

EnGenius®

Wireless N Gigabit Router



User's Manual

Version: 1.0

Table of Contents

1	INTRODUCTION	5
1.1	FEATURES & BENEFITS	5
1.2	PACKAGE CONTENTS	6
1.3	SAFETY GUIDELINES	6
1.4	WIRELESS SOHO ROUTER DESCRIPTION	7
1.5	SYSTEM REQUIREMENTS	8
1.6	APPLICATIONS	8
1.7	NETWORK CONFIGURATION	9
2	UNDERSTANDING THE HARDWARE	10
2.1	HARDWARE INSTALLATION	10
2.2	IP ADDRESS CONFIGURATION	10
3	INTERNET CONNECTION WIZARD	12
3.1	LOGGING IN	12
3.1.1	DHCP CONNECTION (DYNAMIC IP ADDRESS)	15
3.1.2	PPPoE (POINT-TO-POINT PROTOCOL OVER ETHERNET)	16
3.1.3	PPTP (POINT-TO-POINT TUNNELING PROTOCOL)	17
3.1.4	L2TP (LAYER 2 TUNNELING PROTOCOL)	18
3.1.5	STATIC IP ADDRESS CONFIGURATION	19
3.1.6	BIGPOND	21
4	WI-FI PROTECTED SETUP WIZARD	22
4.1	LOGGING IN	22
4.2	ADD A WIRELESS DEVICE	22
4.2.1	USING THE PIN	23
4.2.2	USING THE PUSH BUTTON	24
5	WIRELESS NETWORK SETUP WIZARD	25
5.1	LOGGING IN	25
5.2	WIRELESS NETWORK SETUP	25
5.2.1	AUTOMATIC NETWORK SETUP	26
5.2.2	MANUAL NETWORK SETUP	26
5.2.2.1	WIRELESS SECURITY LEVEL: BEST (WPA2)	28
5.2.2.2	WIRELESS SECURITY LEVEL: BETTER (WPA)	29
5.2.2.3	WIRELESS SECURITY LEVEL: GOOD (WEP 64/128-BIT)	30
5.2.2.4	WIRELESS SECURITY LEVEL: NONE (SECURITY DISABLED)	31
6	ADVANCED WEB CONFIGURATION	32
6.1	LOGGING IN	32
6.2	BASIC	33
6.2.1	WIZARD_WIRELESS	33
6.2.2	NETWORK SETTINGS	33
6.2.2.1	BRIDGE MODE	33
6.2.2.2	ROUTER MODE	34
6.2.3	WIRELESS SETTINGS	35
6.2.3.1	WIRELESS SECURITY MODE	36
6.2.3.1.1	WEP (WIRED EQUIVALENT PRIVACY)	36
6.2.3.1.2	WPA PERSONAL (WI-FI PROTECTED ACCESS)	37
6.2.3.1.3	WPA ENTERPRISE (WI-FI PROTECTED ACCESS & 802.1X)	38
6.2.4	WAN SETTINGS	40
6.2.4.1	STATIC IP ADDRESS CONFIGURATION	40

Table of Contents

6.2.4.2	DHCP CONNECTION (DYNAMIC IP ADDRESS).....	41
6.2.4.3	PPPoE (POINT-TO-POINT PROTOCOL OVER ETHERNET).....	42
6.2.4.4	PPTP (POINT-TO-POINT TUNNELING PROTOCOL)	44
6.2.4.5	L2TP (LAYER 2 TUNNELING PROTOCOL)	45
6.2.5	BIGPOND.....	46
6.3	ADVANCED.....	48
6.3.1	ADVANCED WIRELESS.....	48
6.3.2	VIRTUAL SERVER.....	49
6.3.3	SPECIAL APPLICATIONS	50
6.3.4	PORT FORWARDING.....	51
6.3.5	STREAMENGINE	51
6.3.6	ROUTING	54
6.3.7	ACCESS CONTROL.....	54
6.3.8	WEB FILTER.....	57
6.3.9	MAC ADDRESS FILTER.....	57
6.3.10	FIREWALL	58
6.3.11	INBOUND FILTER.....	61
6.3.12	WISH	62
6.3.13	WI-FI PROTECTED SETUP	63
6.3.14	ADVANCED NETWORK (UPNP, WAN PING...).....	64
6.4	TOOLS.....	66
6.4.1	TIME ZONE SETTING	66
6.4.2	SYSTEM.....	67
6.4.2.1	SAVE CONFIGURATION TO A FILE	67
6.4.2.2	RESTORE THE CONFIGURATION FROM A FILE.....	68
6.4.2.3	RESTORE SETTINGS TO DEFAULT	69
6.4.2.4	SYSTEM REBOOT.....	69
6.4.3	FIRMWARE UPGRADE.....	70
6.4.4	SYSTEM LOGS.....	70
6.4.5	DYNAMIC DNS	71
6.4.6	SYSTEM CHECK.....	71
6.4.7	SCHEDULES.....	72
6.5	STATUS	73
6.5.1	WIRELESS STATUS.....	73
6.5.2	LOGS STATUS.....	73
6.5.3	STATISTICS	74
6.5.4	WISH SESSION STATUS	75
6.5.5	INTERNET SESSION STATUS	76
APPENDIX A – GLOSSARY		77
APPENDIX B – SPECIFICATIONS		89
	HARDWARE SUMMARY	89
	RADIO SPECIFICATIONS.....	89
	ROUTER AND GATEWAY.....	90
	MANAGEMENT.....	91
	ENVIRONMENT & PHYSICAL	92
APPENDIX C – FCC INTERFERENCE STATEMENT		93
APPENDIX D – INDEX.....		94

Revision History

Version	Date	Notes
1.0	September 12, 2007	Initial Version

1 Introduction

The Wireless-N Gigabit Router is a draft 802.11n compliant device that delivers up to 6x faster speeds than 802.11g while staying backward compatible with 802.11g and 802.11b devices.

It is not only a Wireless Access Point, which lets you connect to the network without wires. There's also a built-in 4-port full-duplex 10/100/1000 Gigabit Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

The Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel. The robust signal travels farther, maintaining wireless connections up to 3 times farther than standard 802.11g, eliminates dead spots and extends network range.

To protect the data and privacy, the Router can encode all wireless transmissions with 64/128-bit encryption. It can serve as your network's DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, and supports VPN pass-through. The router also provide easy configuration with the web browser-based configuration utility.

The incredible speed and QoS function of 802.11n (draft2.0) Gigabit Router is ideal for media-centric applications like streaming video, gaming, and VoIP telephony. It is designed to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1 Features & Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	Capable of handling heavy data payloads such as MPEG video streaming
IEEE 802.11n draft Compliant and backward compatible with 802.11b/g	Fully interoperable with IEEE 802.11b/g/n devices
Four built-in 10/100/1000Mbps Gigabit Switch Ports (Auto-Crossover)	Scalability, able to extend your network
Supports DNS/ DDNS	Lets users assign a fixed host and domain name to a dynamic Internet IP address.
Supports NAT (Network Address Translation)/NAPT	Shares single Internet account and provides a type of firewall by hiding internal IP addresses for keeping hacker out
Hide SSID	Avoids unallowable users sharing bandwidth, increases efficiency of the network
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking,	Avoids the attacks of Hackers or Viruses from Internet

SPI	
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-thru mechanisms	Provide mutual authentication (Client and dynamic encryption keys to enhance security
WDS (Wireless Distribution System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
Universal Plug and Play (UPnP™)	Works with most Internet gaming and instant messaging applications for automatic Internet access
Filter Scheduling	The filter can be scheduled by days, hours or minutes for easy management
Real time alert	The detection of a list for Hacker log-in information
Web configuration	Helps administrators to remotely configure or manage the Router via Telnet/Web-browser

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

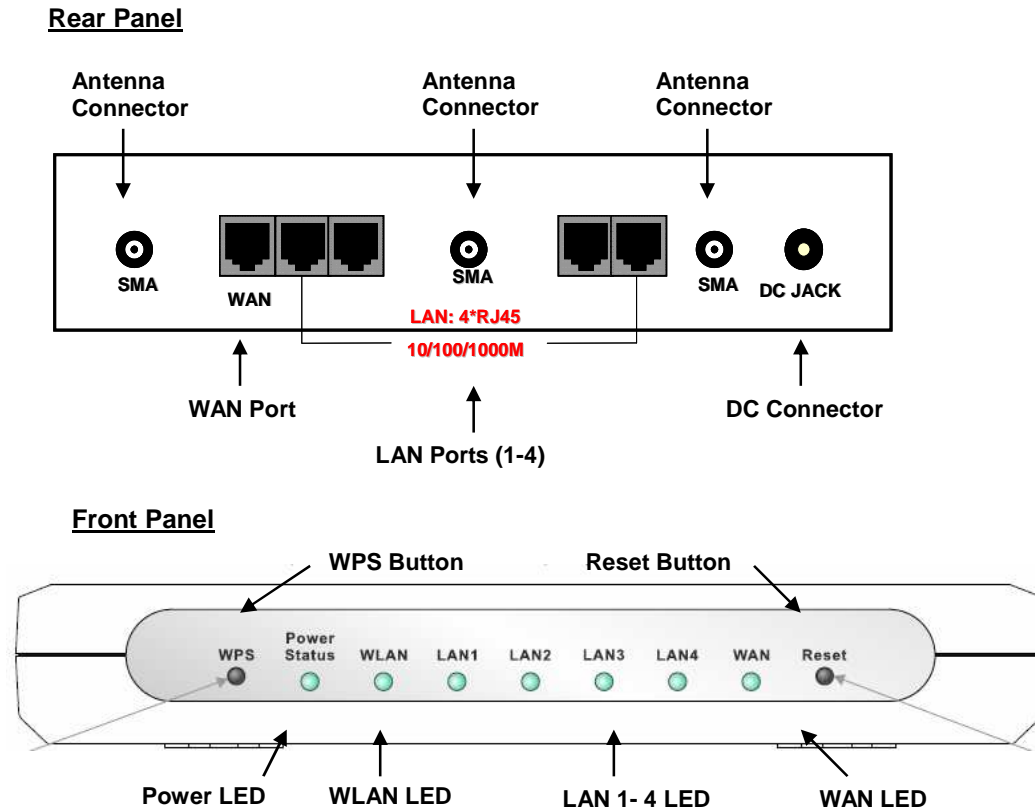
- One Wireless N Gigabit Router
- One 12V/1.25A 90V~240V Power Adapter
- Three 2dBi 2.4GHz Dipole Antennas
- One CD-ROM with User's Manual
- Once Quick Guide

1.3 Safety Guidelines

In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- Carefully follow the instructions in this manual; also follow all instruction labels on this device.
- Except for the power adapter supplied, this device should not be connected to any other adapters.
- Do not spill liquid of any kind on this device.
- Do not place the unit on an unstable stand or table. This unit may drop and become damaged.
- Do not expose this unit to direct sunlight.
- Do not place any hot devices close to this unit, as they may degrade or cause damage to the unit.
- Do not place any heavy objects on top of this unit.
- Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

1.4 Wireless SOHO Router Description



Step	Label	Description
1	LAN Ports (1 – 4)	Use an Ethernet cable to connect each port to a computer on your Local Area Network (LAN).
2	WAN Port	Use an Ethernet cable to connect this port to your WAN router.
3	DC Connector	Use the power cable and connect the adapter to the power socket on the wall, and the DC inlet into the DC connector.
4	Antenna Connector	Connect the three antennas to the SMA connectors.
	Connection / Activity LED	This LED will light up once an Ethernet cable is connected to one of the LAN ports.
	WAN LED	This LED will light up once an Ethernet cable is connected to WAN (Internet) port.
	WLAN LED	This LED will light up once the RF (wireless LAN) feature is enabled
	Power LED	This LED will light up once the power cable is connected to the DC connector.
	Reset Button	Use this button to reset the device. You can restore the device back to its factory default settings by holding down on this button for 5 seconds.
	WPS	WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the

		device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.
--	--	---

1.5 System Requirements

The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with a Ethernet interface.
- Operating system that supports HTTP web-browser

1.6 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) Difficult-to-wire environments

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) Temporary workgroups

Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) The ability to access real-time information

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) Frequently changed environments

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) Small Office and Home Office (SOHO) networks

SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

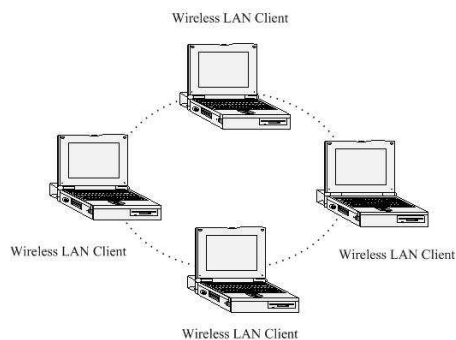
1.7 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.

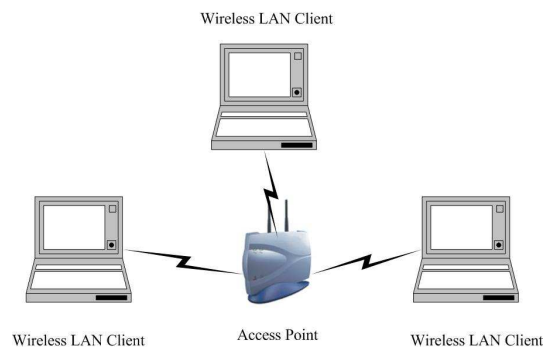
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.

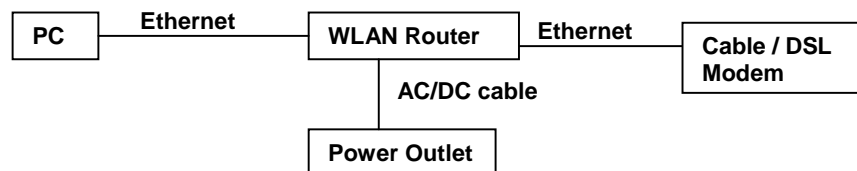


2 Understanding the Hardware

2.1 Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the LAN port of the device and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to WAN port of the device and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

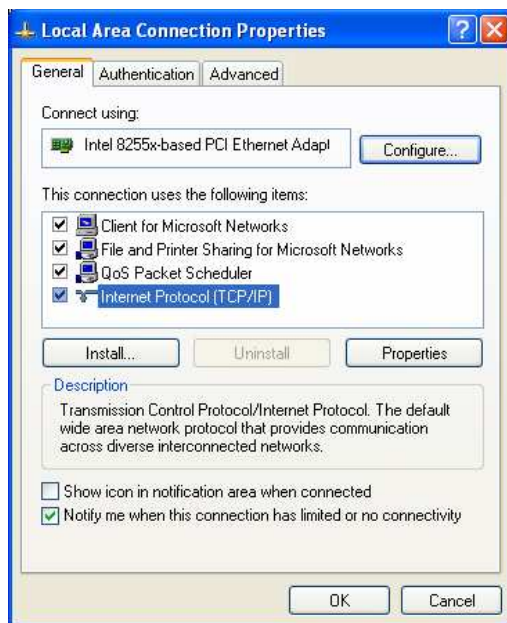
This diagram depicts the hardware configuration



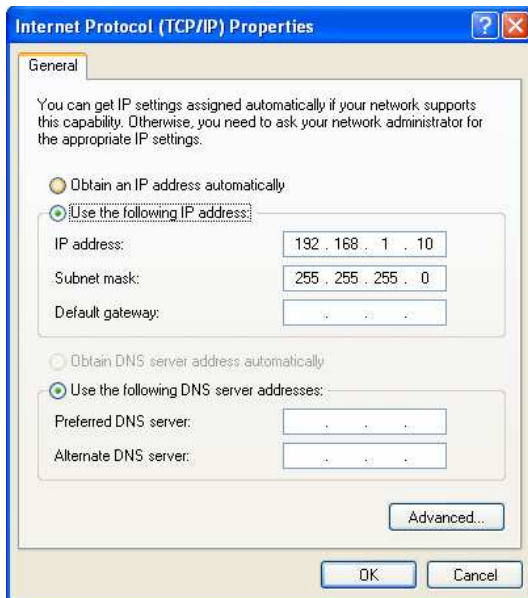
2.2 IP Address Configuration

This device can be configured as a Bridge/Router or Access Point. The default IP address of the device is **192.168.1.2** In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
For Example: Device IP address: 192.168.1.2
 PC IP address: 192.168.1.10
 PC subnet mask: 255.255.255.0
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Internet Connection Wizard

This device offers a quick and simple configuration through the use of wizards. This chapter describes how to use the wizard to configure the WAN, LAN, and wireless settings. Please refer to Chapter 6 in order to configure the more advanced features of the device.

3.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Select **Admin** from the drop-down list and then leave the password field blank. Click on the Log In button to continue.



The screenshot shows a login form with two main fields: 'User Name' and 'Password'. The 'User Name' field is a dropdown menu currently displaying 'Admin'. The 'Password' field is an empty text input box. To the right of the password field is a 'Log In' button. The form is enclosed in a light gray border with dashed lines above and below it.

- This device supports several types of WAN connections:
 - **DHCP Connection (Dynamic IP address)** – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection.
 - **PPPoE (Point-to-Point Protocol over Ethernet)** – Choose this option if your internet connection requires a user name and password. Most DSL modems use this type of connection.
 - **PPTP (Point-to-Point Tunneling Protocol)** – Choose this type of connection if your ISP requires you to use PPTP. Your ISP should provide you with a user name and password.
 - **Static IP address** – Choose this option if you have a dedicated IP address.
 - **BigPond** – Choose this option if you use the BigPond service in Australia.
- The configuration wizard for each connection type is described below.
- Click on the **Internet Connection Setup Wizard** button to begin the process.

Internet Connection

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

Internet Connection Setup Wizard

If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your router to the Internet, click on the button below.

Internet Connection Setup Wizard

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Manual Internet Connection Options

If you would like to configure the Internet settings of your router manually, then click on the button below.

Manual Internet Connection Setup

- Click on the **Internet Connection Setup Wizard Setup** button to begin the process.

Welcome to the Internet Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your router and connect to the Internet.

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

Prev

Next

Cancel

Connect

- The Wizard requires that you configure the password, time zone, and Internet (WAN) connection. Click on the **Next** button to continue.

Step 1: Set your Password

By default, your router does not have a password configured for administrator access to the Web-based configuration page. For a new networking device, please set and verify a password below:

Password :

Verify Password :

Prev

Next

Cancel

Connect

- By default, the device does not use a password. Specify a password for administrator access to the device, then type the password once more in the **Verify Password** field. Click on the **Next** button to continue.

Step 2: Select your Time Zone

Select the appropriate time zone for your location. This information is required to configure the time-based options f

Time Zone :

- Select your time zone from the drop-down list Click on the **Next** button to continue.
- The next step in the wizard is the Internet Connection, select the WAN connection type from the list, and then click on the **Next** button to continue with the wizard.

Step 3: Configure your Internet Connection

Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed; select the "Not Listed or Don't Know" option to manually configure your connection.

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
PPTP client.

Username / Password Connection (L2TP)
L2TP client.

Static IP Address Connection
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
BigPond Cable (Australia)

3.1.1 DHCP Connection (Dynamic IP Address)

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
 Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
 PPTP client.

Username / Password Connection (L2TP)
 L2TP client.

Static IP Address Connection
 Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
 BigPond Cable (Australia)

Prev Next Cancel Connect

- Select the **DHCP Connection (Dynamic IP Address)** radio button and then click on the **Next** button.

DHCP Connection (Dynamic IP Address)

To set up this connection, please make sure that you are connected to the router with the PC that was originally connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the router.

MAC Address : (optional)

Host Name :

Note: You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

Prev Next Cancel Connect

- You have the option of cloning your PCs MAC address onto the device. Click on the **Clone Your PCs MAC Address** to automatically copy the MAC address. You may also specify a host name. Click on the **Next** button to continue.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

Prev Next Cancel Connect

- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

3.1.2 PPPoE (Point-to-Point Protocol over Ethernet)

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
 Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
 PPTP client.

Username / Password Connection (L2TP)
 L2TP client.

Static IP Address Connection
 Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
 BigPond Cable (Australia)

- Select the **Username / Password Connection (PPPoE)** radio button and then click on the **Next** button.

Address Mode : Dynamic IP Static IP

IP Address :

User Name :

Password :

Verify Password :

Service Name : (optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

- **Address Mode:** PPPoE can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Service Name:** Specify the name of the ISP.
- Click on the **Next** button to continue.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

3.1.3 PPTP (Point-to-Point Tunneling Protocol)

- The WAN interface can be configured as PPTP. PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
 Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
 PPTP client.

Username / Password Connection (L2TP)
 L2TP client.

Static IP Address Connection
 Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
 BigPond Cable (Australia)

- Select the **Username / Password Connection (PPTP)** radio button and then click on the **Next** button.

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

- **Address Mode:** PPTP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **PPTP Address:** Specify the IP address
- **PPTP Subnet Mask:** Specify the subnet mask for the IP address.
- **PPTP Gateway IP Address:** Specify the IP address of the PPTP gateway.
- **PPTP Server IP Address:** If the PPTP Server's IP address is different from the default gateway, then you may specify it here.

- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- Click on the **Next** button to continue.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.



- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

3.1.4 L2TP (Layer 2 Tunneling Protocol)

- The WAN interface can be configured as L2TP. L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a user name and password (provided by your Internet Service Provider) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
PPTP client.

Username / Password Connection (L2TP)
L2TP client.

Static IP Address Connection
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
BigPond Cable (Australia)



- Select the **Username / Password Connection (L2TP)** radio button and then click on the **Next** button.

Address Mode :	<input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP
L2TP IP Address :	<input type="text" value="192.168.2.23"/>
L2TP Subnet Mask :	<input type="text" value="255.255.255.0"/>
L2TP Gateway IP Address :	<input type="text" value="192.168.2.24"/>
L2TP Server IP Address (may be same as gateway) :	<input type="text" value="192.168.2.25"/>
User Name :	<input type="text" value="12436"/>
Password :	<input type="password" value="•••••"/>
Verify Password :	<input type="password" value="•••••"/>

- **Address Mode:** L2TP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **L2TP Address:** Specify the IP address
- **L2TP Subnet Mask:** Specify the subnet mask for the IP address.
- **L2TP Gateway IP Address:** Specify the IP address of the L2TP gateway.
- **L2TP Server IP Address:** If the L2TP Server's IP address is different from the default gateway, then you may specify it here.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- Click on the **Next** button to continue.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

3.1.5 Static IP Address Configuration

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address (which does not change as DHCP).

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
 Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
 PPTP client.

Username / Password Connection (L2TP)
 L2TP client.

Static IP Address Connection
 Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
 BigPond Cable (Australia)

- Select the **Static IP Address Connection** radio button and then click on the **Next** button.

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you do not have this information, please contact your ISP.

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Address :

Secondary DNS Address :

- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Gateway Address:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

3.1.6 BigPond

- The WAN interface can be configured as BigPong. This type of service is used through Telstra BigPond Cable Broadband in Australia

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)
 Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

Username / Password Connection (PPPoE)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

Username / Password Connection (PPTP)
 PPTP client.

Username / Password Connection (L2TP)
 L2TP client.

Static IP Address Connection
 Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

BigPond
 BigPond Cable (Australia)

Prev Next Cancel Connect

- Select the **BigPond** radio button and then click on the **Next** button.

User Name : pond01
 Password : ●●●●●●
 Verify Password : ●●●●●●
 BigPond Server : pond.com

Prev Next Cancel Connect

- User Name:** Specify the user name which is provided by your ISP.
- Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- BigPond Server:** Specify the server name or IP address as specified by your ISP.
- Click on the **Next** button to continue.

Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

Prev Next Cancel Connect

- The WAN configuration is complete. Click on the **Connect** button to connect to the Internet.

4 Wi-Fi Protected Setup Wizard

Wi-Fi Protected Setup is a feature that locks the wireless security settings and prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup.

.Please refer to Chapter 6 in order to configure the more advanced features of the device

4.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Select **Admin** from the drop-down list and then leave the password field blank. Click on the **Log In** button to continue.

The screenshot shows a login form with the following elements:

- User Name :** A dropdown menu with 'Admin' selected.
- Password :** An empty text input field.
- Log In** button.

4.2 Add a Wireless Device

- Click on the **Wizard_Wireless** link under the **Basic** menu, and then click on the **Add Wireless Device Wizard** button.

Wireless Settings

The following Web-based wizards are designed to assist you in your wireless network setup and wireless. Before launching these wizards, please make sure you have followed all steps outlined in the Quick Install package.

Add Wireless Device Wizard

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through to get your wireless device connected. Click the button below to begin.

Add Wireless Device Wizard

Wireless Network Setup Wizard

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions to network and how to make it secure.

Wireless Network Setup Wizard

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client and the router.

Manual Wireless Network Setup

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will not be necessary. If you would like to configure the wireless settings of your router manually, then click on the Manual Wireless N

Manual Wireless Network Setup

- The wireless wizard will inform you that there are two major steps in the process.
 - Select the configuration method for your wireless network
 - Connect your wireless device



- Click on the **Next** button to continue.
- You may select from three available options:
 - **PIN:** Select this radio button if your wireless device supports PIN
 - **Push Button:** Select this radio button if your wireless device supports push button.
 - **Manual:** Select the radio button if you would like to setup your wireless device manually. Refer to chapter 5 in order to manually configure the device.
- The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.
- There are several ways to add a wireless device to your network. Access to the wireless network is controlled by a registrar. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.



4.2.1 Using the PIN

- A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

Step 1: Select Configuration Method for your Wireless Network

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

PIN Select this option if your wireless device supports PIN
 Push Button Select this option if your wireless device supports push button
 Manual Select this option if you want to configure your wireless device manually

- Select the **PIN** radio button and then click on the **Next** button.

Step 2: Connect your Wireless Device

Please enter the PIN of your wireless device, then click on the Connect button below.

Wireless Device PIN :

- Specify the PIN and then click on the **Connect** button.
- The wireless device configuration is now complete.

4.2.2 Using the Push Button

- WPS is used for WiFi Protected Setup. By pressing the WPS button on the front panel of the device, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup
- If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

Step 1: Select Configuration Method for your Wireless Network

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

PIN Select this option if your wireless device supports PIN
 Push Button Select this option if your wireless device supports push button
 Manual Select this option if you want to configure your wireless device manually

- Select the **Push Button** radio button and then click on the **Next** button.

Step 2: Connect your Wireless Device

Please push button on your wireless device, then click on the Connect button below.

- Press the **WPS** button on the device (which is located on the left side of the front panel) and then click on the **Next** button.

5 Wireless Network Setup Wizard

This wizard will guide you in the configuration of the wireless network settings such as the SSID and security (WEP/WPA).

Please refer to Chapter 6 in order to configure the more advanced features of the device

5.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Select **Admin** from the drop-down list and then leave the password field blank. Click on the **Log In** button to continue.

The screenshot shows a login form with the following elements:

- User Name :** A dropdown menu with 'Admin' selected.
- Password :** An empty text input field.
- Log In** button.

5.2 Wireless Network Setup

- Click on the **Wizard_Wireless** link under the **Basic** menu, and then click on the **Wireless Network Setup Wizard** button.

Wireless Settings

The following Web-based wizards are designed to assist you in your wireless network setup and wireless. Before launching these wizards, please make sure you have followed all steps outlined in the Quick Install package.

Add Wireless Device Wizard

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through to get your wireless device connected. Click the button below to begin.

Add Wireless Device Wizard

Wireless Network Setup Wizard

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions to network and how to make it secure.

Wireless Network Setup Wizard

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client and the router.

Manual Wireless Network Setup

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will not be required. If you would like to configure the wireless settings of your router manually, then click on the Manual Wireless N

Manual Wireless Network Setup

- The wizard will inform you that there are two options: auto and manual.

Please Select Configuration Method to setup your Wireless Network

Auto Select this option if your wireless device supports Wi-Fi Protected Setup
Manual Select this option if you want to setup your network manually

5.2.1 Automatic Network Setup

- If you select the **Auto** option, then the device will automatically configure the SSID and security mode.

Please Select Configuration Method to setup your Wireless Network

Auto Select this option if your wireless device supports Wi-Fi Protected Setup
Manual Select this option if you want to setup your network manually

- Click on the **Next** button to continue.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Media Gateway_31334455
 Security Mode : Auto (WPA or WPA2) - Personal
 Cipher Type : TKIP and AES
 Pre-Shared Key : 99015d099de49a05ddf542421593ac54a32749d0fb10d807bdba2573ae95095d

- The wizard has automatically configured the SSID and security mode for the device. Click on the **Save** button to complete the setup.

5.2.2 Manual Network Setup

- If you select the **Manual** option, then you will be required to specify the SSID and select the appropriate network security.

Please Select Configuration Method to setup your Wireless Network

Auto Select this option if your wireless device supports Wi-Fi Protected Setup
Manual Select this option if you want to setup your network manually

- Click on the **Next** button to continue.
- The wireless wizard will inform you that there are three major steps in the process.
 - Name your wireless network
 - Secure your wireless network
 - Set your wireless security password

Welcome to the Wireless Security Setup Wizard

This wizard will guide you through a step-by-step process to set up your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

Prev Next Cancel Save

- Click on the **Next** button to continue.

Step 1: Name your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes change the pre-configured network name.

Wireless Network Name (SSID) : Engenius_Gateway

Prev Next Cancel Save

- Specify the Wireless Network Name (SSID) for the device. The SSID is a unique name shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. Click on the **Next** button to continue.

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support.

- BEST** Select this option if your wireless adapters SUPPORT WPA2
- BETTER** Select this option if your wireless adapters SUPPORT WPA
- GOOD** Select this option if your wireless adapters DO NOT SUPPORT WPA
- NONE** Select this option if you do not want to activate any security features

Prev Next Cancel Save

- This step requires that you configure the security features based on your needs. The following options are available.
 - **BEST** – Select this option if your wireless adapters support WPA2
 - **BETTER** – Select this option if your wireless adapters support WPA
 - **GOOD** – Select this option if your wireless adapters do not support WPA, but support WEP instead
 - **None**: Select this option if you do not want to activate any security features.
- In order to protect your network from hackers and unauthorized users, it is highly recommended to secure the network using encryption and authentication. Select a level of security and then click on the **Next** button to continue.
- If you do not want to setup security, then select the **NONE** radio button.

5.2.2.1 Wireless Security Level: BEST (WPA2)

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support.

- BEST** Select this option if your wireless adapters SUPPORT WPA2
BETTER Select this option if your wireless adapters SUPPORT WPA
GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA
NONE Select this option if you do not want to activate any security features

Prev Next Cancel Save

- Select the **BEST** radio button which supports WPA2 encryption. Then click on the **Next** button.

Step 3: Set your Wireless Security Password

You have selected your security level - you will need to set a wireless security password.

Wireless Security Password : (8 to 63 characters)

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Prev Next Cancel Save

- Enter a security password between 2 and 20 characters then click on the **Next** button.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information down to configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Engenius_Gateway

Encryption : WPA2-PSK/AES (also known as WPA2 Personal)

Pre-Shared Key : 9038475938745

Prev Next Cancel Save

- The setup is complete. Click on the **Save** button and then reboot the device.

5.2.2.2 Wireless Security Level: BETTER (WPA)

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support.

- BEST** Select this option if your wireless adapters SUPPORT WPA2
BETTER Select this option if your wireless adapters SUPPORT WPA
GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA
NONE Select this option if you do not want to activate any security features

- Select the **BETTER** radio button which supports WPA encryption. Then click on the **Next** button.

Step 3: Set your Wireless Security Password

You have selected your security level - you will need to set a wireless security password.

Wireless Security Password : (8 to 63 characters)

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

- Enter a security password between 2 and 20 characters then click on the **Next** button.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Engenius_Gateway

Encryption : WPA-PSK/TKIP (also known as WPA Personal)

Pre-Shared Key : 9038475938745

- The setup is complete. Click on the **Save** button and then reboot the device.

5.2.2.3 Wireless Security Level: GOOD (WEP 64/128-bit)

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support.

- BEST** Select this option if your wireless adapters SUPPORT WPA2
BETTER Select this option if your wireless adapters SUPPORT WPA
GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA
NONE Select this option if you do not want to activate any security features

Prev Next Cancel Save

- Select the **GOOD** radio button which supports WEP encryption. Then click on the **Next** button.

Step 3: Set your Wireless Security Password

You have selected your security level - you will need to set a wireless security password.

Wireless Security Password : 123456789012345678901234567 (13 characters or 26 hex digits)

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Prev Next Cancel Save

- Enter a security password between 2 and 20 characters then click on the **Next** button.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information down so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Engenius_Gateway
 Wep Key Length : 128 bits
 Default WEP Key to Use : 1
 Authentication : Open
 Wep Key : 123456789012345678901234567

Prev Next Cancel Save

- The setup is complete. Click on the **Save** button and then reboot the device.

5.2.2.4 Wireless Security Level: None (Security Disabled)

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are several levels of wireless security. The level you choose depends on the security features your wireless adapters support.

- BEST** Select this option if your wireless adapters SUPPORT WPA2
- BETTER** Select this option if your wireless adapters SUPPORT WPA
- GOOD** Select this option if your wireless adapters DO NOT SUPPORT WPA
- NONE** Select this option if you do not want to activate any security features

[Prev](#) [Next](#) [Cancel](#) [Save](#)

- Select the **NONE** radio button if you do not want to activate any security features. Then click on the **Next** button.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : Engenius_Gateway

[Prev](#) [Next](#) [Cancel](#) [Save](#)

- The setup is complete. Click on the **Save** button and then reboot the device.

6 Advanced Web Configuration

6.1 Logging In

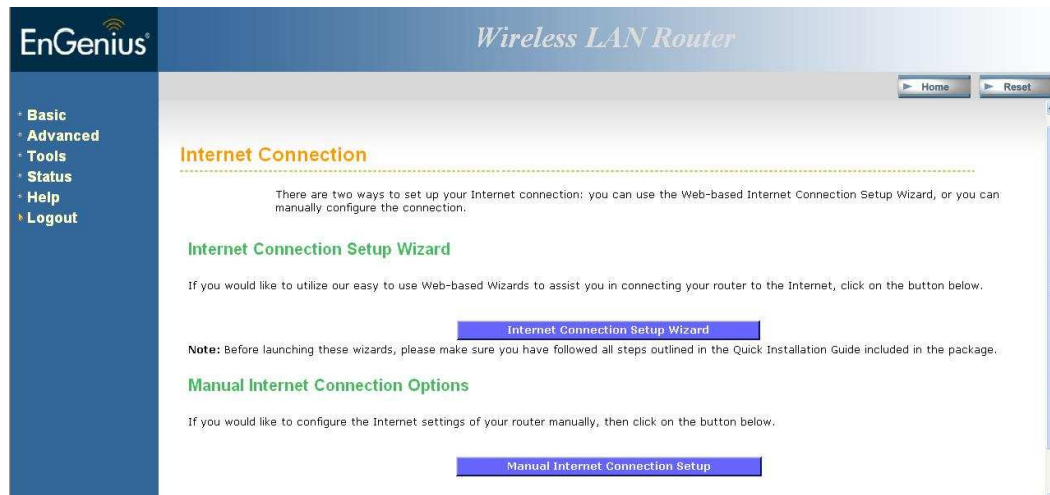
- To configure the device through the web-browser, enter the IP address of the Bridge (default: **192.168.1.2**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Select Admin from the drop-down list and then leave the password field blank.



The screenshot shows a login form with a dashed yellow border. It contains a 'User Name' label followed by a dropdown menu currently showing 'Admin'. Below that is a 'Password' label followed by an empty text input field. To the right of the password field is a 'Log In' button.

After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into six main sections:

1. **Basic:** This menu includes the wireless wizard, network settings, wireless settings, and WAN settings.
2. **Advanced:** This menu includes virtual server, special applications, port forwarding, routing, access control, web filter, MAC address filter, firewall, etc.
3. **Tools:** This menu includes time, firmware, system log, DDNS, schedules, etc.
4. **Status:** This menu displays the wireless status, logs, statistics, routing, and internet sessions.
5. **Help:** Displays the help for configuring the device.
6. **Logout:** Used to logout of the device.



6.2 Basic



- Click on the **Basic** link on the navigation drop-down menu. You will then see four options: Wizard_Wireless, Network Settings, Wireless Settings, and WAN Settings.

6.2.1 Wizard_Wireless

- Refer to Chapters 4 and 5 in order to use the wireless wizard. The other options are described below.

6.2.2 Network Settings

- This device can be configured at a **Router** or a **Bridge**. Select Router mode if the WAN port is connected to the Internet. Select Bridge if the device is connected to a local network downstream from another router.

6.2.2.1 Bridge Mode

- In this mode, the device functions as a bridge between the network on its WAN port and the devices on its LAN port and those connected to it wirelessly. Select the **Bridge Mode** radio button.

WAN Port Mode

WAN Port Mode : Router Mode Bridge Mode

Router Settings

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network again.

Router IP Address:
 Subnet Mask:
 Default Gateway:
 Primary DNS Server:
 Secondary DNS Server:

- **WAN Port Mode:** Select the **Bridge Mode** radio button.
- **Router IP Address:** Specify the IP address of this device.
- **Subnet Mask:** Specify the subnet mask for the IP address.
- **Default Gateway:** Specify the IP address of the upstream router.
- **Primary/Secondary DNS:** Specify the IP address of the DNS server.
- Click on the **Save Changes** button to store these settings.

6.2.2.2 Router Mode

- In this mode, the device functions as a NAT router and is connected to the Internet. Select the **Router Mode** radio button.

WAN Port Mode

WAN Port Mode : Router Mode Bridge Mode

Router Settings

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network again.

Router IP Address:
 Subnet Mask:
 Local Domain Name: (optional)
 Enable DNS Relay:

- **WAN Port Mode:** Select the **Router Mode** radio button.
- **Router IP Address:** Specify the IP address of this device
- **Subnet Mask:** Specify the subnet mask for the IP address
- **Local Domain Name:** This entry is optional. Enter a domain name for the local network. LAN computers will assume this domain name when they get an address from the router's built in DHCP server. So, for example, if you enter mynetwork.net here, and you have a LAN side laptop with a name of chris, that laptop will be known

as chris.mynetwork.net. Note, however, the entered domain name can be overridden by the one obtained from the router's upstream DHCP server.

- **Enable DNS Relay:** Place a check in this box to enable the DNS relay feature. When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.
- Click on the **Save Changes** button to store these settings.

6.2.3 Wireless Settings

- These options allow you to enable/disable the wireless interface, switch between the 11n, 11b/g and 11b radio band and channel frequency

Wireless

Use this section to configure the wireless settings for your router. Please note that changes made are duplicated on your Wireless Client.

Save Settings
Don't Save Settings

Wireless Network Settings

Enable Wireless :

Wireless Network Name : (Also called the SSID)

802.11 Mode :

Enable Auto Channel Scan :

Wireless Channel :

Transmission Rate : (Mbit/s)

Channel Width :

Visibility Status : Visible Invisible

- **Enable Wireless:** Place a check in this box to enable the wireless interface, it is enabled by default.
- **Wireless Network Name:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.

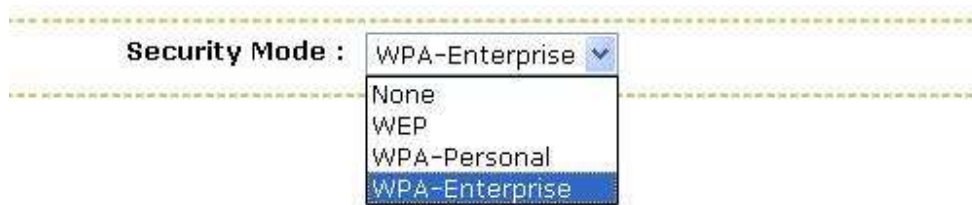
802.11 Mode: Select the IEEE 802.11 mode from the drop-down list. For example, if you are sure that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **2.4 GHz B+G** which will reduce the performance of the wireless network. You may also select **Mixed 802.11n, 802.11g and 802.11b**. If all of the wireless devices you want to connect with this router can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Wireless Channel: Select a channel from the drop-down list. The channels available are based on the country's regulation. A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

- **Transmission Rate:** Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- **Channel Width:** Select a channel width from the drop-down list.
- **Visibility Status:** Select **Visible** or **Invisible**. This is the SSID broadcast feature. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **Show Active Clients:** Click on this button to view a list of clients that are associated with this device.
- Click on the **Save Changes** button to store these settings.

6.2.3.1 Wireless Security Mode

- To protect your privacy this mode supports several types of wireless security: WEP, WPA, WPA2, and WPA-Mixed. WEP is the original wireless encryption standard. WPA provides a higher level of security. The following section describes the security configuration in detail.



6.2.3.1.1 WEP (Wired Equivalent Privacy)

- Select the **WEP** radio button if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.
- WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit key

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means performance due to the fact that WEP is not supported by Draft 11N specification.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key : WEP Key 1

Authentication : Open

Open

Shared Key

- **WEP Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Changes** button to store these settings.

6.2.3.1.2 WPA Personal (Wi-Fi Protected Access)

- Select the **WPA-Personal** radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client support security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher \ network to ensure best security.

WPA Mode :	Auto (WPA or WPA2) ▼
Cipher Type :	TKIP and AES ▼
Group Key Update Interval :	3600 (seconds)

Pre-Shared Key

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a

Pre-Shared Key :	••••••••
-------------------------	----------

- **WPA Mode:** Select the **Auto WPA / WPA2** from the drop-down list.
- **Cipher Type:** Select **TKIP and AES** as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval:** Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Changes** button to store these settings.

6.2.3.1.3 WPA Enterprise (Wi-Fi Protected Access & 802.1x)

- Select the WPA-Enterprise radio button if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

EAP (802.1x)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout :	<input type="text" value="60"/> (minutes)
RADIUS server IP Address :	<input type="text" value="0.0.0.0"/>
RADIUS server Port :	<input type="text" value="1812"/>
RADIUS server Shared Secret :	<input type="password" value="....."/>
MAC Address Authentication :	<input checked="" type="checkbox"/>
<< Advanced	
Optional backup RADIUS server :	
Second RADIUS server IP Address :	<input type="text" value="0.0.0.0"/>
Second RADIUS server Port :	<input type="text" value="1812"/>
Second RADIUS server Shared Secret :	<input type="password" value="....."/>
Second MAC Address Authentication :	<input checked="" type="checkbox"/>

- **WPA Mode:** Select the WPA / WPA2 from the drop-down list.
- **Cipher Type:** Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval:** Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Authentication Timeout:** Specify the number of minutes after which the client will be required to re-authenticate.
- **RADIUS Server IP Address:** Specify the IP address of the RADIUS server.
- **RADIUS Server Port:** Specify the port number of the RADIUS server, the default port is 1812.
- **RADIUS Server Shared Secret:** Specify the pass-phrase that is matched on the RADIUS Server.
- **MAC Address Authentication:** Place a check in this box if you would like the user to always authenticate using the same computer.
- **Optional Backup RADIUS server:** This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding.
- Click on the **Save Changes** button to store these settings.

6.2.4 WAN Settings

- The device offers several types of WAN connections in order to connect to the Internet.
 - Static IP Address
 - Dynamic IP Address
 - PPPoE
 - PPTP
 - L2TP
 - BigPond

WAN

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.

Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings Don't Save Settings

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

Dynamic IP (DHCP) Internet Connection Type

Use this Internet connection type if your Internet Service Provider provides you with IP Address information and/or a username and password.

Dynamic IP (DHCP)
Static IP
Dynamic IP (DHCP)
PPPoE (Username / Password)
PPTP (Username / Password)
L2TP (Username / Password)
BigPond (Australia)

- Select the type of Internet Connection from the drop-down list.

6.2.4.1 Static IP Address Configuration

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address (which does not change as DHCP).
- Select the **Static IP** from the **My Internet Connection** drop-down list.

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

Static IP Address Internet Connection Type :

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Default Gateway :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>
MTU :	<input type="text" value="1500"/> (bytes) MTU default = 1500
MAC Address :	<input type="text" value="00:15:c5:61:a2:91"/>
<input type="button" value="Clone Your PC's MAC Address"/>	

- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Default Gateway:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PC's MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.2.4.2 DHCP Connection (Dynamic IP Address)

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.
- Select the **Dynamic IP (DHCP)** from the **My Internet Connection** drop-down list.

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

Dynamic IP (DHCP) Internet Connection Type :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Use Unicasting : (compatibility for some DHCP Servers)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1500

MAC Address :

- **Host Name:** Specify a host name to define your system or connection.
- **Use Unicasting:** This option is normally turned off, and should remain off as long as the WAN-side DHCP server correctly provides an IP address to the router. However, if the router cannot obtain an IP address from the DHCP server, the DHCP server may be one that works better with unicast responses. In this case, turn the unicasting option on, and observe whether the router can obtain an IP address. In this mode, the router accepts unicast responses from the DHCP server instead of broadcast responses.
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PC's MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.2.4.3 PPPoE (Point-to-Point Protocol over Ethernet)

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.
- Select the **PPPoE** from the **My Internet Connection** drop-down list.

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

PPPOE Internet Connection Type :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode :	<input checked="" type="radio"/> Dynamic IP	<input type="radio"/> Static IP	
IP Address :	<input type="text" value="0.0.0.0"/>		
Username :	<input type="text"/>		
Password :	<input type="password" value="•••••"/>		
Verify Password :	<input type="password" value="•••••"/>		
Service Name :	<input type="text"/>	(optional)	
Reconnect Mode :	<input type="radio"/> Always on	<input checked="" type="radio"/> On demand	<input type="radio"/> Manual
Maximum Idle Time :	<input type="text" value="20"/>	(minutes, 0=infinite)	
Primary DNS Server :	<input type="text" value="0.0.0.0"/>		
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>		
MTU :	<input type="text" value="1492"/>	(bytes) MTU default = 1492	
MAC Address :	<input type="text" value="00:00:00:00:00:00"/>		
	<input type="button" value="Clone Your PC's MAC Address"/>		

- **Address Mode:** PPPoE can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Service Name:** Specify the name of the ISP.
- **Reconnect Mode:** Select a reconnection time: **Always on** (A connection to the Internet is always maintained), **On demand** (A connection to the Internet is made as needed), **Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
- Maximum Idle Time:
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PC's MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.2.4.4 PPTP (Point-to-Point Tunneling Protocol)

- The WAN interface can be configured as PPTP. PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.
- Select the **PPTP** from the **My Internet Connection** drop-down list.

My Internet Connection is :

PPTP Internet Connection Type :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1452

MAC Address :

- **Address Mode:** PPTP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **PPTP Address:** Specify the IP address
- **PPTP Subnet Mask:** Specify the subnet mask for the IP address.
- **PPTP Gateway IP Address:** Specify the IP address of the PPTP gateway.
- **PPTP Server IP Address:** If the PPTP Server's IP address is different from the default gateway, then you may specify it here.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Reconnect Mode:** Select a reconnection time: **Always on** (A connection to the Internet is always maintained), **On demand** (A connection to the Internet is made as needed), **Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
- **Maximum Idle Time:**
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices

send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PC's MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.2.4.5 L2TP (Layer 2 Tunneling Protocol)

- The WAN interface can be configured as L2TP. L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a user name and password (provided by your Internet Service Provider) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.
- Select the **L2TP** from the **My Internet Connection** drop-down list.

My Internet Connection is :

L2TP Internet Connection Type :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1464

MAC Address :

- **Address Mode:** L2TP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **L2TP Address:** Specify the IP address
- **L2TP Subnet Mask:** Specify the subnet mask for the IP address.
- **L2TP Gateway IP Address:** Specify the IP address of the L2TP gateway.

- **L2TP Server IP Address:** If the L2TP Server's IP address is different from the default gateway, then you may specify it here.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Reconnect Mode:** Select a reconnection time: **Always on** (A connection to the Internet is always maintained), **On demand** (A connection to the Internet is made as needed), **Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
- Maximum Idle Time:
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PC's MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.2.5 BigPond

- The WAN interface can be configured as BigPong. This type of service is used through Telstra BigPond Cable Broadband in Australia
- Select the **BigPond** from the **My Internet Connection** drop-down list.

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

Big Pond Internet Connection Type :

Enter the information provided by your Internet Service Provider (ISP).

BigPond Server :

BigPond User Id :

BigPond Password :

Verify Password :

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1500

MAC Address :

- **BingPond Server:** Specify the server name or IP address as specified by your ISP.
- **User Name:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **MAC Address:** If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PCs MAC Address**.
- Click on the **Save Settings** button to store these settings.

6.3 Advanced



- Click on the **Advanced** link on the navigation drop-down menu. You will then see thirteen options: Virtual Server, Special Applications, Port Forwarding, StreamEngine, Routing, Access Control, Web Filter, MAC Address Filter, Firewall, Inbound Filter, WISH, Wi-Fi Protected Setup and Advanced Network. The configuration steps for each option are described below.

6.3.1 Advanced Wireless

- This page allows you to configure the fragmentation threshold, RTS threshold, beacon period, transmit power, DTIM interval, wireless isolation, WMM, and WDS (wireless distribution system).

Advanced Wireless Settings

Transmit Power :	High	▼
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
Wireless Isolation :	<input type="checkbox"/>	
WMM Enable :	<input checked="" type="checkbox"/>	
Short GI :	<input checked="" type="checkbox"/>	
WDS Enable :	<input type="checkbox"/>	

- **Transmit Power:** You may control the output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Beacon Period:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 1 and 65535. The default value is 2346.
- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 65535. The default value is 2346.
- **DTIM Interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Wireless Isolation:** Place a check in this box in order to prevent associated wireless clients from communicating with each other.
- **WMM Enable:** Enable WMM in order to help control latency and jitter when transmitting multimedia content over a wireless connection.
- **WDS:** Place a check in this box to enable WDS (Wireless Distribution System). When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links.
Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.
- **WDS AP MAC Address:** Specify one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.
- Click on the **Save Settings** button to store these changes.

6.3.2 Virtual Server

- The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port.

Add Virtual Server Rule

Enable :
 Name : TELNET TELNET
 IP Address : 192.168.1.199 rdw-user (192.168.1.199)
 Protocol : TCP
 Public Port : 23
 Private Port : 23
 Schedule : Always
 Inbound Filter : Allow All

Virtual Server List

	Name	IP Address	Protocol / Ports	Schedule	Inbound Filter	Edit	Delete
<input checked="" type="checkbox"/>	POP3	192.168.1.199	TCP 110 → 110	Always	Allow All		
<input type="checkbox"/>	FTP	192.168.1.199	TCP 21 → 21	Always	Allow All		

- **Enable:** Place a check in this box to enable the virtual server rule.
- **Name:** Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the **Application Name** drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address:** Specify the IP address for the virtual server entry.
- **Protocol:** Specify a protocol or select one from the drop-down list.
- **Public Port:** Specify the public port number.
- **Private Port:** Specify the private port number.
- **Schedule:** Select a **schedule**, **Always**, or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- **Inbound Filter:** Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Save** button to insert the entry into the Virtual Server list.

6.3.3 Special Applications

- An application rule is used to open single or multiple ports on your router when the router senses data sent to the Internet on a trigger port or port range. An application rule applies to all computers on your internal network.

Add Application Rule

Enable :
 Name : AIM Talk AIM Talk
 Trigger ports : TCP 4099
 Firewall ports : TCP 5190
 Schedule : Always

Application Rules

Enable	Rule Name	Trigger Ports	Firewall Ports	Schedule	Edit	Delete
<input checked="" type="checkbox"/>	BitTorrent	TCP: 6969	TCP: 6881-6889	Always		
<input checked="" type="checkbox"/>	MSN Messenger	Both: 1863,5190,6891,6901	Both: 1863,5190,6891,6901	Always		

- **Enable:** Place a check in this box to enable the special application rule.
- **Name:** Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the **Application Name**

drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

- **Triggering Ports:** Specify the outgoing port range that is used by the application.
- **Firewall Ports:** Specify the port range that you would like to open for Internet traffic.
- **Schedule:** Select a **schedule**, **Always**, or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- Click on the **Save** button to insert the entry into the Special Applications list.

6.3.4 Port Forwarding

- Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.

Add Port Forwarding Rule

Port Forwarding Rules

Enable	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter	Edit	Delete
<input checked="" type="checkbox"/>	Age of Empires	192.168.1.199	2302-2400, 6073	2302-2400, 6073	Always	Allow All		
<input checked="" type="checkbox"/>	eMule	192.168.1.199	4661-4662, 4711	4672, 4665	Always	Allow All		

- **Enable:** Place a check in this box to enable the port forwarding rule.
- **Name:** Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the Application Name drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address:** Specify the IP address for the virtual server entry.
- **TCP/UDP Ports:** Specify the TCP or UDP port numbers.
- **Schedule:** Select a **schedule**, **Always**, or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- **Inbound Filter:** Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Save** button to insert the entry into the Port Forwarding list.

6.3.5 StreamEngine

- The StreamEngine feature helps improve the network performance by prioritizing applications.

StreamEngine

Save Settings Don't Save Settings

WAN Traffic Shaping

Enable Traffic Shaping:

Automatic Uplink Speed:

Measured Uplink Speed: Not Estimated

Manual Uplink Speed: 128 kbps << 128 kbps

Connection Type: Auto-detect

Detected xDSL or Other Frame Relay Network: Auto-detect

xDSL Or Other Frame Relay Network

Cable Or Other Broadband Network

- **Enable Traffic Shaping:** Place a check in the box to enable traffic shaping. When this option is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.
- **Automatic Uplink Speed.** Place a check in this box to enable automatic uplink speed. When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).
- **Measured Uplink Speed:** Displays the uplink speed. This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.
- **Manual Uplink Speed:** Specify an uplink speed or select it from the drop-down list. If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP.
- **Connection Type:** By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either Static or DHCP in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.
- Click on the **Save Settings** button to store these settings.

StreamEngine Setup

Enable StreamEngine:
 Automatic Classification:
 Dynamic Fragmentation:

Add StreamEngine Rule

Enable :
 Name :
 Priority : (1..255, 255 is the lowest priority)
 Protocol : <<
 Local IP Range : to
 Local Port Range : to
 Remote IP Range : to
 Remote Port Range : to

- **Enable StreamEngine:** Place a check in this box to enable this option. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.
- **Automatic Classification:** Place a check in this box to enable this option. This option is enabled by default so that your router will automatically determine which programs should have network priority.
- **Dynamic Fragmentation:** Place a check in this box to enable this option. This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.
- **Add StreamEngine Rule:** A StreamEngine Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific StreamEngine Rules will not be required. StreamEngine supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.
 - **Enable:** Place a check in this box to enable the StreamEngine rule.
 - **Name:** Specify a name for the rule.
 - **Priority:** Specify a priority for the rule. 0 being the highest and 255 the lowest priority.
 - **Protocol:** Specify a protocol or select one from the drop-down list.
 - **Local IP Range:** Specify the local (LAN) IP address range.
 - **Local Port Range:** Specify the local (LAN) port range.
 - **Remote IP Range:** Specify the remote (WAN) IP address range.
 - **Remote Port Range:** Specify the remote (WAN) port range.
 - Click on the **Save** button to insert the entry into the StreamEngine list.



6.3.6 Routing

- This section adds a new entry into the routing table.

Add Route

Enable:	<input checked="" type="checkbox"/>
Name:	route02
Destination IP:	192.168.1.11
Netmask:	255.255.255.0
Gateway:	192.168.1.13
Metric:	2
Interface:	WAN
<input type="button" value="Save"/> <input type="button" value="Clear"/>	

Routes List

	Name	Destination IP	Netmask	Gateway	Metric	Interface	
<input checked="" type="checkbox"/>	route01	192.168.1.12	255.255.255.0	192.168.1.13	3	WAN	 

- Enable:** Place a check in this box to enable the routing table entry.
- Name:** Specify a name for the rule.
- Destination IP:** Specify the destination IP address.
- Netmask:** Specify the subnet mask for the IP address.
- Gateway:** Specify the IP address of the gateway.
- Metric:** Specify the number of routing hops. The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.
- Interface:** Select the interface from the drop-down list.
- Click on the **Save** button to insert the entry into the Routing table.

6.3.7 Access Control

- The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.
- When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.

Access Control

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

Save Settings

Don't Save Settings

Access Control

Enable Access Control :

Add Policy

Policy Table

Enable	Policy	Machine	Filtering	Logged	Schedule
--------	--------	---------	-----------	--------	----------

- Place a check in the **Enable Access Control** check box and then click on the **Add Policy** button. This will bring up the **Add New Policy** wizard.
- The wireless wizard will inform you that there are six major steps in the process.
 - Choose a unique name for your policy
 - Select a schedule
 - Select the machine to which the policy applies
 - Select filtering method
 - Configure web access logging

Add New Policy

This wizard will guide you through the following steps to add a new policy for Access Control.

- Step 1 - Choose a unique name for your policy
- Step 2 - Select a schedule
- Step 3 - Select the machine to which this policy applies
- Step 4 - Select filtering method
- Step 5 - Select filters
- Step 6 - Configure Web Access Logging

Prev

Next

Save

Cancel

- Click on the **Next** button to continue.

Step 1: Choose Policy Name

Choose a unique name for your policy.

Policy Name :

Prev

Next

Save

Cancel

- Specify a policy name and then click on the **Next** button to continue.

Step 2: Select Schedule

Choose a schedule to apply to this policy.

Details :

Always

Always

Never

Define a new schedule

Prev Next Save Cancel

- Select a schedule from the drop-down list: **Always** or **Never**, or you may define a new schedule. Click on the **Next** button to continue.

Step 3: Select Machine

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type : IP MAC Other Machines

IP Address : 192.168.1.46 << Computer Name

Machine Address : << Computer Name

Copy Your PC's MAC Address

OK Cancel

Machine		
00:15:c5:61:a2:91		
192.168.1.45		

Prev Next Save Cancel

- Select a machine to which the policy applies.
- **Address Type**: Select the IP address or MAC address radio button.
- **IP Address**: If you selected IP address above, then specify the IP address here.
- **MAC Address**: If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PCs MAC Address**.
- Click on the **OK** button to insert the entry into the table.
- Click on the **Next** button to continue.

Step 4: Select Filtering Method

Select the method for filtering.

Method : Log Web Access Only Block All Access Block Some Access

Prev Next Save Cancel

- Select a filtering method:
- **Log Web Access Only**: Select this radio but in order to log web access.
- **Block All Access**: Select this radio but in order to block all web access.
- **Block Some Access**: Select this radio but in order to block some web access.
- Click on the **Save** button to store the changes.

6.3.8 Web Filter

- This is a type of parental control feature used to restrict certain websites from being accessed through your network. These filters can be used for securing and restricting your network.

Website Filter

The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

[Don't Save Settings](#)

Add Web Filtering Rule

Website URL/Domain : [Save](#)

Website Filtering Rules

URL	Delete
www.facebook.com	
www.youtube.com	

- **Website/URL/Domain:** Specify the web address that you would like to filter. Do not use "http://"
- Click on the **Save** button to store the changes.

6.3.9 MAC Address Filter

- This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.

MAC Filtering Setup

Configure MAC Filtering below:

Turn MAC Filtering ON and ALLOW computers listed to access the network

Turn MAC Filtering OFF

Turn MAC Filtering ON and ALLOW computers listed to access the network

Turn MAC Filtering ON and DENY computers listed to access the network

MAC Address : <<

[Save](#)

MAC Filtering Rules

MAC Address	Name	Delete
-------------	------	--------

- **Configure MAC Filtering:** Select one of the options from the drop-down list.
 - **Turn MAC Filtering OFF:** When "OFF" is selected, MAC addresses are not used to control network access.
 - **Turn MAC Filtering ON and ALLOW computers listed to access the network:** When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Filtering Rules list are granted network access.
 - **Turn MAC Filtering ON and DENY computers listed to access the network:** When "DENY" is selected, any computer with a MAC address listed in the MAC Filtering Rules list is refused access to the network.
- **MAC Address:** Specify that MAC address that you would like to filter.
- Click on the **Save** button to store the changes.

6.3.10 Firewall

- The device provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.

Firewall Settings

Enable SPI :

NAT Endpoint Filtering

UDP Endpoint Filtering: Endpoint Independent
 Address Restricted
 Port And Address Restricted

TCP Endpoint Filtering: Endpoint Independent
 Address Restricted
 Port And Address Restricted

NAT Port Preservation

Enable port preservation:

- **Enable SPI:** Place a check in this box to enable SPI. SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol. When the protocol is TCP, SPI checks that packet sequence numbers are within the valid range for the session, discarding those packets that do not have valid sequence numbers. Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.
- **TCP / UDP NAT Endpoint Filtering** options control how the router's NAT manages incoming connection requests to ports that are already being used. Select one of the radio buttons.
 - **End Point Independent** Once a LAN-side application has created a connection through a specific port, the NAT will forward any incoming connection requests with the same port to the LAN-side application regardless of their origin. This is the least restrictive option, giving the best connectivity and allowing some applications (P2P applications in particular) to behave almost as if they are directly connected to the Internet.
 - **Address Restricted** The NAT forwards incoming connection requests to a LAN-side host only when they come from the same IP address with which a connection was established. This allows the remote application to send data back through a port different from the one used when the outgoing session was created.
 - **Port And Address Restricted** The NAT does not forward any incoming connection requests with the same port address as an already establish connection.

- **Note:** Some of these options can interact with other port restrictions. Endpoint Independent Filtering takes priority over inbound filters or schedules, so it is possible for an incoming session request related to an outgoing session to enter through a port in spite of an active inbound filter on that port. However, packets will be rejected as expected when sent to blocked ports (whether blocked by schedule or by inbound filter) for which there are no active sessions. Port and Address Restricted Filtering ensures that inbound filters and schedules work precisely, but prevents some level of connectivity, and therefore might require the use of port triggers, virtual servers, or port forwarding to open the ports needed by the application. Address Restricted Filtering gives a compromise position, which avoids problems when communicating with certain other types of NAT router (symmetric NATs in particular) but leaves inbound filters and scheduled access working as expected.
- **Enable Port Preservation:** Place a check in this box to enable Port Preservation. NAT Port preservation (on by default) tries to ensure that, when a LAN host makes an Internet connection, the same LAN port is also used as the Internet visible port. This ensures best compatibility for internet communications. Under some circumstances it may be desirable to turn off this feature.

Anti-Spoof checking

Enable anti-spoof checking:

DMZ Host

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only

Enable DMZ:

DMZ IP Address : <<

Non-UDP/TCP/ICMP LAN Sessions

Enable :

- **Enable anti-spoof checking:** Place a check in this box to enable anti-spoof checking. Enabling this option can provide protection from certain kinds of "spoofing" attacks. However, enable this option with care. With some modems, the WAN connection may be lost when this option is enabled. In that case, it may be necessary to change the LAN subnet to something other than 192.168.0.x (192.168.2.x, for example), to re-establish the WAN connection.
- **Enable DMZ Host:** Place check in this box to enable DMZ host. DMZ host is a demilitarized zone used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web, FTP, email and DNS servers.
- **DMZ IP Address:** Specify the IP address of the DMZ host.
- **Non-UDP/TCP/ICMP LAN Sessions:** Place a check in this box to enable this feature. When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol. This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an ALG.
- **Note:** This feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions.

- Enabling this option (the default setting) enables single VPN connections to a remote host. (But, for multiple VPN connections, the appropriate VPN ALG must be used.) Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled.

Application Level Gateway (ALG) Configuration

PPTP :	<input checked="" type="checkbox"/>
IPSec (VPN) :	<input checked="" type="checkbox"/>
RTSP :	<input checked="" type="checkbox"/>
Windows/MSN Messenger :	<input checked="" type="checkbox"/> (automatically disabled if UPnP is enabled)
FTP :	<input checked="" type="checkbox"/>
H.323 (NetMeeting) :	<input checked="" type="checkbox"/>
SIP :	<input checked="" type="checkbox"/>
Wake-On-LAN :	<input checked="" type="checkbox"/>
MMS :	<input checked="" type="checkbox"/>

- **Application Layer Gateway (ALG) Configuration:** Place a check in appropriate feature boxes to enable them. . Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.
 - **PPTP:** Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to Advanced → Virtual Server).
 - **IPSec:** (VPN) Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option. Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.
 - **RTSP:** Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.
 - **Windows/MSN Messenger:** Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) and MSN Messenger. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled.
 - **FTP:** Allows FTP clients and servers to transfer data across NAT.
 - **H.323 (Netmeeting):** Allows H.323 (specifically Microsoft Netmeeting) clients to communicate across NAT server.
 - **SIP:** Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.