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists configuration options: WAN Setup, NAT, LAN, IPv6 Autoconfig (selected), Static IP Neighbor, and UPnP. The main content area is titled "IPv6 LAN Auto Configuration" and includes a note about Stateful DHCPv6. It features several sections: "LAN IPv6 Link-Local Address Configuration" with radio buttons for EUI-64 (selected) and User Setting, and a text field for Interface Identifier (0:0:0:1); "Static LAN IPv6 Address Configuration" with a text field for Interface Address; "IPv6 LAN Applications" with checkboxes for Enable DHCPv6 Server (checked), Stateless (selected), and Stateful, along with text fields for Refresh Time (14400), Start/End interface IDs, and Leased Time; a table for Static IP Lease List with columns for MAC Address, Interface ID, and Remove, and buttons for Add/Remove Entries; "Enable SLAAC (RADVD)" with checkboxes for MTU (1500) and Enable Prefix Length Relay; "Enable Configuration Mode" (unchecked); "Enable ULA Prefix Advertisement" with radio buttons for Randomly Generate (selected) and Statically Configure, and text fields for Prefix, Preferred Life Time (-1), and Valid Life Time (-1); and "Enable MLD Snooping" with radio buttons for Standard Mode and Blocking Mode (selected). A "Save/Apply" button is located at the bottom right.

Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

Heading	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

Static LAN IPv6 Address Configuration

Heading	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

IPv6 LAN Applications

Heading	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client
Leased Time (hour):	Lease time for dhcpv6 client to use the assigned IP address

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

MAC Address	IP Address	Remove
Add Entries		Remove Entries

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

DHCP Static IP Lease

Enter the Mac address and Static Interface ID then click "Apply/Save" .

MAC Address:

Interface ID:

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

MAC Address	Interface ID	Remove
00:11:22:33:44:55	0:0:0:2	<input checked="" type="checkbox"/>

Heading	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable Configuration Mode	Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure Prefix	Specify the prefix to be used
Statically Configure	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports

5.3.2 Static IP Neighbor



Click the Add button to display the following.



Click **Apply/Save** to apply and save the settings.

Heading	Description
IP Version	The IP version used for the neighbor device
IP Address	Define the IP Address for the neighbor device
MAC Address	The MAC Address of the neighbor device
Associated Interface	The interface where the neighbor device is located

5.3.3 UPnP

Select the checkbox provided and click **Apply/Save** to enable UPnP protocol.



The screenshot displays the Comtrend web interface. At the top left is the Comtrend logo. A navigation bar contains icons and labels for: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side, a menu lists: WAN Setup, NAT, LAN, IPv6 Autoconfig, Static IP Neighbor, and UPnP (highlighted in blue). The main content area is titled 'UPnP Configuration' and includes a note: 'NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.' Below the note is a checked checkbox labeled 'Enable UPnP'. At the bottom right of the main area is an 'Apply/Save' button.

5.4 Wireless

5.4.1 Basic

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

The screenshot shows the Comtrend web interface for configuring wireless settings. The top navigation bar includes: Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists: WAN Setup, NAT, LAN, Wireless (selected), Basic (selected), Security, and Parental Control.

Wireless -- Basic

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/Save" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)
- Enable WiFi Button

SSID:

BSSID:

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A

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

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox <input checked="" type="checkbox"/> that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.

Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open Network Connections from the start Menu and select View Available Network Connections . If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox <input checked="" type="checkbox"/> to enable this function.
Enable WiFi Button	Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button.
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.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	<p>This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes <input checked="" type="checkbox"/> in the Enabled column. To hide a Guest SSID select its checkbox <input checked="" type="checkbox"/> in the Hidden column.</p> <p>Do the same for Isolate Clients and Disable WMM Advertise. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF, Max Clients and BSSID, consult the matching entries in this table.</p> <p>NOTE: Remote wireless hosts cannot scan Guest SSIDs.</p>

5.4.2 Security

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

The screenshot shows the Comtrend web interface for configuring wireless security. The top navigation bar includes the Comtrend logo and icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists configuration categories: WAN Setup, NAT, LAN, Wireless, Basic, Security (highlighted), and Parental Control. The main content area is titled "Wireless -- Security" and contains the following sections:

- Wireless -- Security**: Introduction text stating the page allows configuring security features of the wireless LAN interface, with options for manual setup or WPS.
- WPS Setup**: A section with "Enable WPS" set to "Disabled" via a dropdown menu.
- Manual Setup AP**: A section with instructions on setting network authentication, encryption, and key strength. It includes the following fields:
 - Select SSID: Comtrend9A24 (dropdown)
 - Network Authentication: WPA2-PSK (dropdown)
 - WPA/WAPI passphrase: masked with dots, with a "Click here to display" link.
 - WPA Group Rekey Interval: 3600 (text input)
 - WPA/WAPI Encryption: TKIP+AES (dropdown)
 - WEP Encryption: Disabled (dropdown)

An "Apply/Save" button is located at the bottom of the configuration area.

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

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID

Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication

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

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

Network Authentication:	802.1X
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:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

The settings for WPA authentication are shown below.

Network Authentication:	WPA
WPA Group Rekey Interval:	3600
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled

Apply/Save

The settings for WPA-PSK authentication are shown next.

Network Authentication:	WPA-PSK	<input type="button" value="v"/>
WPA/WAPI passphrase:	●●●●●●●●●●	Click here to display
WPA Group Rekey Interval:	3600	
WPA/WAPI Encryption:	TKIP+AES	<input type="button" value="v"/>
WEP Encryption:	Disabled	<input type="button" value="v"/>
<input type="button" value="Apply/Save"/>		

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.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

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

Encryption Strength

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

Please see section [6.12](#) for MAC Filter, Wireless Bridge and Advanced Wireless features.

5.5 Parental Control

This selection provides WAN access control functionality.

5.5.1 Time Restriction

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

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

WAN Setup
NAT
LAN
Wireless
Parental Control
Time Restriction
URL Filter

Access Time Restriction -- A maximum 16 entries can be configured.

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

Add Remove

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

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

WAN Setup
NAT
LAN
Wireless
Parental Control
Time Restriction
URL Filter

Access Time Restriction

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

User Name

Browser's MAC Address: 00:25:11:af:fd:f8
 Other MAC Address:
(xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Apply/Save

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

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

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

Other MAC Address: MAC address of another LAN device.

Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

End Blocking Time: The time the restrictions end.

5.5.2 URL Filter

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



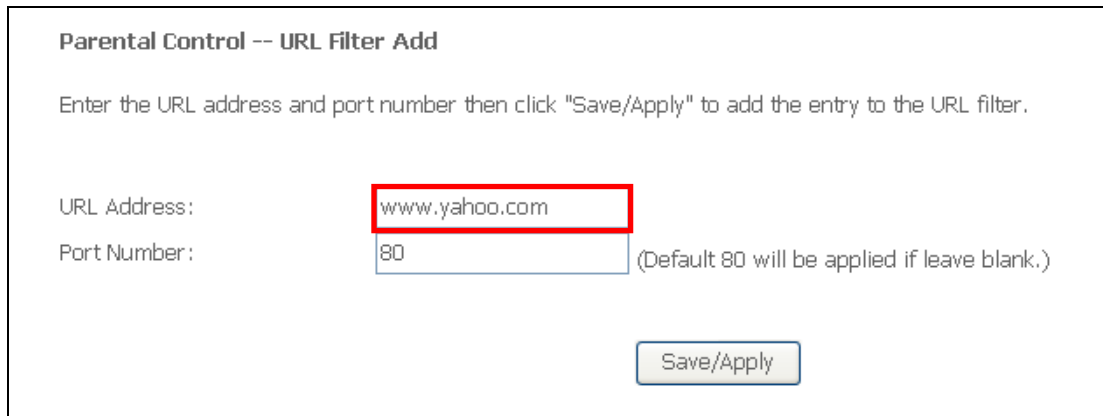
The screenshot shows the COMTREND web interface. At the top, there is a navigation menu with icons and labels: Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with options: WAN Setup, NAT, LAN, Wireless, Parental Control, Time Restriction, and **URL Filter**. The main content area is titled "URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured." Below this, there are two radio buttons for "URL List Type": "Exclude" (selected) and "Include". At the bottom of the main area, there are two buttons: "Add" and "Remove".

Select URL List Type: Exclude or Include.

Tick the **Exclude** radio button to deny access to the websites listed.

Tick the **Include** radio button to restrict access to only those listed websites.

Then click **Add** to display the following screen.



The screenshot shows the "Parental Control -- URL Filter Add" form. It contains the following text: "Enter the URL address and port number then click 'Save/Apply' to add the entry to the URL filter." Below this, there are two input fields: "URL Address:" with the value "www.yahoo.com" (highlighted with a red box) and "Port Number:" with the value "80". A note next to the port number field says "(Default 80 will be applied if leave blank.)". At the bottom right, there is a "Save/Apply" button.

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

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

URL List Type: Exclude Include

Address	Port	Remove
www.yahoo.com	80	<input type="checkbox"/>

Add

Remove

A maximum of 100 entries can be added to the URL Filter list.

5.6 Home Networking

5.6.1 Print Server

This page allows you to enable or disable printer support.



Please reference [Appendix G](#) to see the procedure for enabling the Printer Server.

5.6.2 DLNA

Enabling DLNA allows users to share digital media, like pictures, music and video, to other LAN devices from the digital media server.

Insert USB drive to the USB host port on the back of router. Modify media library path to the corresponding path of the USB drive and click Apply/Save to enable the DLNA media server.



The screenshot displays the Comtrend router's web management interface. At the top left is the Comtrend logo. A navigation bar contains icons and labels for: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists various settings categories: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server, DLNA (highlighted in blue), and Storage Service. The main content area is titled "Digital Media Server settings" and contains the text: "This page allows you to enable / disable digital media server support." Below this text is a single checkbox labeled "Enable on-board digital media server." which is currently unchecked. An "Apply/Save" button is located at the bottom right of the settings area.

5.6.3 Storage Service

This page displays storage devices attached to USB host.



Display after storage device attached (for your reference).

Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	30517 MB	19419 MB	Safely remove

Chapter 6 Advanced Setup

You can reach this page by clicking on the following icon located at the top of the screen.




6.1 Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications.



The Auto Detection page simply provides a checkbox allowing users to enable or disable the feature. Check the checkbox to display the following configuration options.



Auto-Detection

Security
Quality of Service
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.

Enable auto-detect

Auto-detection status: Waiting for DSL or Ethernet line connect

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Select a LAN-as-WAN Ethernet port for auto-detect:

Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order. A maximum 7 entries can be configured.

Select Service:

VPI[0-255]	VCI[32-65535]	Service	Option
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Disable"/>	<input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension
<input type="text" value="0"/>	<input type="text" value="32"/>	<input type="text" value="Default Bridge"/>	

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Enter the PPP username/password given by your service provider for PPP service detection.

Select a LAN-as-WAN Ethernet port for auto-detect:

Select the Ethernet Port that will be used as ETHWAN during auto-detection.

Select Service ATM ▾

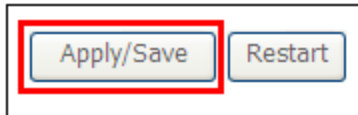
VPI[0-255]	VCI[32-65535]	Service
0	32	Disable ▾
0	32	PPPoE
0	32	PPPoA
0	32	IPoE
0	32	Disable
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Disable ▾
0	32	Default Bridge ▾

WAN services list for ATM mode: A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement and also reduce the detection cycle.

Select Service PTM/ETHWAN ▾

VLAN ID[0-4094]	Service
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Disable ▾
-1	Default Bridge ▾

WAN services list for PTM mode: A maximum of 7 WAN services with corresponding VLAN ID (-1 indicates no VLAN ID is required for the service) are required to be configured for ADSL/VDSL PTM mode and ETHWAN. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of the services to meet their own requirement and also reduce the detection cycle.



Click "Apply/Save" to activate the auto-detect function.

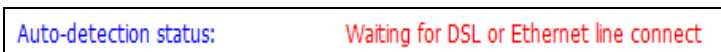
Options for each WAN service: These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

VPI[0-255]	VCI[32-65535]	Service	Option
0	33	PPPoE	<input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

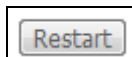
VLAN ID[0-4094]	Service	Option
8	PPPoE	<input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

Auto Detection status and Restart

The Auto-detection status is used to display the real time status of the Auto-detection feature.



The **Restart** button is used to detect all the WAN services that are either detected by the auto-detection feature or configured manually by users.



The following window will pop up upon clicking the **Restart** button. Click the **OK** button to proceed.



Auto Detection notice

Note: The following description concerning ETHWAN is for multiple LAN port devices only.

- 1) This feature will automatically detect one WAN service only. If customers require multiple WAN services, manual configuration is required.
- 2) If a physical ETHWAN port is detected, the Auto Detection for ETHWAN will be fixed on the physical ETHWAN port and cannot be configured for any LAN port; if the physical ETHWAN port is not detected, the Auto Detection for ETHWAN will be configured to the 4th LAN port by default and allows it to be configured for any LAN port as well.
- 3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
- 4) If none of the pre-configured services are detected, a Bridge service will be created.

6.2 Security

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

6.2.1 IP Filtering

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

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

OUTGOING IP FILTER

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



The screenshot shows the Comtrend web interface for configuring outgoing IP filters. The top navigation bar includes the Comtrend logo and menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various settings: Auto-Detection, Security (with IP Filtering expanded to show Outgoing and Incoming), MAC Filtering, Quality of Service, Routing, and DNS. The main content area is titled "Outgoing IP Filtering Setup" and contains the following text:

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

At the bottom of the table area, there are two buttons: "Add" and "Remove".

To add a filter (to block some outgoing IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

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

To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
IP Filtering
 Outgoing
Incoming
 MAC Filtering
Quality of Service
 Routing
 DNS
 DSL
 Interface Grouping
 IP Tunnel
 Certificate
 Power Management
 Multicast
 Wireless

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 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Policy:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All br0/br0

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	Permit/Drop packets specified by the firewall rule.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

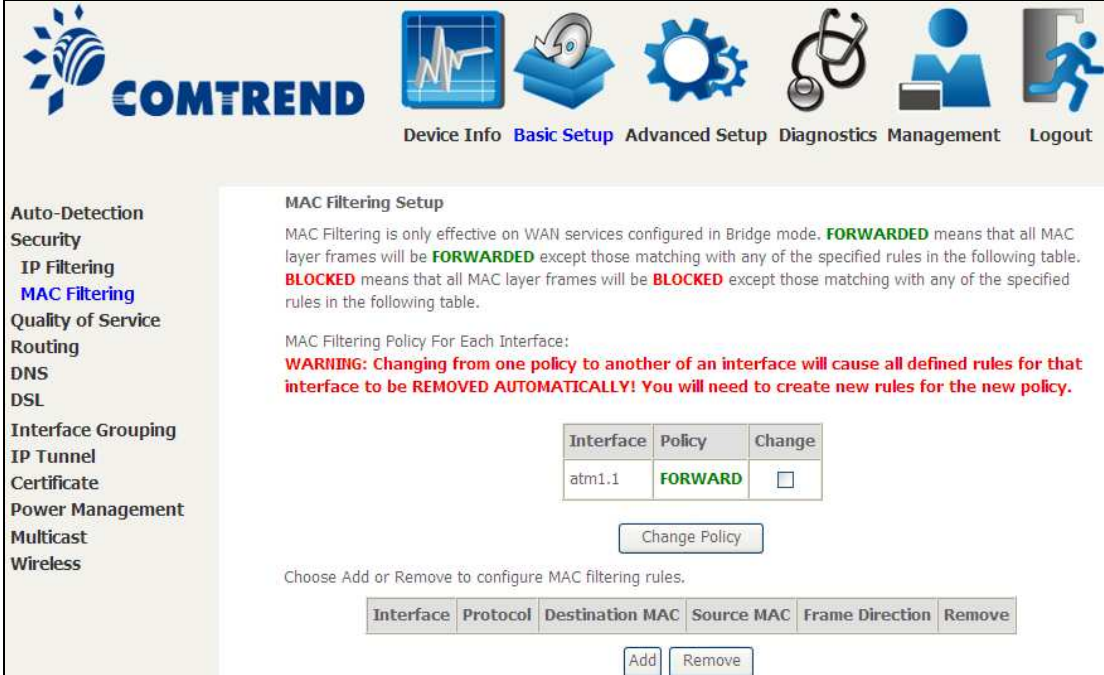
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

6.2.2 MAC Filtering

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

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the AR-5312u can be set according to the following procedure.

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



The screenshot shows the Comtrend web interface for MAC Filtering Setup. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various settings: Auto-Detection, Security, IP Filtering, MAC Filtering, Quality of Service, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled "MAC Filtering Setup" and contains the following text:

MAC Filtering is only effective on WAN services 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.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm1.1	FORWARD	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	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.

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

Consult the table below for detailed field descriptions.

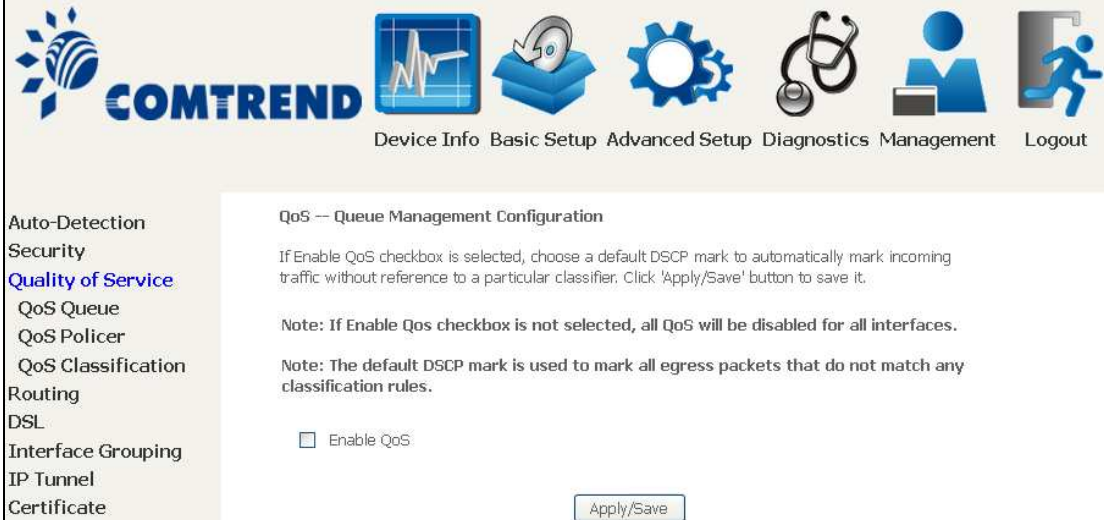
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected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

6.3 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(See [Appendix E - Connection Setup](#) for detailed PVC setup instructions).

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

Click Apply/Save to activate QoS.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different sections: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with the following items: Auto-Detection, Security, Quality of Service (highlighted), QoS Queue, QoS Policer, QoS Classification, Routing, DSL, Interface Grouping, IP Tunnel, and Certificate. The main content area is titled "QoS -- Queue Management Configuration". It contains the following text: "If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it." Below this, there are two notes: "Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces." and "Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules." At the bottom of the main content area, there is a checkbox labeled "Enable QoS" which is currently unchecked. To the right of the checkbox is an "Apply/Save" button.

QoS and DSCP Mark are defined as follows:

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

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

6.3.1 QoS Queue Setup

Configure queues with different priorities to be used for QoS setup.

In ATM mode, maximum 16 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 3 queues can be configured.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 3 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate (bits/s)	Burst Size (bytes)	Enable	Remove
WMM Voice Priority	1	wl0	1	1/SP					Enabled	
WMM Voice Priority	2	wl0	2	2/SP					Enabled	
WMM Video Priority	3	wl0	3	3/SP					Enabled	
WMM Video Priority	4	wl0	4	4/SP					Enabled	
WMM Best Effort	5	wl0	5	5/SP					Enabled	
WMM Background	6	wl0	6	6/SP					Enabled	
WMM Background	7	wl0	7	7/SP					Enabled	
WMM Best Effort	8	wl0	8	8/SP					Enabled	

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

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

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Interface Grouping

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

Click **Apply/Save** to apply and save the settings.

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

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

6.3.2 QoS Policer

To remove policers, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the policer after page reload.

Auto-Detection
Security
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

QoS Policer Setup -- maximum 32 policers can be configured.

To add a policer, click the **Add** button.
To remove policers, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the policer after page reload.

The QoS function has been disabled. Policers would not take effects.

Name	Key	MeteringType	Committed Rate (kbps)	Committed BurstSize (bytes)	Excess BurstSize (bytes)	Peak Rate (kbps)	Peak BurstSize (bytes)	Conform Action	PartialConform Action	NonConform Action	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>												

To add a policer, click the **Add** button.

Auto-Detection
Security
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

QoS Policer Configuration

This screen allows you to configure a QoS policer.
Click 'Apply/Save' to save the policer.

Notes:
--For TwoRateThreeColor policer, Peak Rate shall be higher than Committed Rate.
--CBS and EBS shall be minimally larger than the size of the largest possible IP packet in the stream.
--PBS shall be minimally larger than CBS by the size of the largest possible IP packet in the stream.

Name:

Enable:

Meter Type:

Committed Rate (kbps):

Committed Burst Size (bytes):

Conforming Action:

Nonconforming Action:

Click **Apply/Save** to save the policer.

Field	Description
Name	Name of this policer rule
Enable	Enable/Disable this policer rule
Meter Type	Meter type used for this policer rule
Committed Rate (kbps)	Defines the rate allowed for committed packets
Committed Burst Size (bytes)	Maximum amount of packets that can be processed by this policer
Conforming Action	Defines action to be taken if packets match this policer
Nonconforming Action	Defines actions to be taken if packets do not match this policer

6.3.3 QoS Classification

The network traffic classes are listed in the following table.

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

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

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

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Specify Class Queue	Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.
Specify Class Policer	Packets classified into a policer will be marked based on the conforming action of the policer
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7.
Set Rate Limit	The data transmission rate limit in kbps.

6.4 Routing

The following routing functions are accessed from this menu:

Default Gateway, Static Route, Policy Routing, RIP and IPv6 Static Route.

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

6.4.1 Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different system functions: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, a sidebar on the left lists various configuration categories, with 'Routing' selected and 'Default Gateway' highlighted. The main content area is titled 'Routing -- Default Gateway' and contains the following text: 'Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.' Below this text, there are two empty boxes labeled 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces', with arrows between them for moving items. A 'TODO' message states: 'TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.' At the bottom, there is a dropdown menu for 'Selected WAN Interface' currently set to 'NO CONFIGURED INTERFACE' and an 'Apply/Save' button.

6.4.2 Static Route

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



COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing


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

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

Add Remove

After clicking **Add** the following will display.



COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
DSL
Interface Grouping
IP Tunnel

Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Apply/Save

- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After completing the settings, click **Apply/Save** to add the entry to the routing table.

6.4.3 Policy Routing

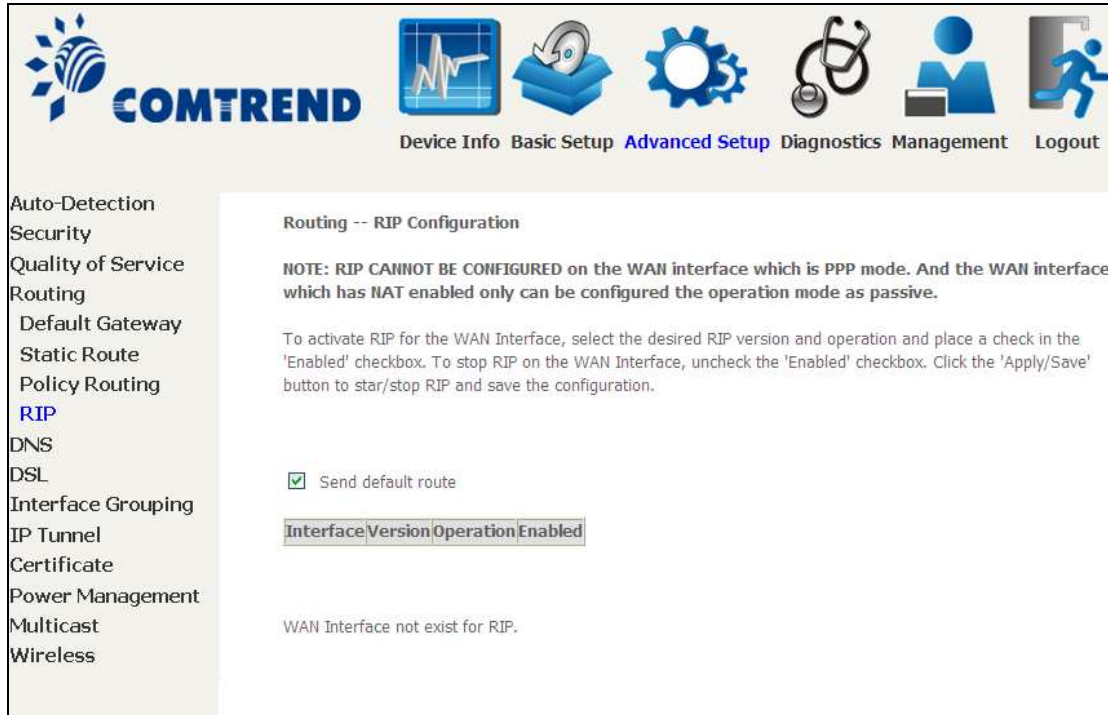
This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.

On the following screen, complete the form and click **Apply/Save** to create a policy.

Field	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway

6.4.4 RIP

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



COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
DSL
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Send default route

Interface	Version	Operation	Enabled
-----------	---------	-----------	---------

WAN Interface not exist for RIP.