

AR-5313u, AR-5310u

Wireless ADSL2+ Router

User Manual



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](#).

FCC & ISED

User Information

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

This device complies with Part 15 of the FCC Rules and Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada. Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s).

Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

Radiation Exposure

FCC ID : L9VAR5313U

IC : 4013C-AR5313U

US : 5SYDL01AAR5313U

REN: 0.1A

FCC

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

ISED

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps. Cet émetteur ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou transmetteur.

The REN statement is the following:

"The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five."

Copyright

Copyright©2016 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	8
CHAPTER 2 INSTALLATION	9
2.1 HARDWARE SETUP.....	9
2.2 FRONT PANEL.....	11
CHAPTER 3 WEB USER INTERFACE	13
3.1 DEFAULT SETTINGS.....	13
3.2 IP CONFIGURATION.....	13
3.3 LOGIN PROCEDURE.....	16
CHAPTER 4 DEVICE INFORMATION	18
4.1 WAN.....	19
4.2 STATISTICS.....	20
4.2.1 LAN Statistics.....	20
4.2.2 WAN Service.....	21
4.2.3 XTM Statistics.....	22
4.2.4 xDSL Statistics.....	23
4.3 ROUTE.....	28
4.4 ARP.....	29
4.5 DHCP.....	29
4.6 NAT SESSION.....	31
4.7 IGMP PROXY.....	32
4.8 IPV6.....	33
4.8.1 IPv6 Info.....	33
4.8.2 IPv6 Neighbor.....	34
4.8.3 IPv6 Route.....	35
4.9 NETWORK MAP.....	36
4.10 WIRELESS.....	37
4.10.1 Station Info.....	37
4.10.2 Site Survey.....	38
CHAPTER 5 BASIC SETUP	39
5.1 LAYER 2 INTERFACE.....	40
5.1.1 WAN Service Setup.....	41
5.2 NAT.....	42
5.2.1 Virtual Servers.....	42
5.2.2 Port Triggering.....	43
5.2.3 DMZ Host.....	46
5.2.4 IP Address Map.....	47
5.2.5 IPSEC ALG.....	48
5.2.6 SIP ALG.....	49
5.3 LAN.....	50
5.3.1 LAN IPv6 Autoconfig.....	53
5.3.2 Static IP Neighbor.....	56
5.3.3 UPnP.....	57
5.4 WIRELESS.....	58
5.4.1 Basic.....	58
5.4.2 Security.....	60
5.5 PARENTAL CONTROL.....	63
5.5.1 Time Restriction.....	63
5.5.2 URL Filter.....	64
5.6 HOME NETWORKING	66
5.6.1 Print Server.....	66
5.6.2 DLNA.....	67
5.6.3 Storage Service.....	68

CHAPTER 6 ADVANCED SETUP	69
6.1 AUTO-DETECTION SETUP	69
6.2 SECURITY	74
6.2.1 IP Filtering	74
6.2.2 MAC Filtering	77
6.3 QUALITY OF SERVICE (QOS)	79
6.3.1 QoS Queue Setup	80
6.3.2 QoS Policer	82
6.3.3 QoS Classification	84
6.4 ROUTING	86
6.4.1 Default Gateway	86
6.4.2 Static Route	87
6.4.3 Policy Routing	88
6.4.4 RIP	89
6.5 DNS	90
6.5.1 DNS Server	90
6.5.2 Dynamic DNS	91
6.5.3 DNS Entries	92
6.5.4 DNS Proxy/Relay	93
6.6 DSL	94
6.7 INTERFACE GROUPING	96
6.8 IP TUNNEL	99
6.8.1 IPv6inIPv4	99
6.8.2 IPv4inIPv6	100
6.9 CERTIFICATE	101
6.9.1 Local	101
6.9.2 Trusted CA	104
6.10 POWER MANAGEMENT	105
6.11 MULTICAST	106
6.12 WIRELESS	108
6.12.1 Basic	108
6.12.2 Security	110
6.12.3 WPS	113
6.12.4 MAC Filter	116
6.12.5 Wireless Bridge	118
6.12.6 Advanced	119
CHAPTER 7 DIAGNOSTICS	122
7.1 DIAGNOSTICS – INDIVIDUAL TESTS	122
7.2 FAULT MANAGEMENT	123
7.3 UPTIME STATUS	124
7.4 PING	125
7.5 TRACE ROUTE	126
7.6 SYSTEM UTILIZATION	127
CHAPTER 8 MANAGEMENT	128
8.1 SETTINGS	128
8.1.1 Backup Settings	128
8.1.2 Update Settings	129
8.1.3 Restore Default	129
8.2 SYSTEM LOG	131
8.3 SNMP AGENT	133
8.4 TR-069 CLIENT	134
8.5 INTERNET TIME	136
8.6 ACCESS CONTROL	137
8.6.1 Accounts	137
8.6.2 Service Access	139
8.6.3 IP Address	140
8.7 UPDATE SOFTWARE	141

8.8 REBOOT	142
CHAPTER 9 LOGOUT	143
APPENDIX A - FIREWALL.....	144
APPENDIX B - PIN ASSIGNMENTS	147
APPENDIX C – SPECIFICATIONS	148
APPENDIX D - SSH CLIENT.....	150
APPENDIX E - CONNECTION SETUP	151
APPENDIX F – PRINTER SERVER.....	203

Chapter 1 Introduction

AR-5313u 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-5313u 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.

Chapter 2 Installation

2.1 Hardware Setup



DO NOT STACK

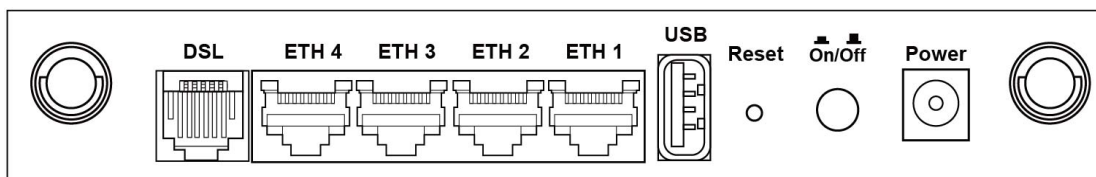
Non-stackable

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 F](#) 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-5313u 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:

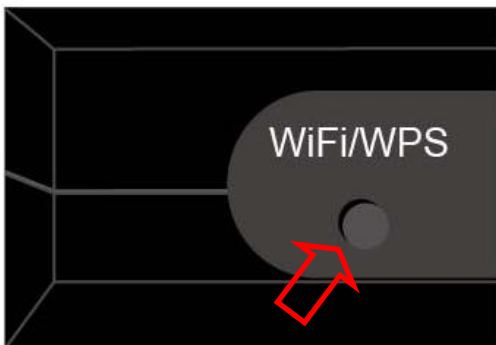
A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such as after power on or during operation through the use of self testing or in operations which result in a unit state 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 10 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 ten 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-5313u 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.

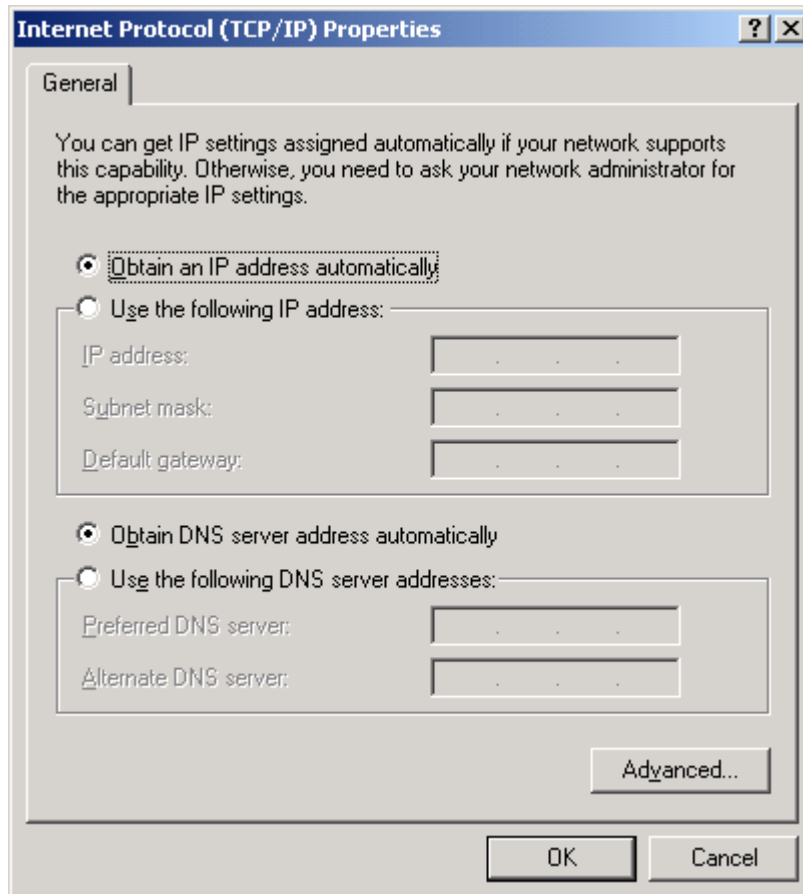
To obtain an IP address from the DHCP server, follow the steps provided below.

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

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.

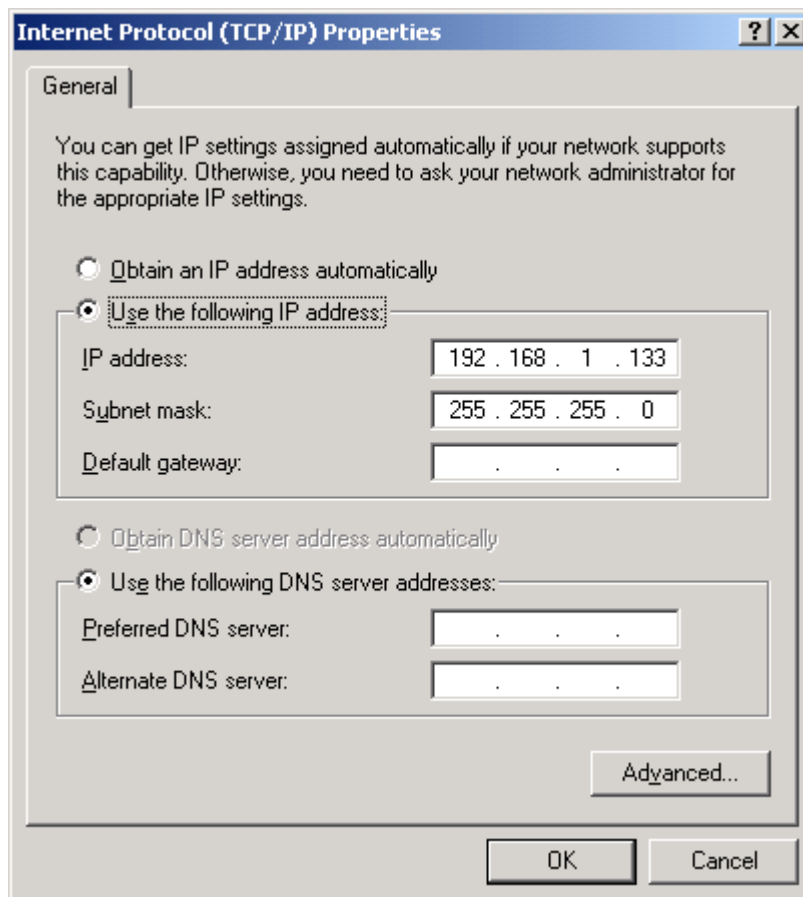
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE: The following procedure assumes you are running Windows. 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 Accounts](#)).

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



[Device Info](#)
[Basic Setup](#)
[Advanced Setup](#)
[Diagnostics](#)
[Management](#)
[Logout](#)

Summary

WAN

Statistics

Route

ARP

DHCP

NAT Session

IGMP Proxy

IPv6


Network Map

Wireless





Device

Model	AR-5313u
Board ID	96318AT-1441N1
Serial Number	1555313JXXF-AA000006
Firmware Version	SE31-412CTU-C01_R01.A2pG039k.d25f
Bootloader (CFE) Version	1.0.38-112.118-46
Up Time	4 mins:19 secs

Wireless


Driver Version	6.30.102.7.cpe4.12L06B.1
Primary SSID	Comtrend0308
Status	Enabled
Channel	1
	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key	•••••••• <input type="button" value="Show"/>

LAN

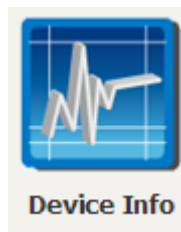
LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:00:03:08
DHCP Server	Enabled
LAN IPv6 ULA Address	

WAN



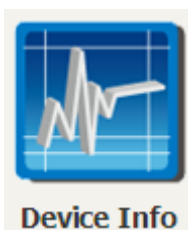
DOWN

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.

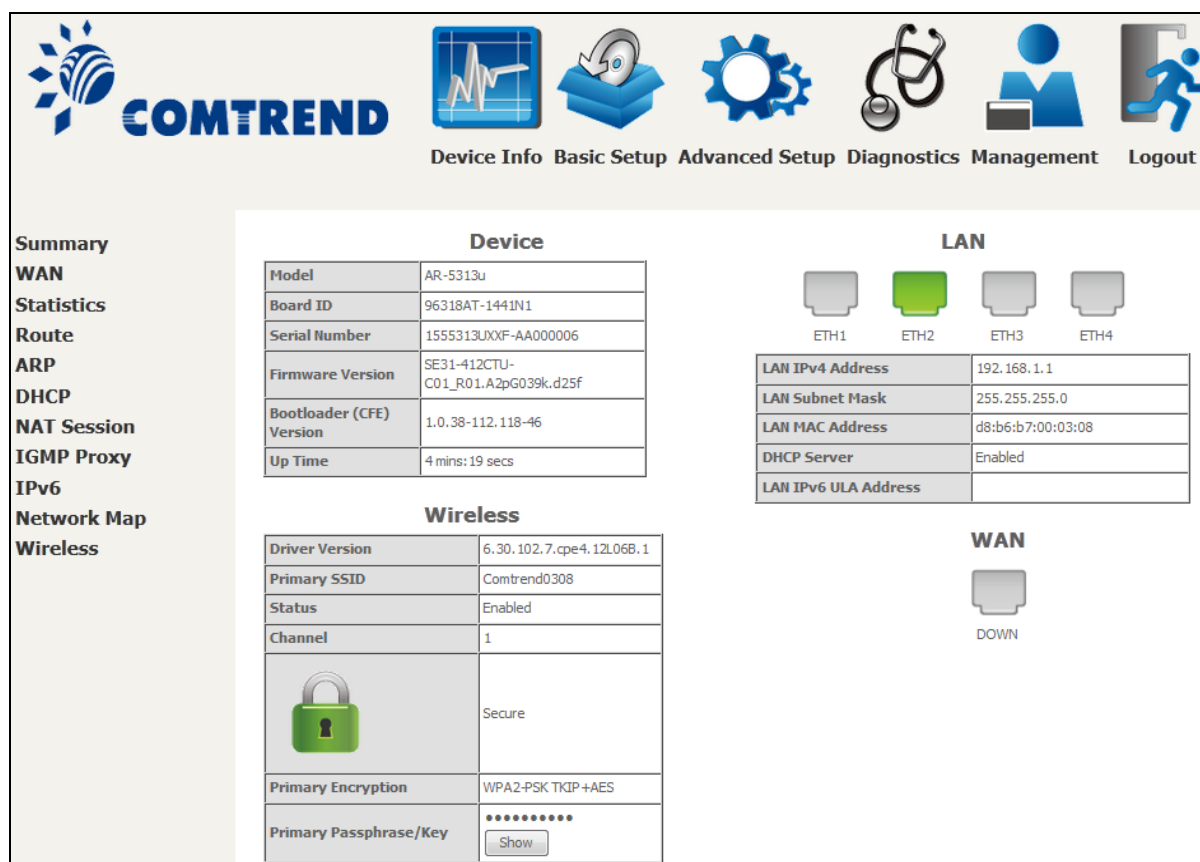


The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

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.



Summary

- WAN
- Statistics
- Route
- ARP
- DHCP
- NAT Session
- IGMP Proxy
- IPv6
- Network Map
- Wireless

Device

Model	AR-5313u
Board ID	96318AT-1441N1
Serial Number	1555313UXF-AA000006
Firmware Version	SE31-412CTU-C01_R01.A2pG039k.d25f
Bootloader (CFE) Version	1.0.38-112.118-46
Up Time	4 mins: 19 secs

LAN

LAN IPv4 Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
LAN MAC Address	d8:b6:b7:00:03:08
DHCP Server	Enabled
LAN IPv6 ULA Address	

Wireless

Driver Version	6.30.102.7.cpe4.12L06B.1
Primary SSID	Comtrend0308
Status	Enabled
Channel	1
Secure	Secure
Primary Encryption	WPA2-PSK TKIP+AES
Primary Passphrase/Key <input type="button" value="Show"/>

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).



WAN Info											
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	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

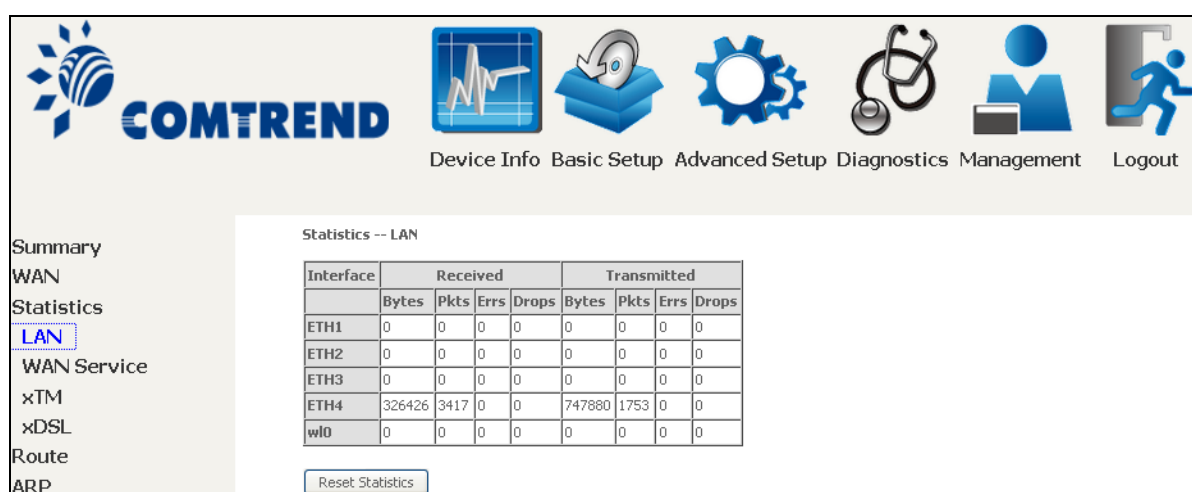
4.2 Statistics

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.

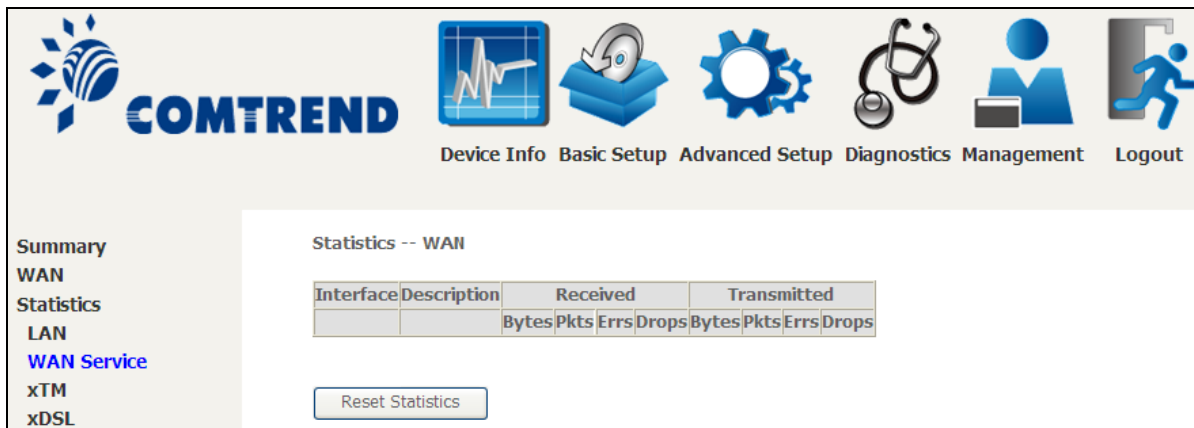


Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ETH1	0	0	0	0	0	0	0	0
ETH2	0	0	0	0	0	0	0	0
ETH3	0	0	0	0	0	0	0	0
ETH4	326426	3417	0	0	747880	1753	0	0
wl0	0	0	0	0	0	0	0	0

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

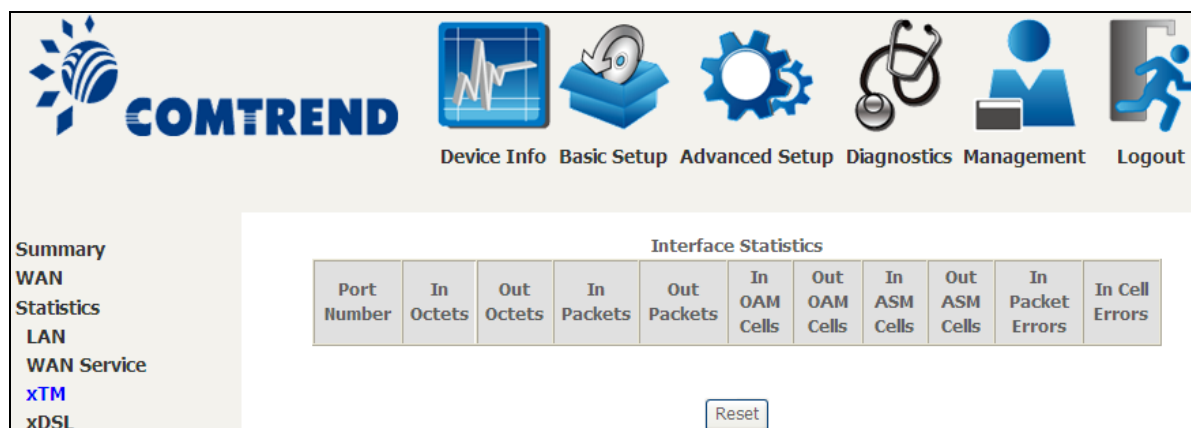
Statistics -- WAN

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

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

4.2.3 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



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
INP (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		

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:	LO			
	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	
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		

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

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

In VDSL mode, the following section is inserted.

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

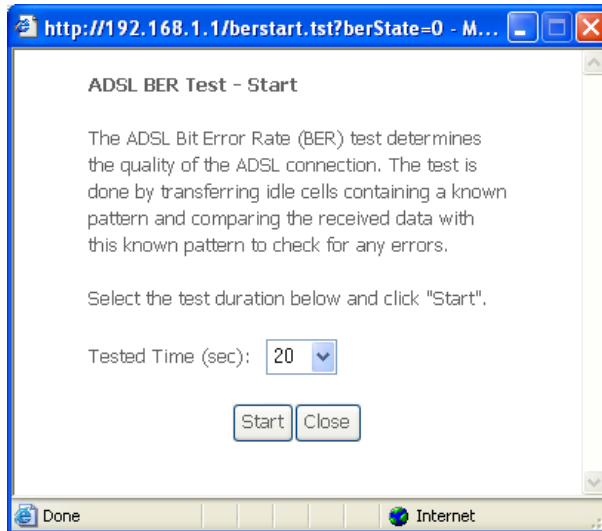
OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

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

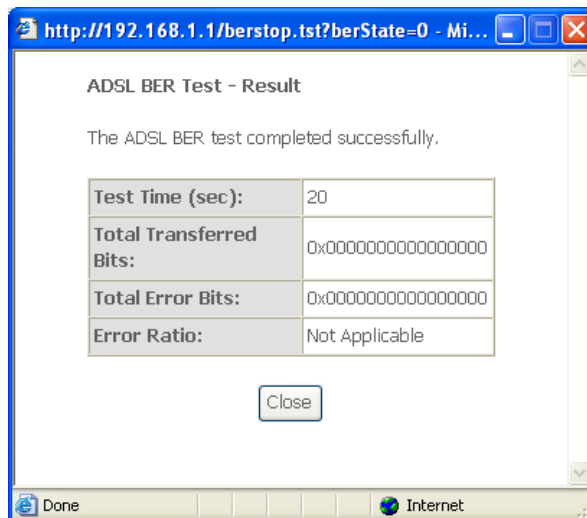
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

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.

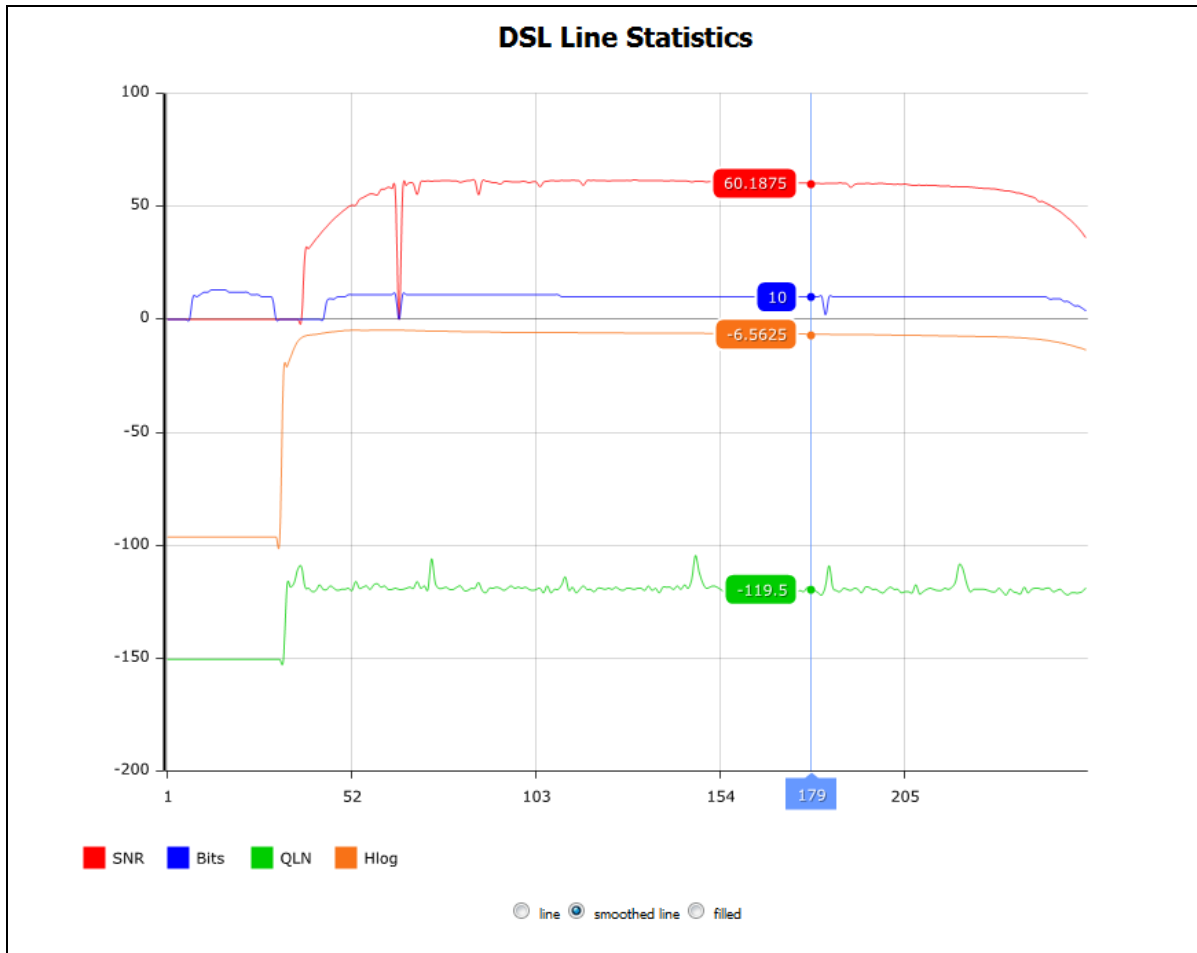


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



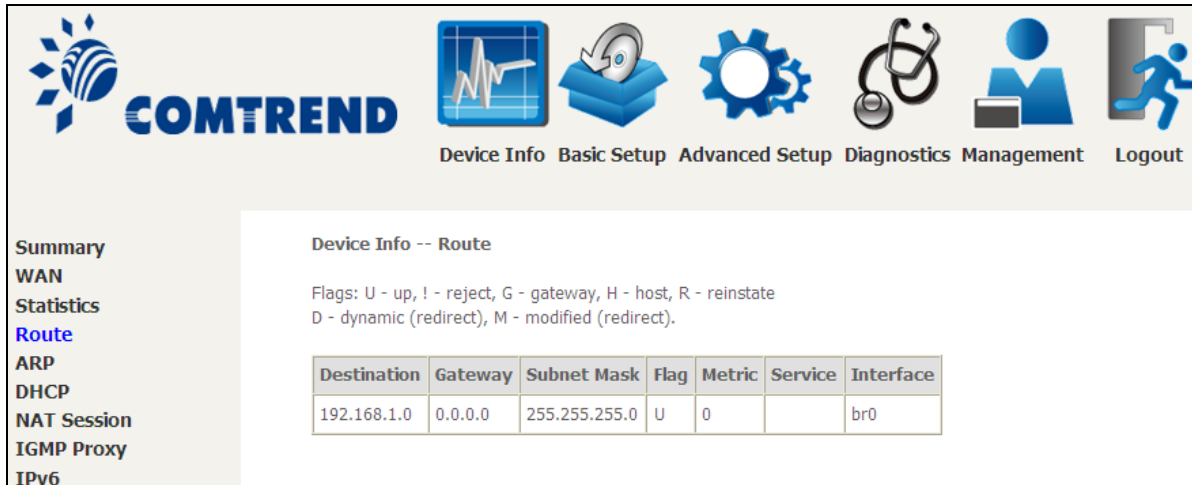
xDSL TONE GRAPH

Click **Draw 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-5313u 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.



Summary
WAN
Statistics
Route
ARP


Device Info -- ARP

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.



Summary
WAN
Statistics
Route
ARP
DHCP
DHCPv4
DHCPv6

Device Info -- DHCP Leases

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 -- 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

This page displays all NAT connection session including both UPD/TCP protocols passing through the device.



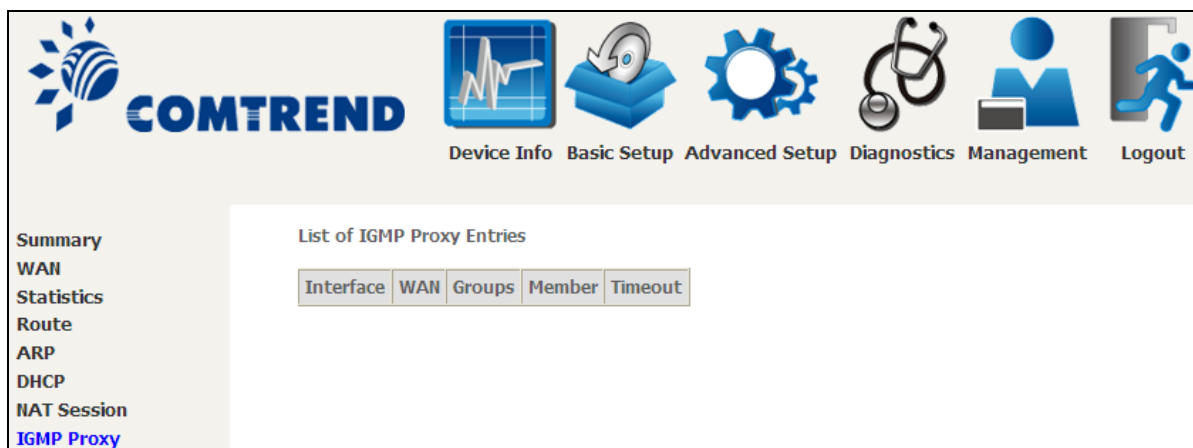
Click the "Show All" button to display the following.

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	53326	192.168.1.1	80	tcp	8
192.168.1.3	53327	192.168.1.1	80	tcp	431999
192.168.1.3	53321	192.168.1.1	80	tcp	7
192.168.1.3	53325	192.168.1.1	80	tcp	8
192.168.1.3	53322	192.168.1.1	80	tcp	7
192.168.1.3	53323	192.168.1.1	80	tcp	7
192.168.1.3	53324	192.168.1.1	80	tcp	8

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

Click **IGMP Proxy** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.

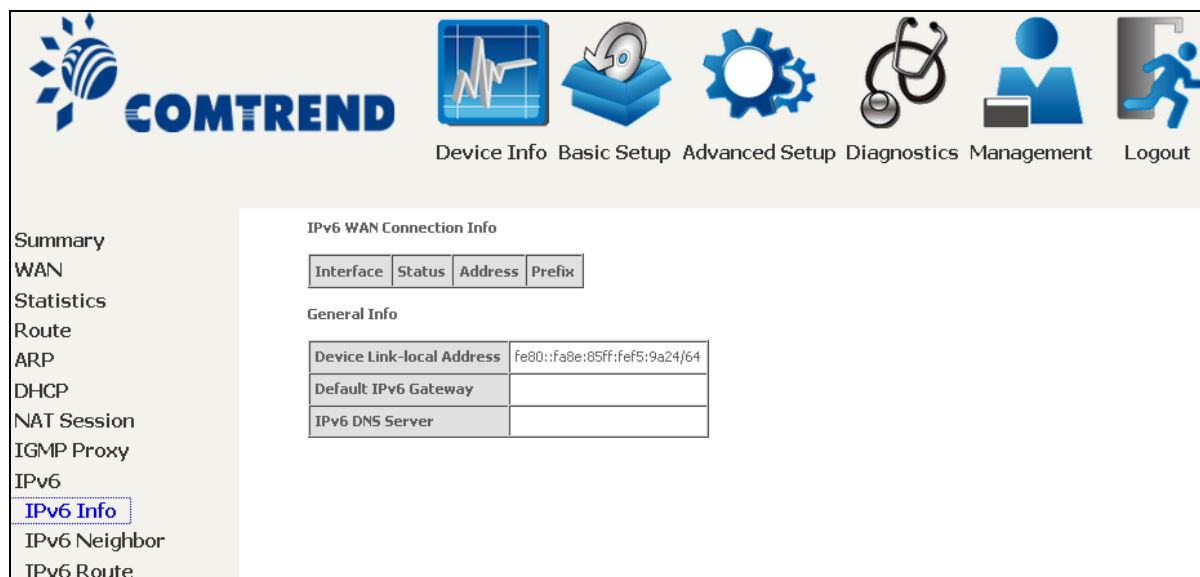


Field	Description
Interface	The Source interface from which the IGMP report was received
WAN	The WAN interface from which the multicast traffic is received
Groups	The destination IGMP group address
Member	The Source IP from which the IGMP report was received
Timeout	The time remaining before the IGMP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

4.8 IPv6

4.8.1 IPv6 Info

Click **IPv6 Info** to display the IPv6 WAN connection info.



Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6
IPv6 Info
IPv6 Neighbor
IPv6 Route

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

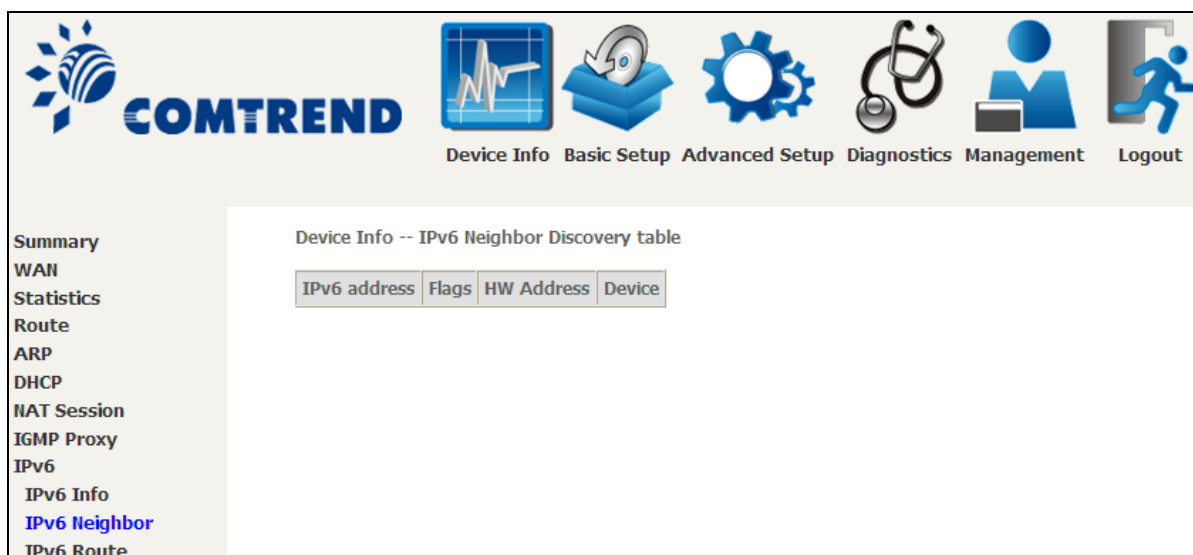
IPv6 WAN Connection Info

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

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

Click **IPv6 Neighbor** to display the list of IPv6 nodes discovered.

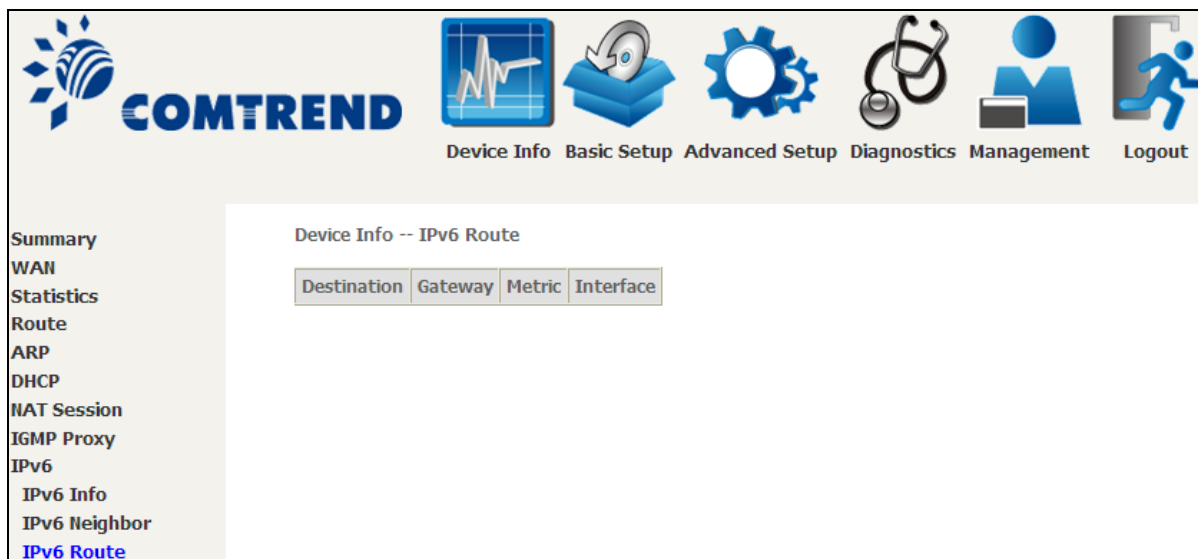


The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the following items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with the following items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, IPv6 Info, **IPv6 Neighbor**, and IPv6 Route. The main content area displays the title "Device Info -- IPv6 Neighbor Discovery table" and a table with the following 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

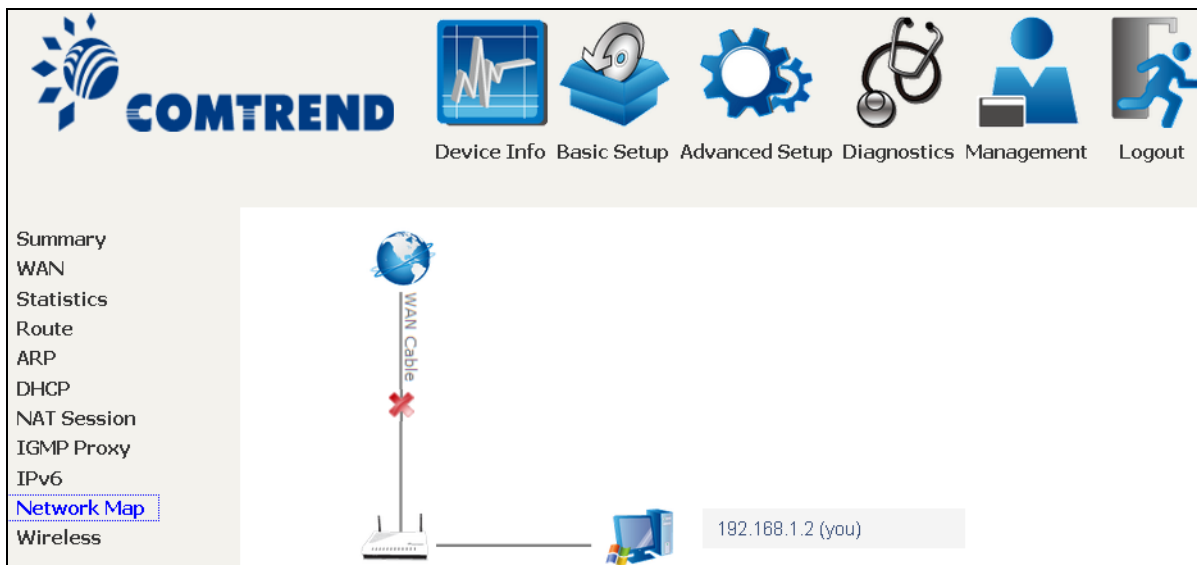
Click **IPv6 Route** to display the IPv6 route info.



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.

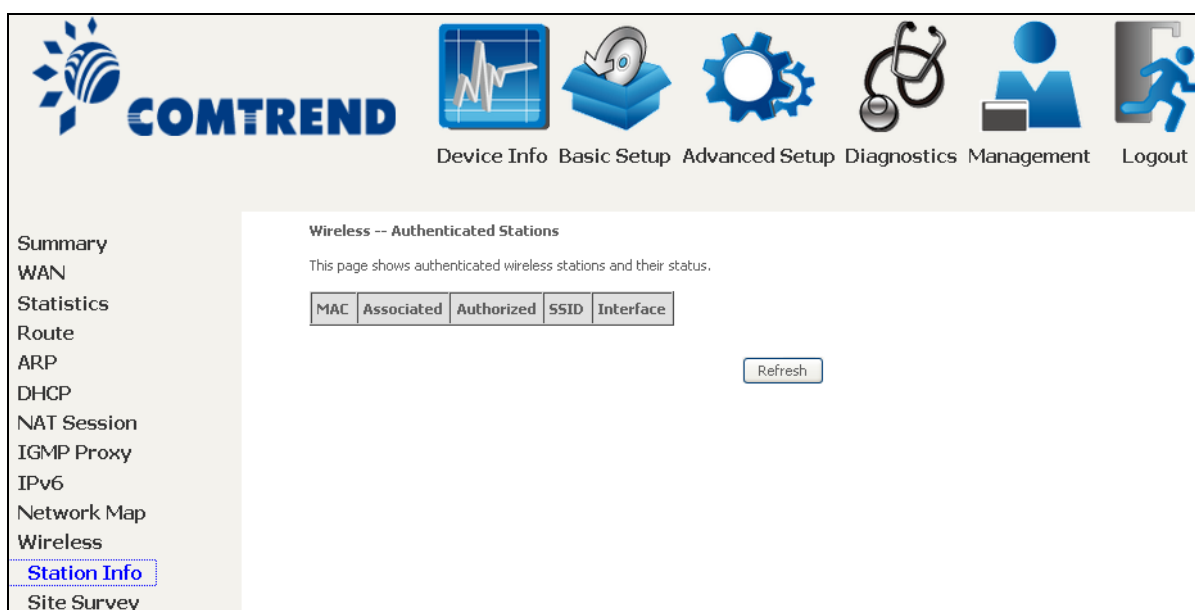


The screenshot displays the COMTREND web management interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, a sidebar on the left lists various configuration options: 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 vertical line labeled 'WAN Cable' which ends in a globe icon. A red 'X' is placed on the WAN Cable line, indicating a connection issue. A horizontal line connects the router to a laptop icon on the right, representing a LAN device. Next to the laptop icon, the IP address '192.168.1.2 (you)' is displayed in a light gray box.

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 on the left with a list of menu items: 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.

Note: This graph is unavailable for Internet Explorer users.



Summary

WAN

Statistics

Route

ARP

DHCP

NAT Session

IGMP Proxy

IPv6

Network Map

Wireless

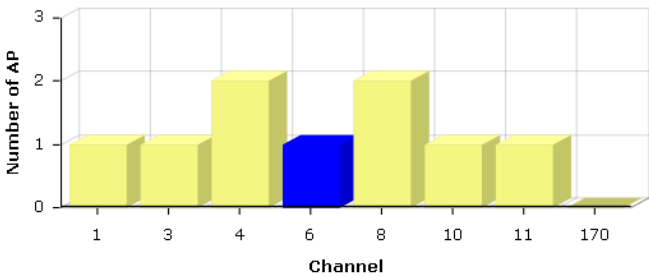
Station Info

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

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

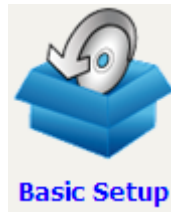
[Refresh](#)

38

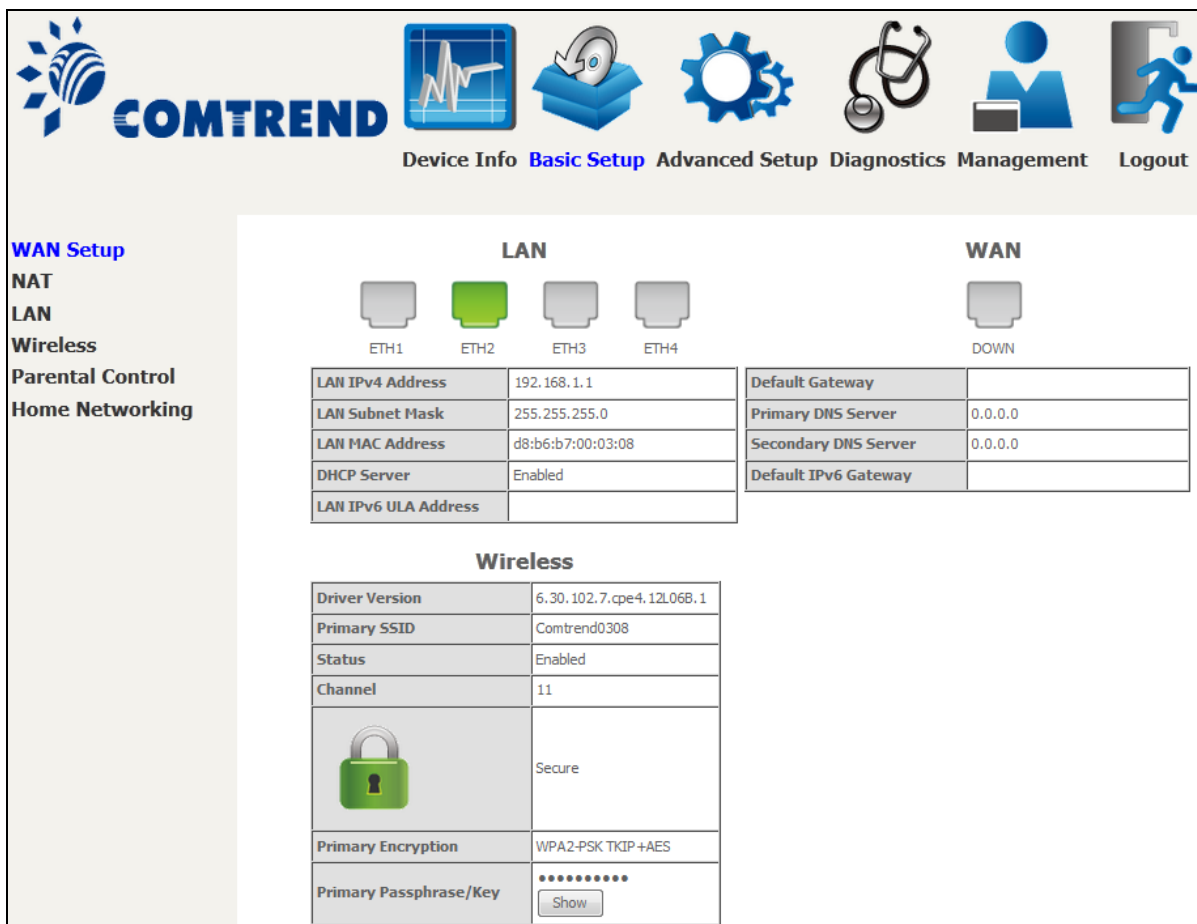
Leading the **Communication Trend**

Chapter 5 Basic Setup

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



This will bring you to the following screen.



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

WAN Setup
NAT
LAN
Wireless
 Parental Control
 Home Networking

LAN


ETH1 ETH2 ETH3 ETH4

LAN IPv4 Address	192.168.1.1	Default Gateway	
LAN Subnet Mask	255.255.255.0	Primary DNS Server	0.0.0.0
LAN MAC Address	d8:b6:b7:00:03:08	Secondary DNS Server	0.0.0.0
DHCP Server	Enabled	Default IPv6 Gateway	
LAN IPv6 ULA Address			

WAN

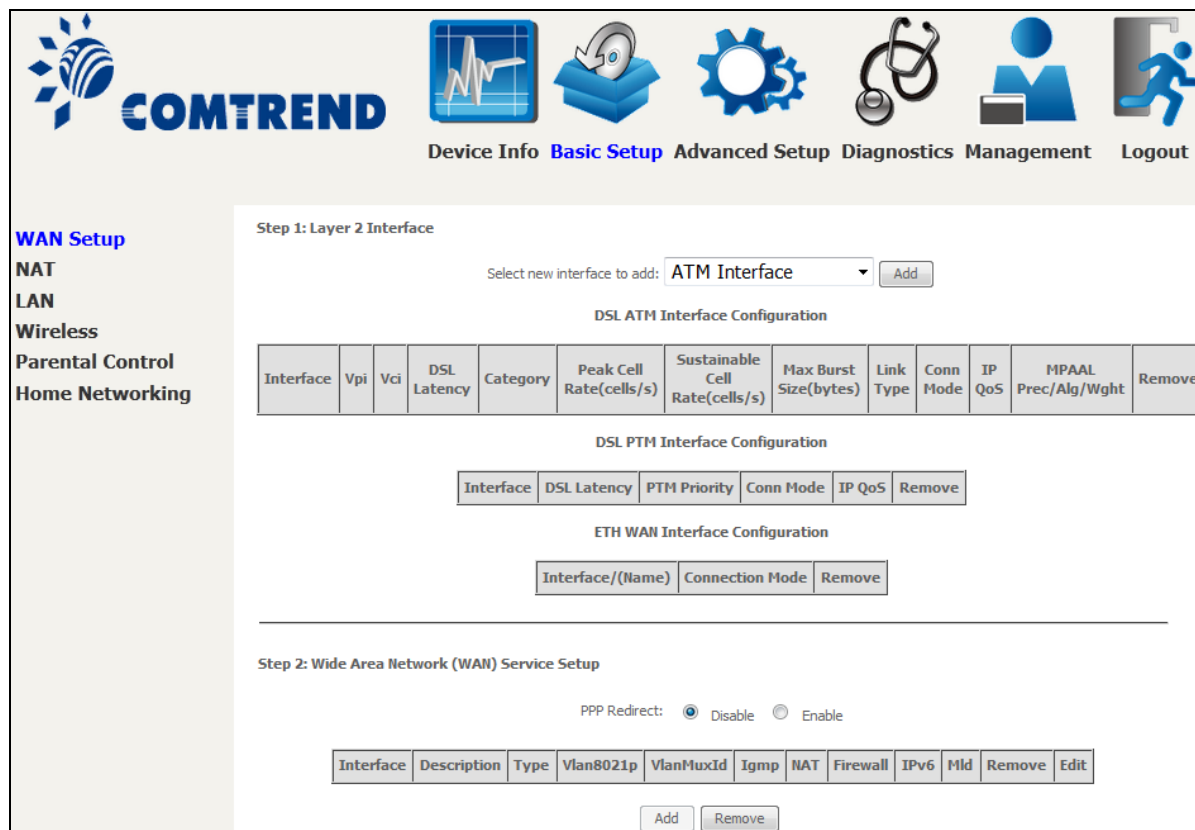
DOWN

Wireless

Driver Version	6.30.102.7.cpe4.12L06B.1
Primary SSID	Comtrend0308
Status	Enabled
Channel	11
	Secure
Primary Encryption	WPA2-PSK TKIP +AES
Primary Passphrase/Key	•••••••• <input type="button" value="Show"/>

5.1 Layer 2 Interface

Click WAN Setup on the on the left of your screen.
Add or remove ATM, PTM and ETH WAN interface connections here.



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

WAN Setup
NAT
LAN
Wireless
Parental Control
Home Networking

Step 1: Layer 2 Interface

Select new interface to add:

DSL ATM Interface Configuration

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
-----------	-----	-----	-------------	----------	-------------------------	--------------------------------	-----------------------	-----------	-----------	--------	---------------------	--------

DSL PTM Interface Configuration

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
-----------	-------------	--------------	-----------	--------	--------

ETH WAN Interface Configuration

Interface/(Name)	Connection Mode	Remove
------------------	-----------------	--------

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: Disable Enable

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	------	-----	--------	------

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
<div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div>											

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.

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 Service). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Service). 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 Service). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Service). 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.



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

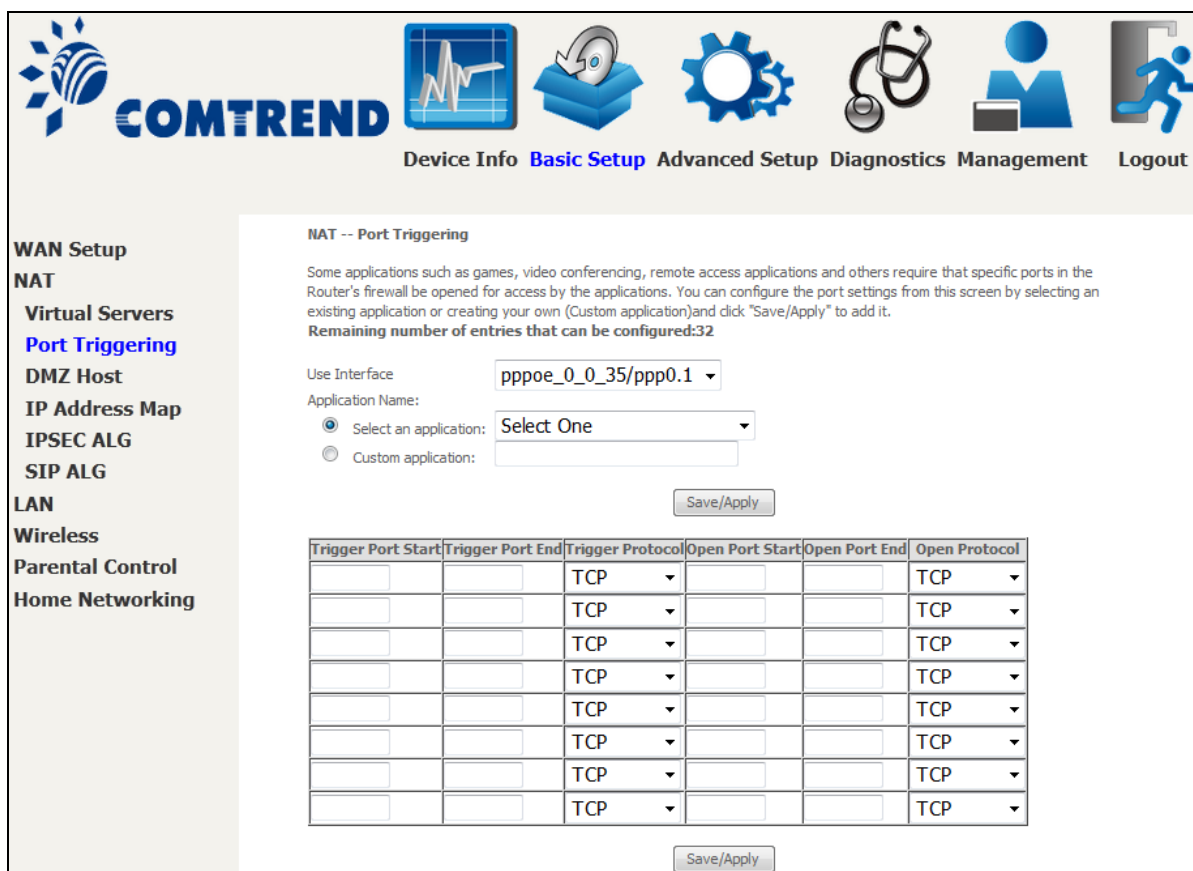
NAT -- Port Triggering Setup

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

Add Remove

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.



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.

Field/Header	Description
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.



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

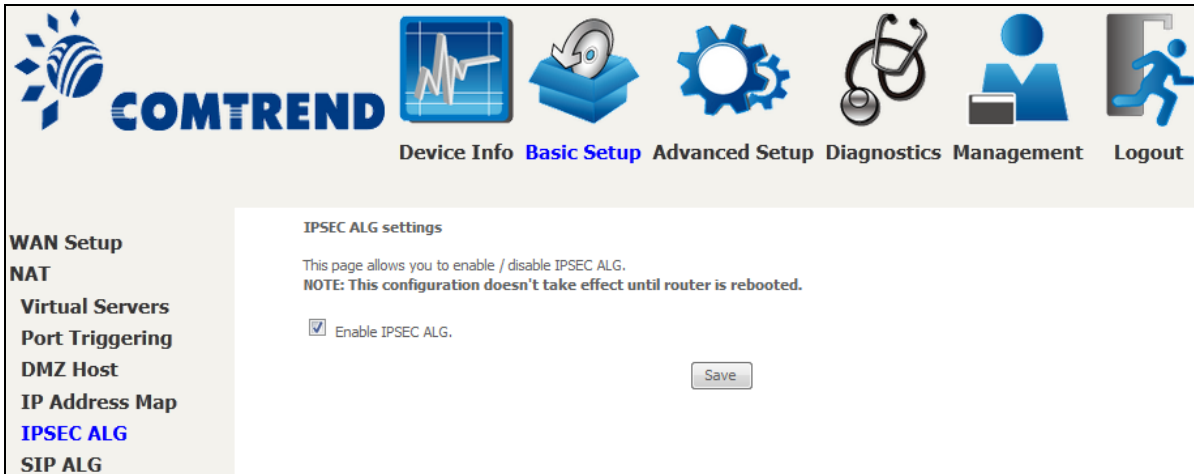
Many to one: mapping a range of local IP to a specific public IP

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.

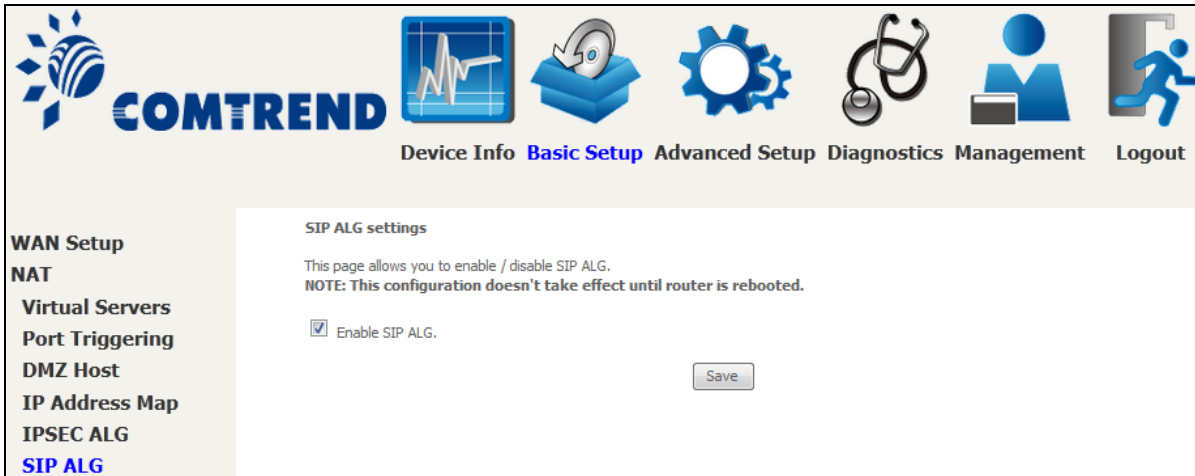


The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, the main content area is titled "IPSEC ALG settings". It contains the following text: "This page allows you to enable / disable IPSEC ALG." and "NOTE: This configuration doesn't take effect until router is rebooted." There is a checkbox labeled "Enable IPSEC ALG." which is checked. To the right of the checkbox is a "Save" button. On the left side of the interface, there is a sidebar menu with the following items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG (highlighted in blue), and SIP ALG.

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

5.2.6 SIP ALG

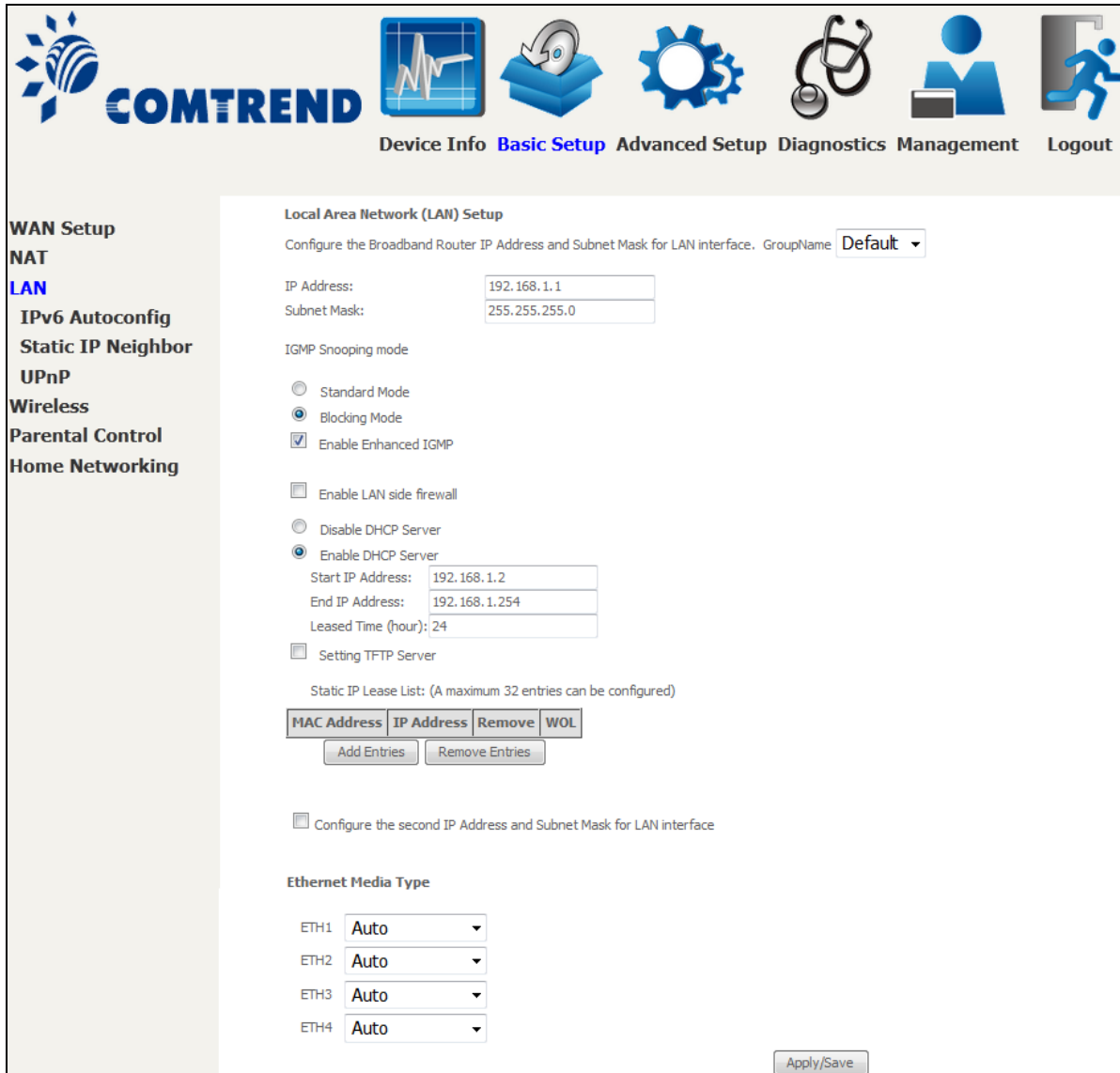
This page allows you to enable / disable SIP ALG.



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, the main content area is titled "SIP ALG settings". It contains the following text: "This page allows you to enable / disable SIP ALG." and "NOTE: This configuration doesn't take effect until router is rebooted." There is a checkbox labeled "Enable SIP ALG." which is checked. A "Save" button is located to the right of the checkbox. On the left side of the interface, there is a sidebar menu with the following items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG, and SIP ALG (highlighted in blue).

5.3 LAN

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



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

WAN Setup
NAT
LAN
 IPv6 Autoconfig
 Static IP Neighbor
 UPnP
 Wireless
 Parental Control
 Home Networking

Local Area Network (LAN) Setup
 Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName **Default** ▾

IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0

IGMP Snooping mode

Standard Mode
 Blocking Mode
 Enable Enhanced IGMP

Enable LAN side firewall

Disable DHCP Server
 Enable DHCP Server

Start IP Address: 192.168.1.2
 End IP Address: 192.168.1.254
 Leased Time (hour): 24

Setting TFTP Server

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

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

Configure the second IP Address and Subnet Mask for LAN interface

Ethernet Media Type

ETH1: Auto ▾
 ETH2: Auto ▾
 ETH3: Auto ▾
 ETH4: Auto ▾

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.

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

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

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

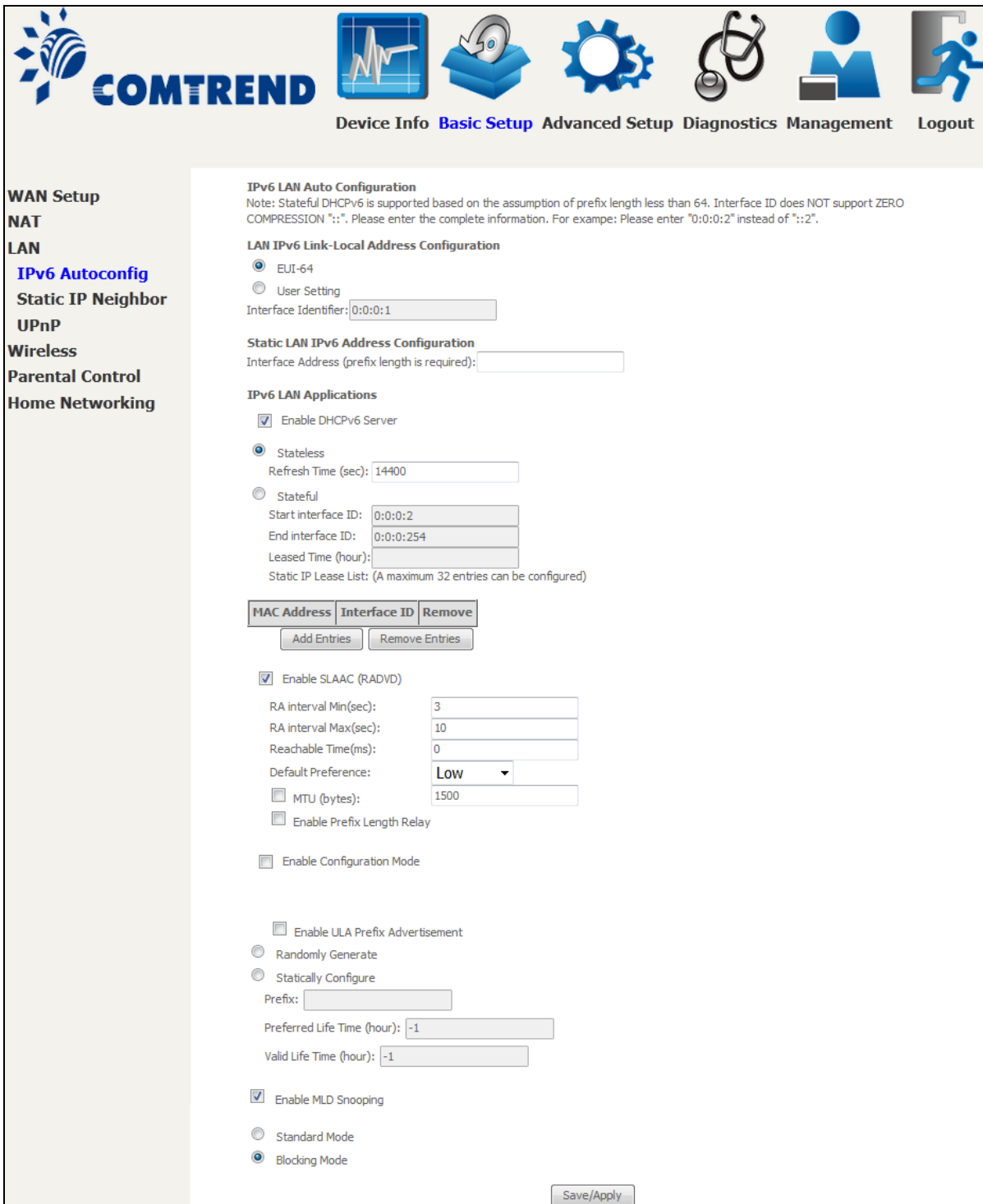
Ethernet Media Type: Configure auto negotiation, or enforce selected speed and duplex mode for the Ethernet ports.

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 displays the COMTREND web interface for IPv6 LAN Auto Configuration. The top navigation bar includes icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various configuration categories: WAN Setup, NAT, LAN (selected), IPv6 Autoconfig (selected), Static IP Neighbor, UPnP, Wireless, Parental Control, and Home Networking.

The main content area is titled "IPv6 LAN Auto Configuration" and includes a note: "Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION ":", Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2"."

The configuration options are as follows:

- IPv6 LAN Link-Local Address Configuration:**
 - EUI-64
 - User Setting
 - Interface Identifier:
- Static LAN IPv6 Address Configuration:**
 - Interface Address (prefix length is required):
- IPv6 LAN Applications:**
 - Enable DHCPv6 Server
 - Stateless
 - Refresh Time (sec):
 - Stateful
 - Start interface ID:
 - End interface ID:
 - Leased Time (hour):
 - Static IP Lease List: (A maximum 32 entries can be configured)
- Table:**

MAC Address	Interface ID	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		
- Enable SLAAC (RADVD)
 - RA interval Min(sec):
 - RA interval Max(sec):
 - Reachable Time(ms):
 - Default Preference:
 - MTU (bytes):
 - Enable Prefix Length Relay
- Enable Configuration Mode
- Enable ULA Prefix Advertisement
 - Randomly Generate
 - Statically Configure
 - Prefix:
 - Preferred Life Time (hour):
 - Valid Life Time (hour):
- Enable MLD Snooping
 - Standard Mode
 - Blocking Mode

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

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	Interface ID	Remove
<input type="button" value="Add Entries"/> <input type="button" value="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	Specify the prefix to be used
Prefix	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.

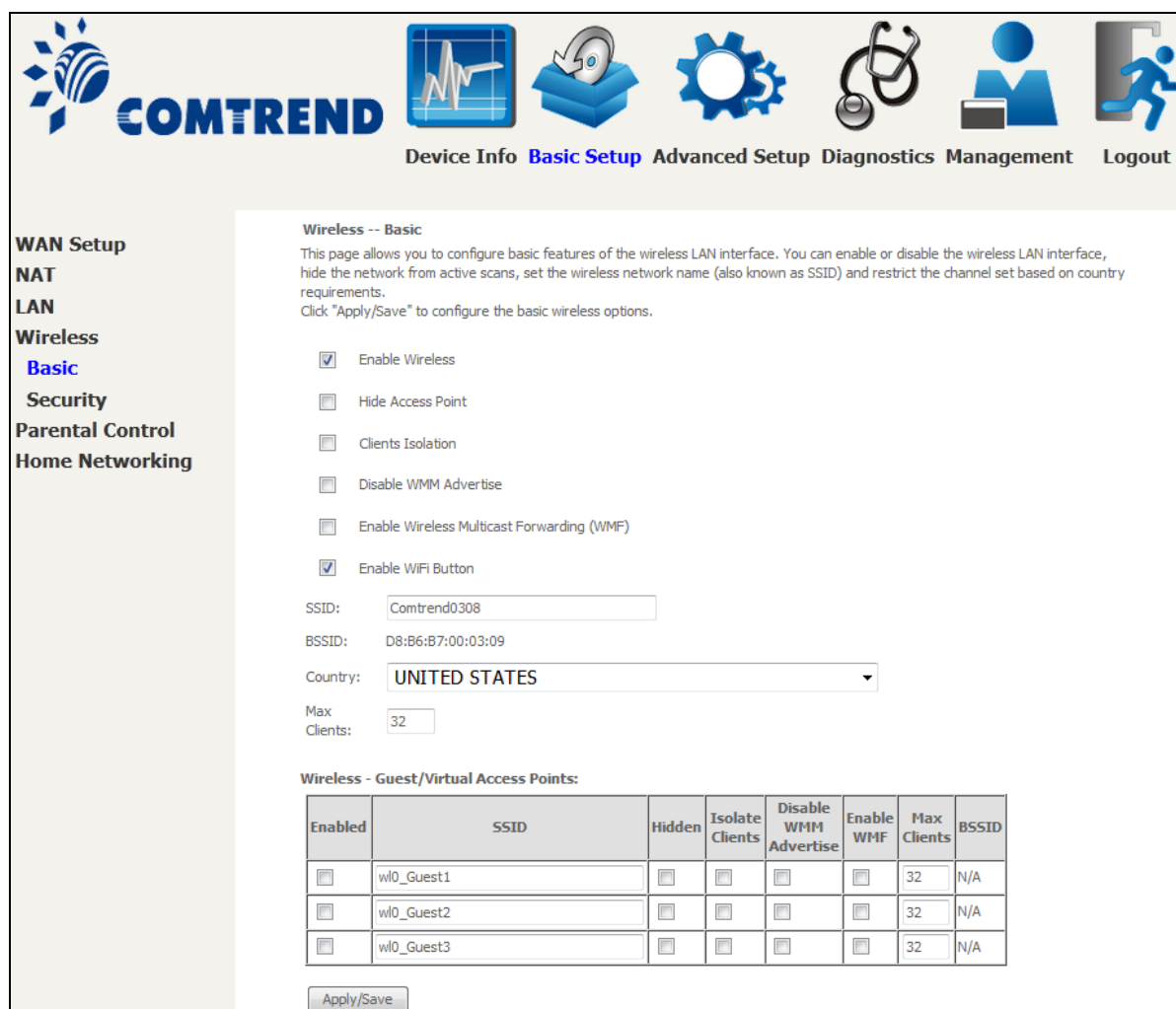


The screenshot displays the COMTREND web interface. At the top left is the COMTREND logo. A navigation bar contains icons and labels for: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists: WAN Setup, NAT, LAN, 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 checkbox labeled 'Enable UPnP' which is checked. At the bottom right of the main content 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 'Basic Setup' page for 'Wireless -- Basic'. The page includes a navigation bar with icons for Device Info, Basic Setup (selected), Advanced Setup, Diagnostics, Management, and Logout. A left sidebar lists menu items: WAN Setup, NAT, LAN, Wireless (selected), Security, Parental Control, and Home Networking. The main content area contains the following configuration options:

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

Below these are input fields for SSID (Combrend0308), BSSID (D8:B6:B7:00:03:09), a Country dropdown menu (UNITED STATES), and a Max Clients field (32). At the bottom, there is an 'Apply/Save' button.

Wireless - Guest/Virtual Access Points:

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

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

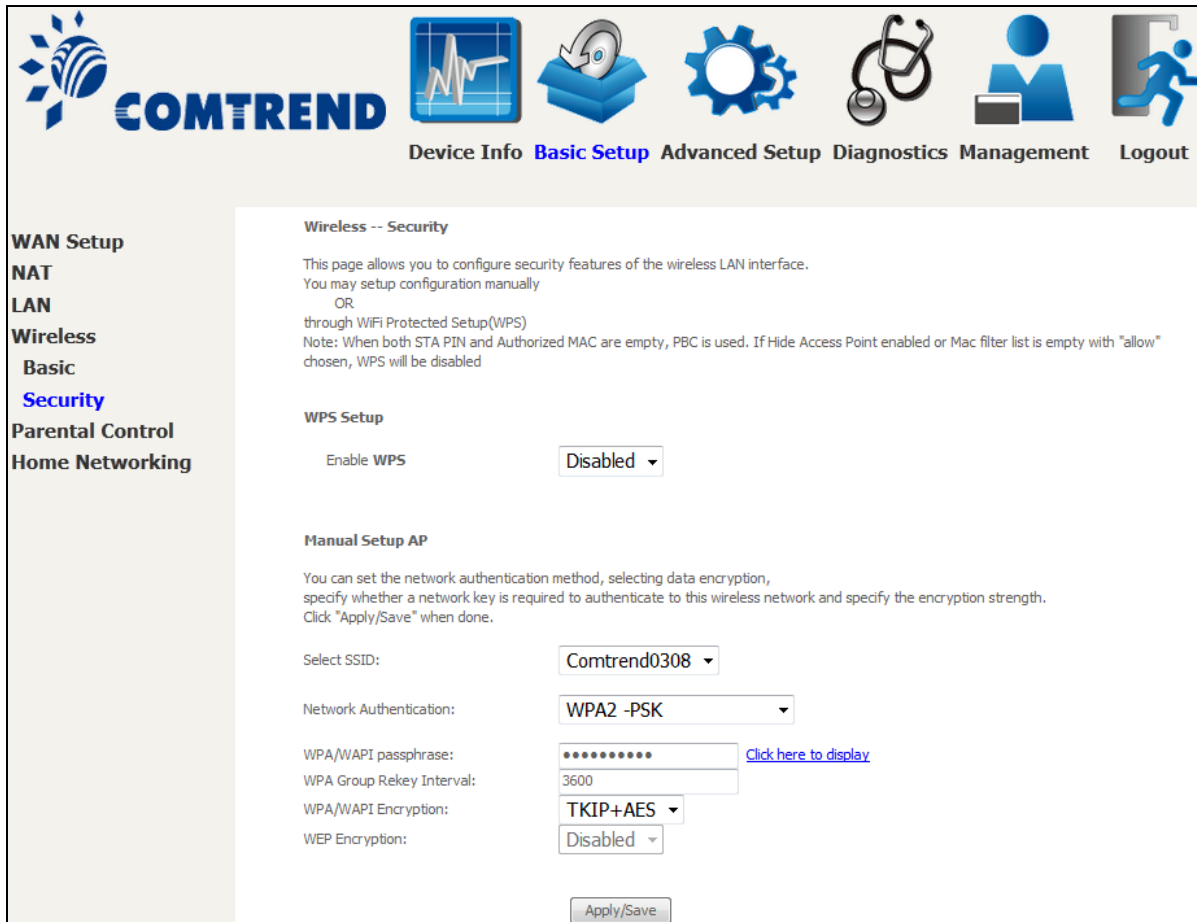
Consult the table below for descriptions of these options.

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. If the access point is hidden, it will not be listed or listed with empty SSID in the scan result of wireless stations. 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	Local regulations limit channel range: US/Canada = 1-11.
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.



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

WAN Setup
NAT
LAN
Wireless
 Basic
Security
 Parental Control
 Home Networking

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
 You may setup configuration manually
 OR
 through WiFi Protected Setup(WPS)
 Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled

WPS Setup

Enable WPS

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

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
WPA/WAPI passphrase:	•••••••• Click here to display
WPA Group Rekey Interval:	3600
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled

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

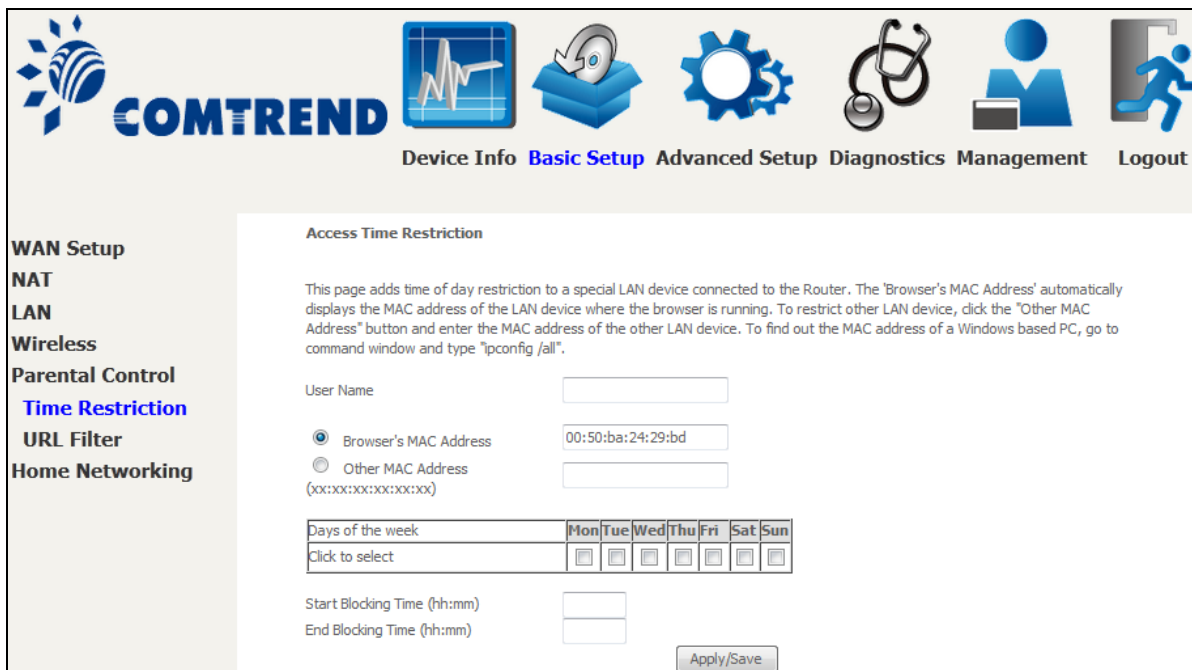
WAN Setup
NAT
LAN
Wireless
Parental Control
Time Restriction
URL Filter

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
Home Networking

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

Other MAC Address

(xx:xx:xx:xx:xx:xx)

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

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.

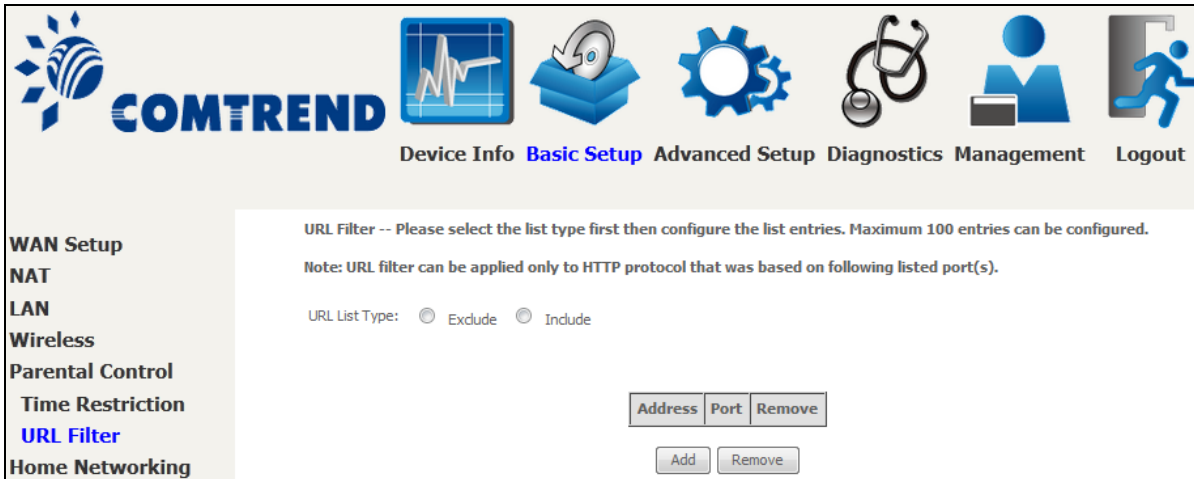
Days of the Week: The days the restrictions apply.

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.

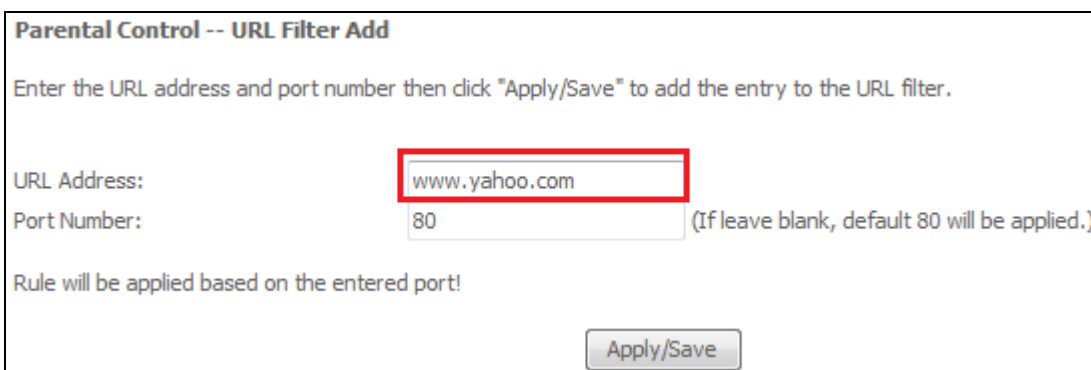


Select URL List Type: Exclude or Include.

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.



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 -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s).

URL List Type: Exclude Include

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

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.



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of settings categories: WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking (with Print Server highlighted in blue), DLNA, and Storage Service. The main content area is titled "Print Server settings" and contains the following text: "This page allows you to enable / disable printer support." Below this text are three input fields labeled "Manufacturer", "Product", and "Serial Number". There is a checkbox labeled "Enable on-board print server." and an "Apply/Save" button at the bottom right of the settings area.

Please reference [Appendix F](#) 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.

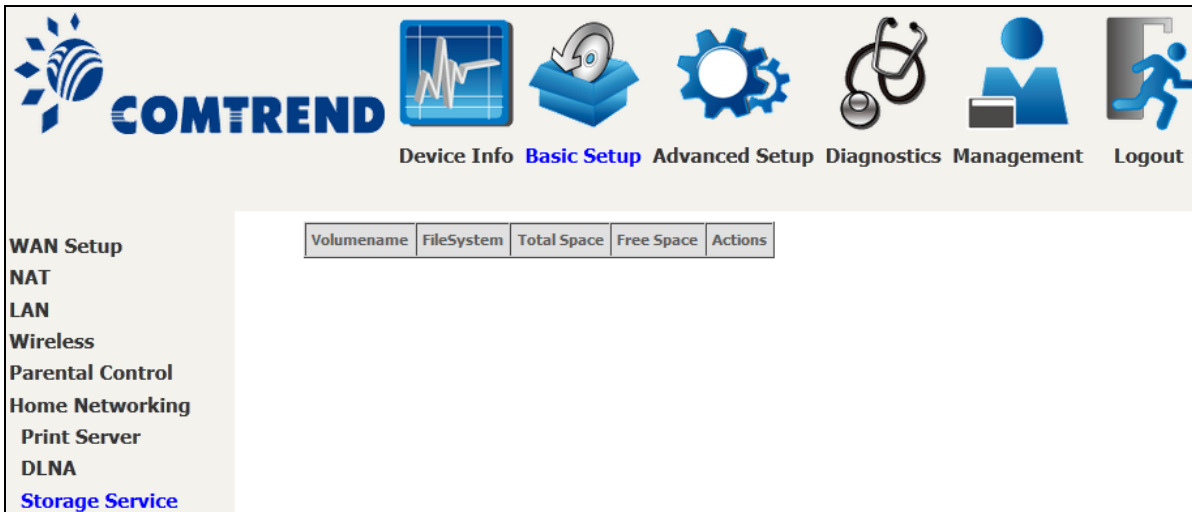
Insert USB drive to the USB host port on the back of router. Modify media library path to the corresponding path of the USB drive and click Apply/Save to enable the DLNA media server.



The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several menu items: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar on the left with a list of 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 following text: "This page allows you to enable / disable digital media server support." Below this text is a checkbox labeled "Enable on-board digital media server." which is currently unchecked. At the bottom right of the main content area, there is an "Apply/Save" button.

5.6.3 Storage Service

This page displays storage devices attached to USB host.



Volumename	FileSystem	Total Space	Free Space	Actions
------------	------------	-------------	------------	---------

Display after storage device attached (for your reference).

Volumename	FileSystem	Total Space	Free Space	Actions
usb1_1	fat	14770 MB	5762 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 screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo on the left and several icons representing different functions: Device Info (line graph), Basic Setup (box with arrow), Advanced Setup (gears, highlighted in blue), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). Below the navigation bar, the "Advanced Setup" page is displayed. On the left side, there is a vertical menu with the following items: Auto-Detection (highlighted in blue), Security, Quality of Service, Routing, DNS, DSL, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled "Auto-detection setup" and contains the following text: "The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface when applicable. 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." Below this text, there is a checkbox labeled "Enable auto-detect" which is currently unchecked. At the bottom of the main content area, there are two buttons: "Apply/Save" and "Restart".

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 when applicable. 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"/>	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"/>	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"/>	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"/>	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"/>	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"/>	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"/>	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"/>	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	PPPoE
-1	IPoE
-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.

Apply/Save

Restart

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	32	PPPoE ▾	<input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

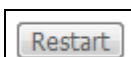
VLAN ID[0-4094]	Service	Option
-1	PPPoE ▾	<input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension

Auto Detection status and Restart

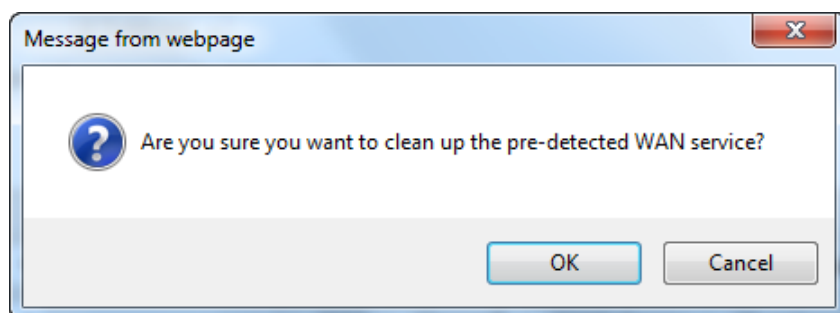
The Auto-detection status is used to display the real time status of the Auto-detection feature.

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

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.



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

Auto-Detection
Security
IP Filtering
Outgoing
 Incoming
 MAC Filtering

Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="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**.