

# WAP-5813n Gigabit Wireless Router User Manual

Version C1.0, May 20, 2009



#### Preface

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

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

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

#### **Important Safety Instructions**

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

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

CAUTION:

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

# A WARNING

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

#### Copyright

Copyright©2009 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

**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**

<b>CHAPTER 1</b>	INTRODUCTION	5
1.1 Featur	ES	5
1.2 APPLICA	ATION	5
CHADTED A		
CHAPIER 2	INSTALLATION	6
2.1 HARDW	ARE SETUP	6
2.2 LED IN	DICATORS	8
<b>CHAPTER 3</b>	WEB USER INTERFACE	9
3.1 DEFAUI	T SETTINGS	9
3.2 IP CONI	FIGURATION	10
3.3 Login I	PROCEDURE	12
CHAPTER A	DEVICE INFORMATION	1/
A 1 WAN		15
4.1 WAIN	1/2	15
4.2 STATIST	I AN Statistics	15
4.2.1	WAN Statistics	16
4.2.2	WAIN SIGUISUCS	17
4/APP		1 / 1 8
ч.ч ллг 4 5 пµ∩р		10 19
4.5 DHCI .		10
CHAPTER 5	ADVANCED SETUP	19
5.1 ETH W.	AN INTERFACE	19
5.2 WAN		20
5.3 LAN		20
5.4 NAT		23
5.4.1	Virtual Servers	23
5.4.2	Port Triggering	25
5.4.3	DMZ Host	26
5.5 Securi	ГҮ	27
5.5.1	IP Filtering	27
5.5.2	MAC Filtering	30
5.6 PARENT	AL CONTROL	31
5.6.1	Time Restriction	31
5.6.2	URL Filter	32
5.7 ROUTIN	G	33
5.7.1	Default Gateway	33
5.7.2	Static Route	34
5.7.3	RIP	35
5.8 DNS		35
5.8.1	DNS Server	35
5.8.2	Dvnamic DNS	36
5.9 UPNP		38
5.10 INTERI	ACE GROUPING	38
5.11 CERTI	FICATE	40
5.11.1	Local	40
5.11.2	Trusted CA	42
CHAPTER 6	WIRELESS	43
6.1 BASIC	·······	43
6.2 SECURI	۲Y	44
6.2.1	WPS	47
6.3 MAC F	ILTER	51
6.4 WIRELE	ss Bridge	52
6.5 ADVAN	CED	53
6.6 STATION	v Info	55
CHAPTER 7	DIAGNOSTICS	57

CHAPTER 8 MANAGEMENT	
8.1 Settings	
8.1.1 Backup Settings	
8.1.2 Update Settings	
8.1.3 Restore Default	
8.2 System Log	60
8.3 TR-069 CLIENT	61
8.4 Internet Time	
8.5 Access Control	
8.5.1 Passwords	
8.6 Update Software	64
8.7 SAVE AND REBOOT	
APPENDIX A – FIREWALL	66
APPENDIX B – PIN ASSIGNMENTS	69
APPENDIX C – SPECIFICATIONS	
APPENDIX D – SSH CLIENT	72
APPENDIX E – WSC EXTERNAL REGISTRAR	

# **Chapter 1 Introduction**

The WAP-5813n Gigabit Wireless Router provides wired and wireless access for high-bandwidth applications in the home or office. It is designed to connect to an ADSL or GPON (Gigabit-Capable Passive Optical Network) modem. It includes one 10/100/1000 Base-T Gigabit Ethernet WAN port and four 10/100/1000 Base-T Gigabit Ethernet LAN ports. It also has TR-068 compliant color panels and LED indicators, for easy installation and use.

An integrated 802.11n (draft) WLAN Access Point (AP) supports faster connections and increased range, without sacrificing compatibility with older wireless devices. WPS (Wi-Fi Protected Setup) and Wi-Fi On/Off buttons are included for easy wireless network setup. WPA data encryption, Firewall and VPN passthrough options are provided for state-of-the-art network security.

### **1.1 Features**

- Integrated 802.11n AP (802.11b/g backward-compatible)
- WPA/WPA2 and 802.1x
- RADIUS client
- Static routing
- NAT/PAT
- IGMP Proxy
- Applications Diagram
- Web-based management
- Supports remote administration

- WMM & UPnP
- IP filtering
- Dynamic IP assignment
- Parental Control
- DHCP Server/Client
- DNS Relay
- Configuration backup and restoration
- FTP/TFTP server

# **1.2 Application**

The following diagram depicts the application of the WAP-5813n with GPON.



# **Chapter 2 Installation**

# 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

#### **BACK PANEL**

The figure below shows the back panel of the device.



#### Power ON

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

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

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

#### **Reset Button**

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

**NOTE:** If pressed down for more than 20 seconds, the WAP-5813n will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

#### **ETHERNET (LAN) PORTS**

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

#### **ETH WAN PORT**

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

#### **FRONT PANEL**

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



#### WI-FI BUTTON (1)

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

#### WPS BUTTON

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

# 2.2 LED Indicators

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



LED	Color	Mode	Function
		On	The wireless module is ready. (i.e. installed and enabled).
WLAN	Green	Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.
		On	An Ethernet Link is established.
LAN 1X-4X	Green	Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
		On	WPS enabled.
WPS	Green	Off	WPS disenabled.
		Blink	The router is searching for WPS clients.
		On	An Ethernet WAN Link is established.
WAN	Green	Off	An Ethernet WAN Link is not established.
		Blink	Data transmitting or receiving over Ethernet WAN.
		On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present.
INTERNET	Green	Off	Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
	Green	On	The device is powered up.
DOWER		Off	The device is powered down.
(logo)	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.

# **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: **1234**, password: **1234**)
- User access (username: **user**, password: **user**)
- WAN IP address: none
- Remote WAN access: disabled
- Remote (WAN) access (username: **support**, password: **support**)
- WLAN access: **disabled**
- Service Set Identifier (SSID): WLAN\_67E1

This device supports the following connection types.

- PPP over Ethernet (PPPoE)
- IP over Ethernet (IPoW)
- Bridging

The following connections are configured by default.

Interface	Туре	Vlan Tag	Vlan Mux	IGMP	NAT	FIREWALL
eth0.3	IPoW	4	3	Ν	Y	N
ppp0.6	PPPoE	1	6	N	Y	Y

#### **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 WAP-5813n powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

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

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

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

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

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

#### STATIC IP MODE

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

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

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

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

Internet Protocol (TCP/IP) Propertie	s <u>? ×</u>
General	
You can get IP settings assigned autom this capability. Otherwise, you need to a the appropriate IP settings.	atically if your network supports isk your network administrator for
O Obtain an IP address automaticall	y 📗
<ul> <li>Use the following IP address:</li> </ul>	
<u>I</u> P address:	192.168.1.133
S <u>u</u> bnet mask:	255.255.255.0
Default gateway:	<u> </u>
C Obtain DNS server address autom	natically
─● Use the following DNS server add	Iresses:
Preferred DNS server:	· · ·
<u>A</u> lternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

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

## **3.3 Login Procedure**

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

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

- **STEP 1:** Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.
- **NOTE:** For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Information screen and login with remote username and password.
- **STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.

Enter Netw	vork Passwor	d	<u>? ×</u>
<b>?</b> >	Please type yo	ur user name and password.	
IJ	Site:	192.168.1.1	
	Realm	DSL Router	
	<u>U</u> ser Name		
	<u>P</u> assword		
	🔲 <u>S</u> ave this p	assword in your password list	
		OK Cano	el

Click **OK** to continue.

**NOTE:** The login password can be changed later (see section 8.5.1)

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

COMMEREND O WIFI ROL	iter	
in	Device Info	
	Board ID:	96369R-1231N
Device Info	Software Version:	P401-402TLF-C02_R12
Advanced Setup	Bootloader (CFE) Versio	n: 1.0.37-102.1-2
Diagnostics	Wireless Driver Version:	4.174.64.12.cpe4.402
Management	This information reflects the	e current status of your connection.
	LAN IPv4 Address:	192.168.1.1
	Default Gateway:	ppp0.6
	Primary DNS Server:	80.58.61.250
	Secondary DNS Server:	80.58.61.254

# **Chapter 4 Device Information**

The web user interface is divided into two windowpanes, 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.

COMPREND O WIFI ROU	ter Device Info		
	Board ID:	96369R-1231	N
Device Info	Software Version:	P401-402TLF	-C02_R12
Advanced Setup Wireless	Bootloader (CFE) Versio	n: 1.0.37-102.1-	-2
Diagnostics	Wireless Driver Version:	4.174.64.12.0	cpe4.402
Management	This information reflects the	e current status c	of your connection.
	LAN IPv4 Address:	192.168.1.1	
	Default Gateway:	ppp0.6	
	Primary DNS Server:	80.58.61.250	
	Secondary DNS Server:	80.58.61.254	

The Device Info Summary screen will display at startup.

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

# 4.1 WAN

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

- I				١	WAN Info	0			
	Interface	Description	Туре	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
evice Info	eth0.3	ipoe_eth0.3	IPoW	3	Disabled	Enabled	Disabled	Connecting	0.0.0
Summary				-	Distant	E-H-H	C-LL-I	Concertion 1	( 11)

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

# 4.2 Statistics

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

**NOTE:** These screens are updated every 15 seconds.

### 4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

COMTREND O WIFI RO	uter Statistics	LAN							
	Interface		Recei	ved		Tr	ansm	itted	
Device Info		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Summary	eth1	0	0	0	0	0	0	0	0
WAN	eth2	0	0	0	0	0	0	0	0
Statistics	eth3	0	0	0	0	0	0	0	0
LAN	eth4	261112	2057	0	0	1464062	2221	0	0
WAN Service	wl0	0	0	0	0	0	0	2	0
ARP DHCP Advanced Setup Wireless Diagnostics Management	Reset S	tatistics	-	-		-			-

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

### 4.2.2 WAN Statistics

This screen shows data traffic statistics for each WAN interface.

COMMEND O WIFI R	outer									
w	Statistics	WAN								
	Interface	Description		Rece	eived		T	ransn	nitte	d
Device Info			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Summany	eth0.3	ipoe_eth0.3	0	0	0	0	41400	138	0	0
WAN	eth0.6	pppoe_eth0.6	0	0	0	0	0	0	0	0
Statistics										
LAN	Reset S	Statistics								
WAN Service		an a								

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

### 4.3 Route

Choose **Route** to display the routes that the WAP-5813n has found.

COMMEND O WIFI Ro	uter							
Device Info	<b>Device Info</b> F Flags: U - up, ! - D - dynamic (redi	Route reject, G - ( irect), M - n	gateway, H - host, I nodified (redirect).	R - reir	nstate			
Summary	Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface	
Statistics	192.168.249.0	0.0.0.0	255.255.255.252	U	0		br0	
Route ARP DHCP	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 hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

### 4.4 ARP

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

COMPREND O	outer			
Davies Info	Device Info IP address	ARP Flags	HW Address	Device
Summary WAN Statistics	192.168.1.33	Complete	00:05:5D:A0:CD:E9	br0
Route ARP DHCP				

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

# 4.5 DHCP

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

COMPREND O WIFI RO	Device Info	DHCP Leases		
Device Info Summary WAN Statistics	Hostname	MAC Address	IP Address	Expires In
Route ARP DHCP				

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

# **Chapter 5 Advanced Setup**

This chapter explains the following screens:

5.1 ETH WAN INTERFACE	5.2 WAN
5.3 LAN	5.4 NAT
5.5 Security	5.6 Parental Control
5.7 Routing	5.8 DNS
5.9 UPnP	5.10 Interface Grouping
5.11 Certificate	

# **5.1 ETH WAN INTERFACE**

This screen displays the Ethernet WAN Interface configuration.

GOMTREND O WiFi Router			
Device Info	ETH WAN In Choose Add, or Remove Allow one ETH	terface Configurati to configure ETH W l as layer 2 wan interf	i <b>on</b> AN interfaces. face.
Advanced Setup	Interface/(Name)	Connection Mode	Remove
ETH Interface	etb0/ETHWAN	VanMuxMode	
LAN	GUIVETIWAN	Vianniuxinoue	
NAT		remove	
Security			
Parental Control			
Routing			
DNS			
Upnp Taba fara Caracian			
Certificate			

Heading	Description
Interface/ (Name)	ETH WAN Interface
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection MSC Mode – Multiple Service over one Connection
Remove	Select the checkbox and click <b>Remove</b> to remove the connection.

# 5.2 WAN

This screen allows for the configuration of WAN interfaces.

COMPRESS CONTRACT										
Device Info		Choose Ad	W Id, or Re E	<b>fide Area Net</b> move to conf	t <b>work (WAN)</b> figure a WAN s 'ATM service c	Service service service over	<b>Setup</b> er a select exist.	ed interfa	ce.	
ETH Interface	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
WAN Service	eth0.3	ipoe_eth0.3	IPoW	4	3	N/A	Disabled	Enabled	Disabled	
NAT	ppp0.6	pppoe_eth0.6	PPPoE	1	6	N/A	Disabled	Enabled	Enabled	
Security Parental Control Routing DNS Upnp Interface Grouping Certificate			1	A	dd Remov	e	1	1	1	

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Туре	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
IGMP	Shows Internet Group Management Protocol (IGMP) 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

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

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

### 5.3 LAN

From this screen, LAN interface settings can be configured.

WiFi Rou	ter
- Al	Local Area Network (LAN) Setup
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Routing	Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0 Loopback IP and Subnetmask IP Address: 127.0.0.1 Subnetmask: 255.0.0.0 IC Enable IGMP Snooping
DNS Uppp Interface Groupi Certificate Wireless Diagnostics Management	<ul> <li>Standard Mode</li> <li>Blocking Mode</li> <li>Enable LAN side firewall</li> <li>Disable DHCP Server</li> <li>Enable DHCP Server</li> <li>Start IP Address: <u>192.168.1.33</u> End IP Address: <u>192.168.1.254</u> Leased Time (hour):<sup>124</sup> Static IP Lease List: (A maximum 32 entries can be configured) [MAC Address IP Address Remove] Add Entries Remove Entries</li> </ul>
	Vendor Class ID (DHCP option 60) differential IP range assignment: (A maximum 32 entries can be configured) Vendor ID IP range start IP range end Primary DNS Secondary DNS Remove Add Entries Remove Entries Configure the second IP Address and Subnet Mask for LAN interface Apply/Save

**NOTE:** NAT is enabled so the **DHCP Server Relay** option is hidden above. (see underlined notes below).

Consult the field descriptions below for more details.

#### LOCAL AREA NETWORK (LAN) SETUP

**GroupName:** You can ignore this checkbox.

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

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

#### LOOPBACK IP AND SUBNETMASK

**IP Address:** Enter the IP address.

Subnet Mask: Enter the subnet mask.

**Enable IGMP Snooping:** Enable by ticking the checkbox .

<u>Standard Mode</u>: 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.

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

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

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

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

MAC Address	IP Address Remove				
Add Entries	Remove Entries				

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

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

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



- **DHCP Server Relay**: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. <u>This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.</u>
- **Vendor Class ID:** A maximum 32 entries can be configured. To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button.

To add an entry, click **Add Entries**. The following screen will display.

Vendor Class ID IP range setting									
Enter the Vendor Class ID and its corresponding IP range then click "Apply/Save" . If necessary, enter custom DNS servers for this Vendor Class ID. Otherwise, let them blank.									
Vendor Class ID:		]							
IP range start:		]							
IP range end:		]							
Primary DNS:		]							
Secondary DNS:		]							
		Apply/Save							

Enter appropriate information for each setting and then click **Apply/Save**.

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

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

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

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

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

### 5.4 NAT

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

### 5.4.1 Virtual Servers

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

GOMTREND O WIFI RO	uter								
Device Info Advanced Setup ETH Interface WAN Service	NAT Virt Virtual Serv with private port numbe	tual Servers Set ver allows you to d IP address on the r used by the serv	cup lirect incoming e LAN side. Th rer on the LAN	) traffic from \ e Internal por side. A maxir	NAN side (identif t is required only mum 32 entries o Add Remove	ied by Protoco r if the externa an be configu	ol and External p al port needs to b red.	ort) to the Interr	al server a different
LAN NAT Virtual Servers Port Triggering DMZ Host	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

To add a Virtual Server, click  $\boldsymbol{Add}.$  The following will be displayed.

_00	
COMTREND O	
WIEI RO	puter
1V	NAT Virtual Servers
	Select the service name, and enter the server IP address and click "Apply/Save" to forward IP nackets 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
Device Into	"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
ETH Interface	Remaining number of encies that can be configured.32
WAN Service	Use Interface br0
LAN	Service Name:
NAT	Select a Service: Select One
Virtual Servers	
Port Triggering	<ul> <li>Costoni Scivici,</li> </ul>
DMZ Host	Server IP Address: 192.168.1.
Security	
Parental Control	
Routing	Apply/Save
DNS	
Upnp	External Port Start External Port End Protocol Internal Port Start Internal Port End
Interface Grouping	TCP 💌
Certificate	
Wireless	
Management	TCP
rialiagement	TCP V
	TCP 🔽
	TCP V
	TCP 💌
	Apply/Save

Consult the table below for field and header descriptions.

Field/Header	Description
Use Interface	Select the WAN interface from the drop-down box.
Select a Service <b>Or</b> Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
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.

Field/Header	Description
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.

### 5.4.2 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 O	outer										
- AV	NAT Port T	riggering Setup									
Device Info Advanced Setup ETH Interface WAN Service LAN	Some applicati dynamically op party using the application on t	ons require that speci ens up the 'Open Port 'Triggering Ports'. Th the LAN side using the	ific ports in s' in the fir ne Router a e 'Open Por	the Rout ewall wh illows the ts'. A ma	er's fir en an remo iximun Add	rewall be of application te party fro 32 entries Remove	pened fo on the L m the W can be	AN ini AN ini AN sid config	ss by the remote p tiates a TCP/UDP c Je to establish new ured.	arties. Port onnection t connectior	Trigger o a remote is back to the
NAT			Т	rigger		C	pen				Ê.
Virtual Servers		Application Name		Port R	ange		Port R	ange	WAN Interface	Remove	
Port Triggering			Protocol	Start	End	Protocol	Start	End			
Security Parental Control Routing DNS Upnp Interface Grouping Certificate			I	1			<u> </u>	<u> </u>	1	I	

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

Perice Info   Advanced Setup   TH Interface   With Marene Setup   Name   Virtual Servers   Port Tiggering   Mart   Virtual Servers   Port Tiggering   Mart   Name   Parental Control   Roung   Minerace Grouping   Certificate   Wirelass   Diagnostics   Marteness   Diagnostics   Diagnostics   Diagnostics   Marteness   Dia	GOMVREND O	iter
	Device Info Advanced Setup ETH Interface WAN Service LAN NAT Virtual Servers Port Triggering DMZ Host Security Parental Control Routing DMS Upnp Interface Grouping Certificate Wireless Diagnostics Management	IV         INT Port Triggering         Some applications such as games, video conferencing, remote access applications and others require that specific ports in the source's firewall be opened for access by the application, You can configure the port settings from this screen by selecting an extern gaplication or creating your own (Custom application) and click "Save/Apply" to add it.         Image: Image

Consult the table below for field and header descriptions.

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

#### 5.4.3 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.

COMPREND O	outer
- AN	NAT DMZ Host
Device Info	The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Advanced Setup	Enter the computer's IP address and click "Apply" to activate the DMZ host.
ETH Interface	Clear the TD address field and alide "A sub-" to dearth she the DMT back
WAN Service	Clear the IP address held and click Apply to deactivate the DMZ host.
LAN	DM7 Host ID Address:
NAT	DHZ HOSCIF Address.
Virtual Servers	Saun/Applu
Port Triggering	Save/Apply
DMZ Host	

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

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

### **5.5 Security**

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

### 5.5.1 IP Filtering

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

**NOTE:** This function is not available when in bridge mode. Instead, MAC Filtering (pg. 30) performs a similar function.

#### **OUTGOING IP FILTER**

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

COMPREND O WIFI R	outer
- A	Outgoing IP Filtering Setup
Device Info Advanced Setup ETH Interface	By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be <b>BLOCKED</b> by setting up filters. Choose Add or Remove to configure outgoing IP filters.
WAN Service LAN NAT	Filter Name       Protocol       Source Address / Mask       Source Port       Dest. Address / Mask       Dest. Port       Remove         Add       Remove
Security IP Filtering Outgoing Incoming	

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

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

Contratto O WiFi Ro	uter
N	Add IP Filter Outgoing
Device Info Advanced Setup ETH Interface WAN Service	The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition 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.
LAN NAT Security IP Filtering Outgoing Incoming Parental Control	Protocol: Source IP address: Source Subnet Mask: Source Port (port or port;port): Destination IP address: Destination Subnet Mask:
Routing DNS Upnp Interface Grouping Certificate	Destination Port (port or port:port):

Consult the table below for field descriptions.

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

#### **INCOMING IP FILTER**

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

N	Incoming	IP Filtering Se	etup	AN or LAN inter	face all incoming ID traf		Hewever come	ID traffic ca	a ha
evice Info Idvanced Setup ETH Interface	Choose Ac	by setting up	filters.	incoming IP filt	ers.	TIC IS BLOCKEL	, nowever, some	IF traine ca	n be
WAN Service LAN NAT	Filter Name	Interfaces	Protocol	Allow/Deny	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Security	ICMP	ppp0.6	ICMP	Allow					
IP Filtering Outgoing	FTP1	ppp0.6	тср	Allow	193.152.37.192 / 255.255.255.240		_	21	
Parental Control Routing	FTP2	ppp0.6	ТСР	Allow	80.58.63.128 / 255.255.255.128			21	
DNS Upnp	FTP3	ppp0.6	тср	Allow	172.20.25.0 / 255.255.255.0			21	
Interface Grouping Certificate	FTP4	ppp0.6	тср	Allow	172.20.45.0 / 255.255.255.0			21	
Vireless Diagnostics	Telnet1	ppp0.6	тср	Allow	193.152.37.192 / 255.255.255.240			23	
Management	Telnet2	ppp0.6	тср	Allow	80.58.63.128 / 255.255.255.128			23	
	Telnet3	ppp0.6	ТСР	Allow	172.20.25.0 / 255.255.255.0			23	
	Telnet4	ppp0.6	тср	Allow	172.20.45.0 / 255.255.255.0			23	

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**.

COMPLEXID O WIFI Ro	uter
- Int	Add IP Filter Incoming
Device Info Advanced Setup ETH Interface WAN Service LAN	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.
NAT Security	pass the firewall first. Then, configure the specific denied IP address at a later time for successful implementation.
IP Filtering Outgoing Incoming Parental Contr Routing DNS Upnp Interface Grou Certificate Wireless Diagnostics	Protocol:       Image: Constraint of the second secon
Mahagement	r       Select All         r       br0         r       br0:1         r       eth1         r       eth2         r       eth3         r       eth4         r       pppoe_eth0.6/ppp0.6         r       br0/br0         r       br0:1/br0:1
	Apply/Save

Consult the table below for field descriptions.

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

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

#### 5.5.2 MAC Filtering

**NOTE:** This option is only available in bridge mode. Other modes use IP Filtering (pg. 27) 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 WAP-5813n 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.

COMPREND O WIFI R	outer
1V	MAC Filtering Setup
Device Info Advanced Setup	MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
ETH Interface	MAC HIEFING POICY FOT EACH INTERACE: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be
LAN	REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
NAT	Interface Policy Change
Security	
IP Filtering	
Parental Control	
Routing	Change Policy
DNS	
Upnp	Choose Add or Remove to configure MAC filtering rules.
Interface Grouping	Protocol Destination MAC Source MAC Dest Interface Src Interface Remove
Certificate	
Diagnostics	Add Remove
Management	

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of

them must be met. Click **Save/Apply** to save and activate the filter rule.

COMUREND O WIFI RO	nter
- A	Add MAC Filter
Device Info	Create a niter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.
Advanced Setup	
ETH Interface	Protocol Type:
WAN Service	Destination MAC Address: Set Multicast
LAN	Source MAC Address:
NAT	
IP Filtering	Source Interface
MAC Filtering	
Parental Control	Destination Interface:
Routing	
DNS	Save/Apply
Upnp	
Interface Grouping	
Cortificato	

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
Source/Destination Interfaces	Applies the filter to selected WAN interfaces.

### **5.6 Parental Control**

This selection provides WAN access control functionality.

### 5.6.1 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 8.4, so that the scheduled times match your local time.

COMPREND O WIFI R	outer											
M	Access Tin	e Restriction A ma	ximum	16 ei	ntries	can b	e con	figur	ed.			
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Time Restriction Url Filter		Username	MAC	Mon	Tue	Add	Re	Fri S	Sat Sun	Start	Stop	Remove

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

COMPREND O WIFI R	Outer Access Time Restriction
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security	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 Browser's MAC Address
Parental Control Time Restriction Url Filter Routing DNS Upnp Interface Grouping Certificate Wireless Diagnostics Management	C       Other MAC Address (xxxxxxxxxxxxxxx)         Days of the week       MonTue/Wed/ThuFri Sat/Sun Click to select         Click to select           Start Blocking Time (hh:mm)           End Blocking Time (hh:mm)           Save/Apply

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

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

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

Other MAC Address: MAC address of another LAN device.

Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

**End Blocking Time:** The time the restrictions end.

#### 5.6.2 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.

COMMEND O WIFI Ro	uter
A	URL Filter Please select the list type first then configure the list entries. Maximum 100 entries can be configured.
	URL List Type: O Exclude O Include
Device Info	
Advanced Setup	
ETH Interface	
WAN Service	Address Port Remove
LAN	
NAT	Add Remove
Security	
Parental Control	
Time Restriction	
Url Filter	

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

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

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

URL Filter A	maximum 10	)0 en	ntries ca	n be	configured.		
URL List Type:	O Exclude	0	Include				
				-	Advass	Dout	Domoulo
				ļ	Address	Port	Remove
					Address www.yahoo.com	<b>Port</b> 80	Remove

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

### 5.7 Routing

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

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

### 5.7.1 Default Gateway

Select a WAN Interface as the default gateway and click **Save/Apply**.

COMVIREND O WIFI RO	uter
N	Routing Default Gateway
	Select a preferred wan interface as the system default gateway.
Device Info	
Advanced Setup	Selected WAN Interface pppoe_eth0.6/ppp0.6
ETH Interface	
WAN Service	
LAN	
NAT	
Security	
Parental Control	
Routing	
Default Gateway	Save/Apply
Static Route	
RIP	

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

### 5.7.2 Static Route

This option allows for the configuration of static routes. Click **Add** to create a new static route. Click **Remove** to delete the selected static route.

COMURIND O WIFI RO	outer
N	Routing Static Route (A maximum 32 entries can be configured)
	Destination Subnet Mask Gateway Interface Remove
Device Info	
Advanced Setup	Add Remove
ETH Interface	
WAN Service	
LAN	
NAT	
Security	
Parental Control	
Routing	
Default Gateway	
Static Route	

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

COMPRESS O WIFI R	outer
N	Routing Static Route Add
Device Info Advanced Setup	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.
ETH Interface WAN Service LAN	Destination Network Address: Subnet Mask:
NAT Security Parental Control	Use Interface ipoe_eth0.3/eth0.3
Routing Default Gateway	Use Gateway IP Address Apply/Save
Static Route RIP	

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

#### 5.7.3 RIP

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

COMTREND O WIFI R	outer
- A	Routing RIP Configuration
Device Info Advanced Setup ETH Interface WAN Service	NOTE: RUP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE). 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.
LAN NAT Security Parental Control Routing	Interface Version Operation Enabled eth0.3 2 Passive V
Default Gateway Static Route RIP	Save/Apply

### 5.8 DNS

#### 5.8.1 DNS Server

To obtain DNS information from a WAN interface, select the first radio button and then choose a WAN interface from the drop-down box. For Static DNS, select the second radio button and enter the IP Address of the primary (and secondary) DNS server(s). Click **Save/Apply** to save the new configuration.
GOMTREND O WIFI R	outer
Device Info Advanced Setup ETH Interface WAII Service LAN NAT Security Parental Control Routing DNS DNS Server Dynamic DNS Upnp Interface Grouping Certificate Wireless Diagnostics Management	DIS Server Configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IP Addresses for single PVC

**NOTE:** You must reboot the router to make the new configuration effective.

# 5.8.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the WAP-5813n to be more easily accessed from various locations on the Internet.

COMPREND O WIFI R	puter
w	Dynamic DNS
Device Info	The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.
Advanced Setup ETH Interface WAN Service	Choose Add or Remove to configure Dynamic DNS.           Hostname         Username         Service         Interface         Remove
NAT Security Parental Control	Add Remove
Routing DNS	
DNS Server Dynamic DNS Upnp Interface Grouping	

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

COMPRESSION OF WIFI ROL	uter	
N	Add Dynamic DNS	
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Routing DNS DNS Server	This page allows you to a D-DNS provider Hostname Interface <b>DynDNS Settings</b> Username Password	add a Dynamic DNS address from DynDNS.org or TZO.          DynDNS.org         br0
Upnp Interface Grouping Certificate		Apply/Save

Consult the table below for field descriptions.

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

# 5.9 UPnP

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

GOMHREND O WIFI R	outer	
N	Upnp Configuration	
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Routing DNS Upnp Interface Grouping Certificate	☐ Enable or disnable Upnp protocol.	Apply/Save

# 5.10 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

Contrand O WiFi Ro	outer						
Device Info Advanced Setup ETH Interface	Interface Group Interface Group support this fea button will rem	uping A ing suppor iture, you r ove the gro	A maximum 16 en ts multiple ports to nust create mappin uping and add the	PVC and bridging o PVC and bridging ng groups with app ungrouped interfa	<b>figured</b> groups. Each group v ropriate LAN and WA ces to the Default gro	vill perform as an independent N interfaces using the Add butt rup. Only the default group has	network. To ion. The Remove IP interface.
LAN	Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs	1	
NAT			ppp0.6	ENET1			
Security			atho D	ENETO			
Parental Control	Default		ethu.3	ENETZ			
Routing				ENET3			
DNS				ENET4			
Upnp			1				
Interface Grouping Certificate	Add Remov	e					

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

Wilt RG					
- M	Interface grouping Configuration				
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Routing DNS Upp Interface Grouping Cartificate Wireless Diagnostics Management	Interface grouping Configuration To create a new interface group: 1. Enter the force group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below: 2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the sectified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. 3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain a. Click Save/Apply button to make the changes effective limitediately. IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. Grouped LAN Interface Available LAN Interfaces INTERCENTION				
	Automatically Add Cients With the following DHCP Vendor IDs				

#### Automatically Add Clients With the Following DHCP Vendor IDs:

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

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE and the others are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

- 1. Default: ENET1, ENET2, ENET3, and ENET4.
- 2. Video: nas\_0\_36, nas\_0\_37, and nas\_0\_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the ISP's DHCP server is running on PVC 0/36. It is for set-top box use only. On the LAN side, the PC can get IP address from the CPE's DHCP server and access the Internet via PPPoE (0/33).

If the set-top box is connected with interface "ENET1" and sends a DHCP request with vendor id "Video", the CPE's DHCP server will forward this request to ISP's DHCP server. Then the CPE will change the port-mapping configuration automatically. The port-mapping configuration will become:

- 1. Default: ENET2, ENET3, and ENET4.
- 2. Video: nas\_0\_36, nas\_0\_37, nas\_0\_38, and ENET1.

# 5.11 Certificate

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

# 5.11.1 Local

COMPREMD O WIFI R	outer
W	Local Certificates
Device Info	Add, view of Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.
Advanced Setup	
ETH Interface	Name In Nea Subject Tune Action
WAN Service	name in ose subject type Action
LAN	Create Certificate Request Import Certificate
NAT	
Security	
Parental Control	
DNS	
Upnp	
Interface Grouping	
Certificate	
Local	
Trusted CA	

# **CREATE CERTIFICATE REQUEST**

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

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

COMPREND O WIFI R	outer	
- w	Create new certificate request	
Device Info	To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2- letter Country Code for the certificate.	
Advanced Setup	Cartificate Name:	
ETH Interface		
WAN Service		
LAN	organization Name:	
nA1 Econvitu	State/Province Name:	
Parental Control	Country/Region Name: US (United States)	
Routing		
DNS		
Upnp	Apply	
Interface Grouping		
Certificate		
Local		
Trusted CA		

The following table is provided for your reference.

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

## IMPORT CERTIFICATE

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

COMPREND O WIFI Rot	iter		
- A	Import certificate		
Device Info Advanced Setup ETH Interface WAN Service LAN	Enter certificate nam Certificate Name:	ne, paste certificate content and private key.	×
Security Parental Contr Routing DNS Upnp Interface Grou	Certificate:		
Certificate Local Trusted CA Wireless Diagnostics Management		BEGIN RSA PRIVATE MEY <insert here="" key="" private=""> END RSA PRIVATE MEY</insert>	<u>v</u> ] 61
	Private Key:		
		Apply	Y

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

# 5.11.2 Trusted CA

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

COMPREND O WIFI RO	outer
- AND	Trusted CA (Certificate Authority) Certificates Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Device Info	Maximum 4 certificates can be stored.
Advanced Setup	
ETH Interface	Name Subject Time Action
WAN Service	Name Subject Type Action
LAN	Import Cartificate
NAT	Import Ceruncate
Security	
Parental Control	
Routing	
DNS	
Upnp	
Interface Grouping	
Certificate	
Local	
Trusted CA	

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

	outer
Device Info Advanced Setup ETH Interface WAN Service LAN NAT Security Parental Control Routing DNS Upnp Interface Grouping Certificate Local Trusted CA Wireless Diagnostics Management	Import CA certificate         Enter certificate name and paste certificate content.         Certificate         Name:        BEGIN CERTIFICATE <insert certificate="" here="">        END CERTIFICATE         Certificate:</insert>
	Арріу

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

# **Chapter 6 Wireless**

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

# 6.1 Basic

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

COLTREND O WIFI RO	uter							
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management	Wireless This page hide the n country re Click "App Click "App Hid Cli Cli Dis SSID: BSSID: BSSID: Country: Max Clien	Basic allows you to configure base etwork from active scans, s quirements. y" to configure the basic wi able Wireless le Access Point ents Isolation able WMM Advertise WLAN_67E1  SPAIN ts: 16	sic features of the wir et the wireless netwo ireless options.	eless LAI rk name	V interface. (also known	√ou can ( a as SSID	enable o	r disable the wireless LAN interface, estrict the channel set based on
	Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Max Clients	BSSID	
		wl0_Guest1			Π	16	N/A	
		wl0_Guest2			Π	16	N/A	
		wl0_Guest3			Π	16	N/A	
	Save/A	upply.						

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

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox $\square$ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open <b>Network Connections</b> from the <b>start</b> Menu and select <b>View</b> <b>Available Network Connections</b> . 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.

Option	Description		
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).		
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	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes $\square$ in the <b>Enabled</b> column. To hide a Guest SSID select its checkbox $\square$ in the <b>Hidden</b> column.		
	Do the same for <b>Isolate Clients</b> and <b>Disable WMM Advertise</b> . For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for <b>Max Clients</b> and <b>BSSID</b> , consult the matching entries in this table.		
	<b>NOTE:</b> Remote wireless hosts cannot scan Guest SSIDs.		

# 6.2 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.

	uter	
Device Info Advanced Setup Wireless	Wireless Security This page allows you to config You may setup configuration n OR through WiFi Protcted Setup(W	ure security features of the wireless LAN interface. nanually (PS)
Basic Security MAC Filter Wireless Bridge	WSC Setup Enable WSC	Enabled 💌
Advanced Station Info Diagnostics Management	Add Client (This feature	is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)           O Push-Button         O PIN           Add Enrolee         Help
	Set WSC AP Mode	Configured
	Device PIN	21143892 <u>Help</u>
	WSC Add External Registrar	Start AddER
	Manual Setup AP	
	You can set the network authe specify whether a network ke Click "Save/Apply" when don	intication method, selecting data encryption, $\gamma$ is required to authenticate to this wireless network and specify the encryption strength, e,
	Select SSID:	WLAN_67E1
	Network Authentication:	WPA-PSK
	WPA Pre-Shared Key: WPA Group Rekey Interval: WPA Encryption: WEP Encryption:	Click here to display       0       TKIP       Disabled
		Save/Apply

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

## WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see section 6.2.1) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

## Select SSID

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

## Network Authentication

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

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

	Network Authentication:	802.1X	•		
	RADIUS Server IP Address:	0.0.0.0			
	RADIUS Port:	1812			
	RADIUS Key:				
	WEP Encryption:	Enabled -			
	Encryption Strength: Current Network Key:	128-bit 💌			
	Network Key 1:				
	Network Key 2:				
	Network Key 3:				
	Network Key 4:				
		Enter 13 ASCI Enter 5 ASCII	II characters or 26 hexade characters or 10 hexadeo	ecimal digits for 128-bit encry imal digits for 64-bit encrypt	ption keys on keys
			Save/Appl	/	
The set	tings for WPA authe	entication	are shown belo	ow.	
	Network Auther	ntication :	WPA	•	
	W/PA Group Rek	ev Interval:	0		
	RADIUS Server	IP Address:	0.0.0		
	RADIUS Port:		1812		
	RADIUS Kev:				
	WPA Encryption	1:	TKIP 🔻		
	WEP Encryption	i:	Disabled 💌		
				Save/Apply	
The set	tings for WPA-PSK	authentic	ation are showr	n next.	
	Select SSID:				
	Network Authenti	cation:			
	WPA Pre-Shared	Key:		Click here to display	
	WPA Group Reke	y Interval:	0		
	WPA Encryption:		TKIP 🔽		
	WEP Encryption:		Disabled 💌		
				Save/Apply	
				· · · · · · · ·	]

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.

# 6.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The WAP-5813n has both a WPS button on the rear panel and a virtual button accessed from the web user interface (WUI).

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



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

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

## I. Setup

**Step 1:** Enable WPS by selecting **Enabled** from the drop down list box shown.

WSC Setup	
Enable <b>WSC</b>	Enabled <b>•</b>

**Step 2:** Set the WSC AP Mode. **Configured** is used when the WAP-5813n will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the WAP-5813n.



**NOTES:** Your client may or may not have the ability to provide security settings to the WAP-5813n. If it does not, then you must set the WSC AP mode to Configured. Consult the device documentation to check its capabilities.

In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix E has detailed instructions).

## **II. NETWORK AUTHENTICATION**

**Step 3:** Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.

Manual Setup AP		
You can set the network auther specify whether a network key network and specify the encry Click "Save/Apply" when done	entication method, selecting data encryption,	
Select SSID:	Comtrend	
Network Authentication:	WPA2 -PSK	
WPA Pre-Shared Key: WPA Group Rekey Interval: WPA Encryption: WEP Encryption:	0 AES V Disabled	- star 2
	Save/Apply	Step 3

**Step 4:** For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



**Step 5:** Click the **Save/Apply** button at the bottom of the screen.

## **IIIa. PUSH-BUTTON CONFIGURATION**

The WPS push-button configuration provides a semi-automated configuration

method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

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

**NOTE:** The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

#### Step 6: First method: WPS button

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

#### Second method: WUI virtual button

Select the Push-Button radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

## **A** - For **Configured** mode, click the **Add Enrollee** button.

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

## **B** - For **Unconfigured** mode, click the **Config AP** button.

Setup AP (Configure all security settings with an external registar)				
⊙ Push-Button O PIN	Config AP			

**Step 7:** Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.

<u>P</u> IN	WPS Associate IE		Progress >> 25%
P <u>B</u> C	WPS Probe IE	PBC - Sending EAPO	)L-Start

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

## **IIIb. WPS – PIN CONFIGURATION**

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

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

**NOTE:** Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

**Step 6:** Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

**A** - For **Configured** mode, enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).

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

#### **B** - For **Unconfigured** mode, click the **Config AP** button.

Setup AP (Configure all security settings with an external registar)	
C Push-Button O PIN	Config AP

**Step 7:** Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

The figure below provides an example of a WPS client PIN function in-progress.

PIN 🔽 WPS Associate II	
PBC WPS Probe IE	PIN - Sending EAP-Rsp(ID)

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

## **IV. CHECK CONNECTION**

Г

**Step 8:** If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

# 6.3 MAC Filter

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

GOMTREND O WIFI R	outer
A	Wireless MAC Filter ( Limit to 16 entries )
Device Info	Select SSID: WLAN_67E1
Advanced Setup Wireless Basic	MAC Restrict Mode:      O Disabled      Allow      Deny
Security MAC Filter Wireless Bridge	No MAC Address Remove
Advanced Station Info	Add Remove
Diagnostics Management	

Option	Description
Select SSID	Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

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

COMPREND O WIFI R	outer
M	Wireless MAC Filter
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management	Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.          MAC Address:

# **6.4 Wireless Bridge**

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

COMMEND O WIFI Ro	outer	
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management	Wireless Bridge         This page allows you to configure wireless bridge features of the wireless LAN interface. You can as Wireless Distribution System) to disable access point functionality. Selecting Access Point enable Wireless bridge restriction. Any wireless bridge will be granted access. Se enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges will be granted access. Sc enables wireless bridge restriction. Only those bridge selected in Remote Bridges MAC Address:         AP Mode:       Access Point V         Bridge Restrict:       Enabled V         Remote Bridges MAC Address:       Seve/Apply         Refresh       Save/Apply	select Wireless Bridge (also known oles access point functionality. t the AP. Select Disabled in Bridge lecting Enabled or Enabled(Scan) d access.

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

Feature	Description
AP Mode	Selecting <b>Wireless Bridge</b> (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting <b>Access</b> <b>Point</b> enables AP functionality. In <b>Access Point</b> mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

Feature	Description
Bridge Restrict	Selecting <b>Disabled</b> disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting <b>Enabled</b> or <b>Enabled (Scan)</b> enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click <b>Refresh</b> to update the station list when Bridge Restrict is enabled.

# 6.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save/Apply** to set new advanced wireless options.

GOMHREND O WIFI R	outer	
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management	Wireless Advanced This page allows you to configu operate, force the transmission interval for clents in power-save preambles are used. Click "Apply" to configure the ai Band: Channel: Auto Channel Timer(min) 802.11n/EWC: Bandwidth: Control Sideband: 802.11n Rate: 802.11n Protection: Support 802.11n Clent Only: 54g <sup>rm</sup> Rate: Multicast Rate: Basic Rate: Fragmentation Threshold: RTS Threshold: DTIM Interval: Beacon Interval: Global Max Clents: XPress <sup>rm</sup> Technology: Transmit Power: WMM(Wi-FI Multimedia): WMM No Acknowledgement:	re advanced features of the wireless LAN interface. You can select a particular channel on which to rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup e mode, set the beacon interval for the access point, set XPress mode and set whether short or long dvanced wireless options.  24GHz   24GHz   Current: 5  Current: 5  Current: 20MHz in 24G Band and 40MHz in 5G Band Current: 20MHz  Lower  Current: None  Auto Current: None  Auto Default Default Disabled  Disabled Default Dit Disabled Default Dit Dit Disabled Default Disabled Default Disab
		Save/Apply

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.

Field	Description	
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)	
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)	
Bandwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.	
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.	
802.11n Rate	Set the physical transmission rate (PHY).	
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.	
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.	
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.	
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)	
Basic Rate	Setting basic transmission rate.	
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.	
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.	
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.	

Field	Description
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is $1 - 65535$ . The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

# 6.6 Station Info

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

COMTREND O	outer
w	Wireless Authenticated Stations
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management	This page shows authenticated wireless stations and their status.           MAC         Associated         Authorized         SSID         Interface           Refresh         Refresh

Consult the table below for descriptions of each column heading.

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

# **Chapter 7 Diagnostics**

Diagnostics screens for IPoW and PPPoE connection types are shown below.

## **IPoW Connection**

COMPRESSION OF WIFI RO	uter			
Device Info Advanced Setup	ipoe_eth0.3 Diagnostics Your modem is capable of testing your DSI "Rerun Diagnostic Tests" at the bottom of I and follow the troubleshooting procedures	L connectio this page t	on. The ir o make s	ndividual tests are listed below. If a test displays a fail status, click sure the fail status is consistent. If the test continues to fail, click "Help"
Wireless	Test the connection to your local net	work		
Diagnostics	Test your ENET4 Connection:	PASS	Help	
Management	Test your ENET1 Connection:	FAIL	Help	
	Test your ENET2 Connection:	FAIL	Help	
	Test your ENET3 Connection:	FAIL	Help	
	Test your Wireless Connection:	PASS	Help	
	Test the connection to your Internet	service p	rovider	
	Ping default gateway:	FAIL	<u>Help</u>	
	Ping primary Domain Name Server:	FAIL	<u>Help</u>	
	Test Loopback IP:	PASS	Help	
		Те	Ne>	d: Connection

## **PPPoE Connection**

GOMTREND O	l													
Device Info Advanced Setup Wireless	pppoe_eth0.6 Diagnostics Your modem is capable of testing your DSL "Rerun Diagnostic Tests" at the bottom of ti and follow the troubleshooting procedures.	connectio his page t	on. The o make	e indiv e sure	idual the f	tests ail sta	are lis tus is	sted be consis	low. If tent. I	f a tesi f the t	t display est conf	/s a fail tinues to	status, cli fail, click	ck "Help"
Diagnostics	Test your ENET4 Connection:	PASS	Help											
Management	Test your ENET1 Connection:	FAIL	Help											
	Test your ENET2 Connection:	FAIL	Help											
	Test your ENET3 Connection:	FAIL	Help											
	Test your Wireless Connection:	PASS	Help											
	Test the connection to your Internet s	service p DISAB	rovid	er <u>Help</u>										
	Test authentication with ISP:	DISABLED		Help										
	Test the assigned IP address:	DISABLED		Help										
	Ping default gateway:	FAIL		нер										
	Ping primary Domain Name Server:	FAIL		Help										
	Test Loopback IP:	PASS		Help										
			Pre	vious	Conn	ection								
		Те	st	Tes	With	OAM	F4							

The Diagnostics menu provides feedback on the connection status of the WAP-5813n. If a test displays a fail status, click the **Test** button to retest and confirm the error. If the test continues to fail, click <u>Help</u> and follow the troubleshooting procedures provided.

# **Chapter 8 Management**

The Management menu has the following maintenance functions and processes:

8.1 Settings	8.2 System Log
8.3 TR-069 Client	8.4 Internet Time
8.5 Access Control	8.6 Update Software
8.7 Save and Reboot	

# 8.1 Settings

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

# 8.1.1 Backup Settings

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

COMPREND O WIFI R	outer
- IN	Settings - Backup
Device Info Advanced Setup Wireless Diagnostics Management Settings Backup Update	Backup DSL router configurations. You may save your router configurations to a file on your PC. Backup Settings

# 8.1.2 Update Settings

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

COMPREND O WIFI RO	uter
Device Info	Tools Update Settings Update DSL router settings. You may update your router settings using your saved files.
Advanced Setup	Settings File Name: Browse
Wireless Diagnostics	Update Settings
Management	
Backup	
Update	
Restore Default	

# 8.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.

COMTREND O WIFI R	uter	
N	Tools Restore Default Settings	
	Restore DSL router settings to the factory defaults.	
Device Info		
Advanced Setup	Restore Default Settings	
Wireless	Restore berdare berdings	
Diagnostics		
Management		
Settings		
Backup		
Update		
Restore Default		

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

#### DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

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

# **NOTE:** This entry has the same effect as the **Reset** button. The WAP-5813n board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

# 8.2 System Log

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

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

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

COMPREND O WIFI R	outer
M	System Log
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log TR-069 Client Internet Time Access Control Update Software Reboot	The System Log dialog allows you to view the System Log and configure the System Log options. Click "View System Log" to view the System Log. Click "Configure System Log" to configure the System Log options. View System Log

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

Compression O WiFi Ro	buter
A	System Log Configuration
Device Info Advanced Setup Wireless	If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Diagnostics	Select the desired values and click 'Apply/Save' to configure the system log options.
Management Settings	Log: • Disable C Enable
System Log TR-069 Client Internet Time Access Control Update Software Reboot	Log Level:     Debugging       Display Level:     Error       Mode:     Local
	Apply/Save

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

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

Option	Description
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the WAP-5813n SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.
	The log levels are defined as follows:
	<ul> <li>Emergency = system is unusable</li> <li>Alert = action must be taken immediately</li> <li>Critical = critical conditions</li> <li>Error = Error conditions</li> <li>Warning = normal but significant condition</li> <li>Notice= normal but insignificant condition</li> <li>Informational= provides information for reference</li> <li>Debugging = debug-level messages</li> </ul> Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the <b>View</b> <b>System Log</b> window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

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

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

# 8.3 TR-069 Client

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

COMPREND O		
WiFi Ro	uter	
- I	TR-069 client - Configuration	
Device Info	WAN Management Protocol (TR-069) a and diagnostics to this device.	llows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection,
Advanced Setup Wireless	Select the desired values and click "App	ply/Save" to configure the TR-069 client options.
Diagnostics Management	Inform	Disable C Enable
Settings	Inform Interval:	300
System Log	ACS URL:	
TR-069 Client	ACS User Name:	admin
Access Control	ACS Password:	****
Update Software	WAN Interface used by TR-069 client:	Any_WAN 💌
Reboot	Display SOAP messages on serial conso	ole © Disable © Enable
	Connection Request Authentication	
	Connection Request User Name:	admin
	Connection Request Password:	
	Connection Request URL:	
		Apply/Save GetRPCMethods

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

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

# 8.4 Internet Time

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

GOMTREND O WIFI RO	uter		
M	Time settings		
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log TR-069 Client Internet Time Access Control Update Software Reboot	This page allows you to the Automatically synchron First NTP time server: Second NTP time server: Third NTP time server: Fourth NTP time server: Fifth NTP time server: Time zone offset:	he modem's time configuration. Inize with Internet time servers Itime.nist.gov Intp1.tummy.com None None None (GMT-08:00) Pacific Time, Tijuana Save/Apply	<u> </u>

**NOTE:** Internet Time must be activated to use Parental Control (page 31). In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

# 8.5 Access Control

# 8.5.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the WAP-5813n is controlled through the following three user accounts:

- **1234** this has unrestricted access to change and view the configuration.
- **support** used for remote maintenance and diagnostics of the router
- **user** this has limited access. This account can view configuration settings and statistics, as well as, update the router firmware.

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

COMMENTE O WIFI Ro	uter			
- A	Access Control Passwords			
	Access to your DSL router is controlled through three user accounts: '1234', support, and user.			
Device Info				
Advanced Setup	The user name "1234" has unrestricted access to change and view configuration of your DSL Router.			
Wireless	The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.			
Diagnostics				
Management	The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's			
Settings	sortware.			
System Log	Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a			
TR-069 Client	space.			
Internet Time				
Access Control	Username:			
Passwords	Old Password:			
Update Software	New Password:			
Reboot	Confirm Password:			
	Save/Apply			

**NOTE:** Passwords must be 16 characters or less.

# 8.6 Update Software

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

COMPREND O WIFI R	outer			
- M	Tools Update Software			
	Step 1: Obtain an updated software image file from your ISP.			
Device Info	Shan 2: Enter the path to the image file legation in the her below or dick the "Browse" butten to legate the image file			
Advanced Setup	Step 2: Enter the path to the image me location in the box below of click the provise button to locate the image me.			
Wireless	Step 3: Click the "Update Software" button once to upload the new image file.			
Diagnostics				
Management	NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.			
Settings	Software Elle Names			
System Log	Soltware File Name: Drowse			
TR-069 Client	Undets Coffware			
Internet Time	Update Software			
Access Control				
Update Software				
Reboot				

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

- **STEP 2**: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.
- STEP 3: Click the Update Software button once to upload and install the file.
- **NOTE**: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** at the top of the Device Information screen with the firmware version installed, to confirm the installation was successful.

# 8.7 Save and Reboot

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

COMUREND O WIFI R	outer
- John Stand	Click the button below to reboot the router.
Device Info	Reboot
Advanced Setup	
Wireless	
Diagnostics	
Management	
Settings	
System Log	
TR-069 Client	
Internet Time	
Access Control	
Update Software	
Reboot	

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

# Appendix A – Firewall

## STATEFUL PACKET INSPECTION

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

# **DENIAL OF SERVICE ATTACK**

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

# TCP/IP/PORT/INTERFACE FILTER

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

## **OUTGOING IP FILTER**

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

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

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

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

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

## **INCOMING IP FILTER**

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

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

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

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

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

#### MAC LAYER FILTER

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

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

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

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

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

## DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the WAP-5813n, as per chosen days of the week and the chosen times.

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

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

# **Appendix B – Pin Assignments**

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

# **ETHERNET Ports (RJ45)**

# **Appendix C – Specifications**

## **Hardware Interface**

RJ-45 X 1 for WAN (Giga Ethernet), RJ-45 X 4 for LAN (Giga Ethernet), WPS Button X 1, Power Switch X 1, Wi-Fi On/Off Button X 1, Reset Button X 1

## LAN Interface

Standard..... IEEE 802.3, IEEE 802.3u 10/100 BaseT..... Auto-sense MDI/MDX support...... Yes

## **WLAN Interface**

Standard	IEEE802.11n (IEEE802.11b/g compatible)
Encryption	64/128-bit Wired Equivalent Privacy (WEP)
Channels	11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate	Up to 300Mbps
WPA/WPA2	Yes
IEEE 802.1x	Yes
WMM	Yes
WPS	Yes
MAC Filtering	Yes
Optional	Afterburner mode (Turbo mode)***

#### Management

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

## **Routing Functions**

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

## **Security Functions**

Authentication protocol : PAP, CHAP Port Triggering/Forwarding, Packet and MAC address filtering, DoS Protection, SSH, VPN

## **Application Passthrough**

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

Power Supply	Input:	100 - 240 Vac
	Output:	12 Vdc / 1.0 A

## **Environment Condition**

# Kit Weight

(1\*WAP-5813n, 1\*RJ45 cable, 1\*power adapter, 1\*CD-ROM) = 1.0 kg

Certifications ...... CE 0197,CE

**NOTE:** Specifications are subject to change without notice
## **Appendix D – SSH Client**

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

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

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

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

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

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

## Appendix E – WSC External Registrar

Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows Vista operating system:

**Step 1:** Enable UPnP on the Advanced Setup  $\rightarrow$  LAN screen in the WUI.



**NOTE:** A PVC must exist to see this option.

**Step 2:** Open the Network folder and look for the BroadcomAP icon.



**Step 3:** On the Wireless  $\rightarrow$  Security screen, enable WSC by selecting **Enabled** from the drop down list box and set the WSC AP Mode to Unconfigured.

COMPRESS OF	
Device Info	Wireless Security This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WIFE Protected Setup(WPS)
Wireless Basic Security MAC Filter Wireless Bridge Advanced	WSC Setup Enable WSC Enabled
Station Info Diagnostics Management	Set WSC AP Mode Unconfigured Setup AP (Configure all security settings with an external registar) C Push-Button © PIN Config AP
	Device PIN Help
	WSC Add External Registrar Start AddER 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 "Save/Apply" when done.
	Select SSID: Comtrend Step 4
	WEP Encryption: Disabled Save/Apply

**Step 4:** Click the **Save/Apply** button at the bottom of the screen. The screen will go blank while the router applies the new Wireless settings. When the screen returns, press the **Start AddER** button, as shown above.

**Step 5:** Now return to the Network folder and click the BroadcomAP icon. A dialog box will appear asking for the Device PIN number. Enter the Device PIN as shown on the Wireless → Security screen. Click **Next**.

Configure a W	CN device			
Type the PI	N for the sele	ected device		
To configure information f	this device for us that came with th	se on your network, type ne device or on a sticker o	the PIN. You can find on the device.	the PIN in the
PIN:	The device Some device	PIN is usually eight digit: ces may use four digits, v	long and shown on t which are shown on a	he device using a label or on i device's display.
51048594				
<b>Display cha</b>	racters			
				Next Cancel

**Step 6:** Windows Vista will attempt to configure the wireless security settings.



**Step 7:** If successful, the security settings will match those in Windows Vista.