



# LevelOne

## User Manual

WBR-6020

***N\_Max Wireless Router***

Ver. 1.0.1

# Safety

## FCC WARNING

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

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

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

## CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

## CE Marking Warning

Hereby, Digital Data Communications, declares that this product (Model-no. WBR-6020) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

<http://www.levelone.eu/support.php>



# General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at <http://global.level1.com>.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US\$9.99 plus the cost of shipping.

# Table of Content

<b>TABLE OF CONTENT</b> .....	<b>4</b>
<b>1. INTRODUCTION</b> .....	<b>5</b>
USER MANUAL OVERVIEW .....	5
<b>2. UNPACKING AND SETUP</b> .....	<b>6</b>
FEATURES.....	6
PACKAGE CONTENTS.....	6
<b>3. HARDWARE INSTALLATION</b> .....	<b>7</b>
FRONT VIEW .....	7
REAR VIEW .....	8
HARDWARE INSTALLATION .....	9
<b>4. CHECK YOUR NETWORK SETTINGS</b> .....	<b>12</b>
<b>5. CONFIGURATION WIZARD</b> .....	<b>13</b>
<b>6. ADVANCED SETUP</b> .....	<b>18</b>
BASIC SETTING .....	19
<i>Green Function</i> .....	20
<i>Primary Setup</i> .....	22
<i>DHCP Server</i> .....	27
<i>Wireless Settings</i> .....	28
<i>Change Password</i> .....	39
FORWARDING RULES.....	40
<i>Virtual Server</i> .....	41
<i>Special AP</i> .....	42
<i>Miscellaneous Items</i> .....	43
SECURITY SETTINGS.....	44
<i>Packet Filter</i> .....	45
<i>Packet Filter</i> .....	45
<i>Domain Filter</i> .....	47
<i>URL Blocking</i> .....	48
<i>MAC Address Control</i> .....	49
<i>Miscellaneous Items</i> .....	51
ADVANCED SETTINGS .....	52
<i>System Log</i> .....	53
<i>Dynamic DNS</i> .....	54
<i>QoS Rule</i> .....	55
<i>SNMP Setting</i> .....	56
<i>Routing</i> .....	57
<i>System Time</i> .....	59
<i>Schedule Rule</i> .....	60
TOOLBOX.....	62
<i>System Info</i> .....	63
<i>Firmware Upgrade</i> .....	64
<i>Backup Setting</i> .....	64
<i>Reset to Default</i> .....	64
<i>Reboot</i> .....	64
<i>Miscellaneous Items</i> .....	65
<b>TECHNICAL SPECIFICATIONS</b> .....	<b>76</b>

## Default Settings

IP Address	192.168.0.1
Password	password
Wireless Mode	Enable
Wireless SSID	WBR-6020
Wireless Security	None

# 1. Introduction

---

Congratulations on your purchase of LevelOne WBR-6020 *N\_Max* Wireless Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users.

Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read the manual carefully for fully exploiting the functions of this product.

## User Manual Overview

<b>Introduction</b>	Describes the <i>N_Max</i> Wireless Router.
<b>Unpacking and Setup</b>	Helps user to get started with the basic installation of the router.
<b>Hardware Installation</b>	Describes the LED indicators router.
<b>Configuration</b>	Describes the functionalities and its settings.
<b>Technical Specifications</b>	Lists the technical (general, physical and environmental) specifications of the router.

## 2. Unpacking and Setup

---

This chapter provides the package contents and setup information for the *N\_Max Wireless Router*.

### Features

- Smart Power Saving Features and Wireless Disable button
- Delivers *N\_Max* Wireless Performance at up to 300Mbps
- Increased Wireless Range with MIMO Technology
- Auto-Channel Selection to avoid interference from neighbors
- Simple Security Control with One-Button WPS Protection
- Advanced Firewall and Traffic Priority Features.
- Quick and Easy Installation Wizard

### Package Contents

Open the box of the *N\_Max Wireless Router* and carefully unpack it. The box should contain the following items:

- WBR-6020 *N\_Max Wireless Router*
- Power Adapter
- Cat.5 Cable
- Antenna x2
- CD Manual / Utility
- Quick Installation Guide

If any item is found missing or damaged, please contact your local reseller for replacement.

### 3. Hardware Installation

---

#### Front View



<b>WLAN Button</b>	<ul style="list-style-type: none"> <li>• Press and hold for 3 seconds to turn the Wireless LAN on or off.</li> <li>• Please confirm WLAN status as indicated by WLAN Light</li> </ul>
<b>Status Light</b>	<ul style="list-style-type: none"> <li>• A steady blinking light indicates the device is ready</li> </ul>
<b>WAN Light</b>	<ul style="list-style-type: none"> <li>• A solid light indicates the WAN port is connected.</li> </ul>
<b>WLAN Light</b>	<ul style="list-style-type: none"> <li>• Off indicates Wireless LAN is turned off, or no wireless client is connected to the router.</li> <li>• LED blinks during wireless data transmission, or when there is a wireless client connected to the router.</li> <li>• Fast and Steady blinking indicates WPS function is activated and the router is pairing with wireless client.</li> </ul>
<b>LAN Lights</b>	<ul style="list-style-type: none"> <li>• A solid light indicates to an Ethernet enable computer on ports 1 ~ 4.</li> <li>• LED blinks during data transmission.</li> </ul>
<b>Sleep Light</b>	<ul style="list-style-type: none"> <li>• When solid light (orange) means that the router is in sleep mode.</li> </ul>
<b>WPS Button</b>	<ul style="list-style-type: none"> <li>• Wi-Fi Protected Setup push button. Press to activate WPS pairing with wireless client.</li> </ul>
<b>Reset (WLAN and WPS Buttons)</b>	<ul style="list-style-type: none"> <li>• Press the WLAN and WPS buttons together for 5 seconds to reboot and restore the device to factory default settings.</li> </ul>

## Rear View



<b>Power Jack</b>	<ul style="list-style-type: none"><li>• Receptor for the supplied power adapter</li></ul>
<b>LAN Ports (1~4)</b>	<ul style="list-style-type: none"><li>• Connect Ethernet devices such as computers, switches or hubs.</li></ul>
<b>WAN Port</b>	<ul style="list-style-type: none"><li>• The WAN port is the connection for the Ethernet cable to the Cable or DSL Modem.</li></ul>
<b>Sleep Button</b>	<ul style="list-style-type: none"><li>• This button is used to force the router to enter sleep mode, or wake up. It has the highest priority and overrides the Power Saving Schedule.</li></ul>
<b>Antennas</b>	<ul style="list-style-type: none"><li>• Detachable antennas allows users to change antenna if necessary.</li></ul>



# Hardware Installation

## Decide where to place your Wireless Router

You can place your Wireless Router on a desk or other flat surface. For optimal performance, place your Wireless Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

1. Attach the included antennas.



2. Connect your broadband internet connection to WBR-6020's WAN port.



3. Connect the Computer LAN cable.



4. Plug in the Power Adapter



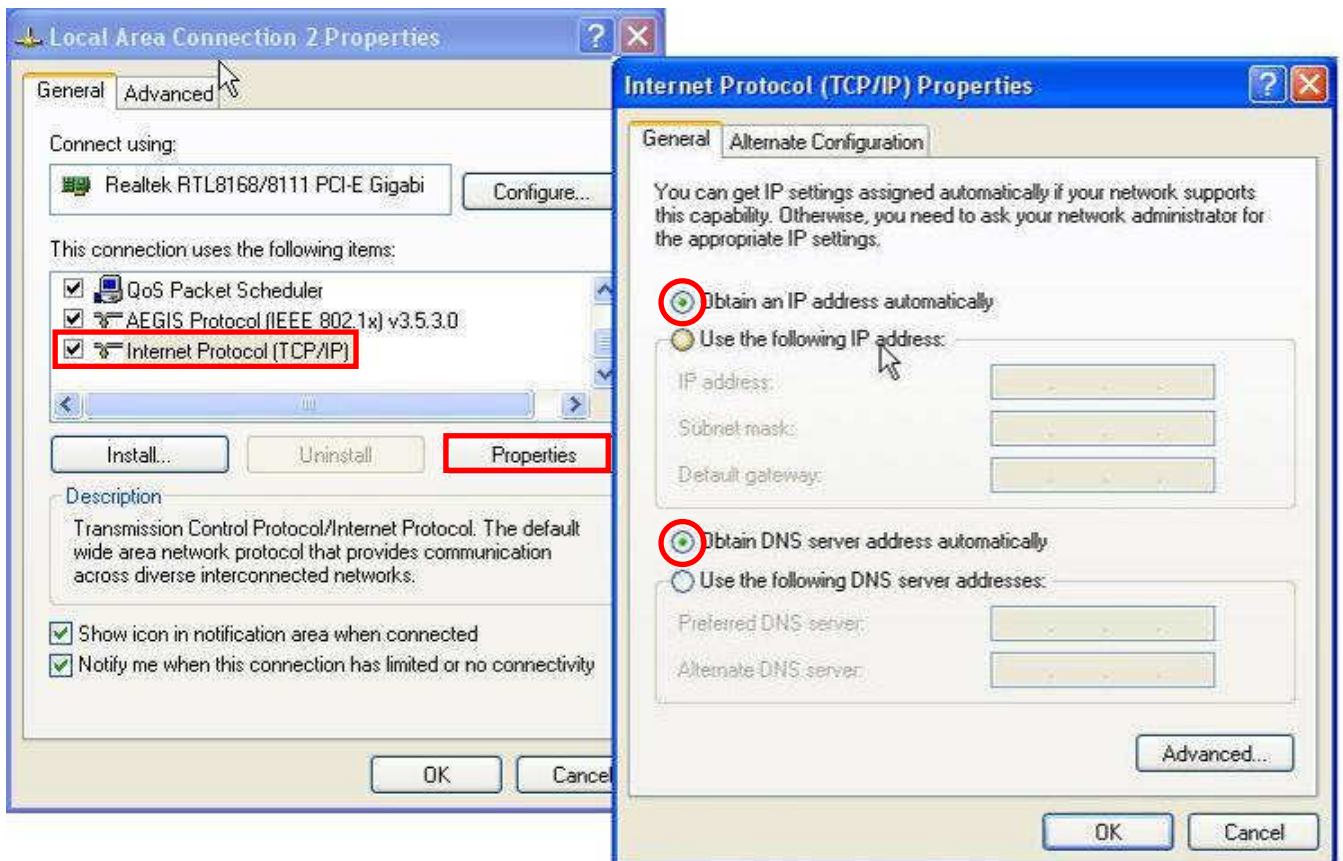
5. Wait until the Status light is blinking steadily.  
This means the router is ready for use.



## 4. Check Your Network Settings

---

1. Please make sure your PC can get IP address automatically so the WBR-6020 can communicate with your PC during configuration.
  - Select “Control Panel” > “Network Connections”.
  - Right click the “Local Area Connection” and choose “Properties”.
  - Select the TCP/IP protocol for your network card.
  - Click on the Properties button. You should then see the following screen and make sure you have selected “Obtain IP address automatically”



2. Reboot computer to make sure you have received the IP address correctly.

## 5. Configuration Wizard

---

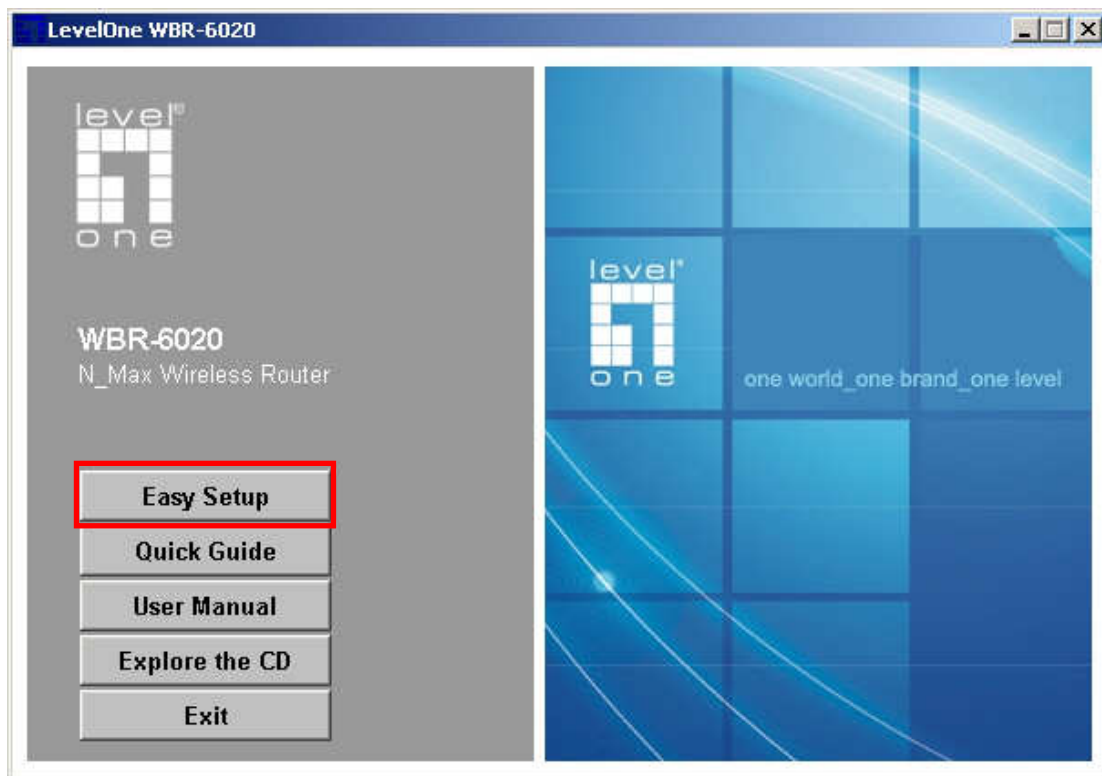
Once properly configured, the WBR-6020 *N\_Max Wireless* Router will obtain and assign IP address information automatically. Configuration settings can be established through the Web-Based Configuration Menu, or the Easy Setup Utility on the CD.

### Easy Setup Utility

Insert the CD into your CD-ROM drive of your computer.

The autorun program should start automatically.  
If it does not, please run autorun.exe on your CD.

In the autorun screen, click **Utility** to begin the Easy Setup Utility.



## Web-Based Configuration

Open a web browser (Internet Explorer/Firefox/Safari) and type in the IP Address <http://192.168.0.1>

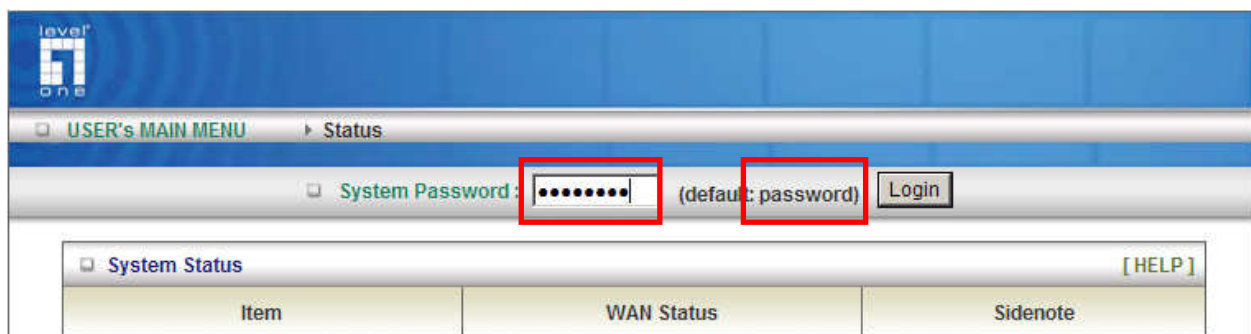
**Note:**

If you have changed the default IP Address assigned to the WBR-6020, ensure you enter the correct IP Address.



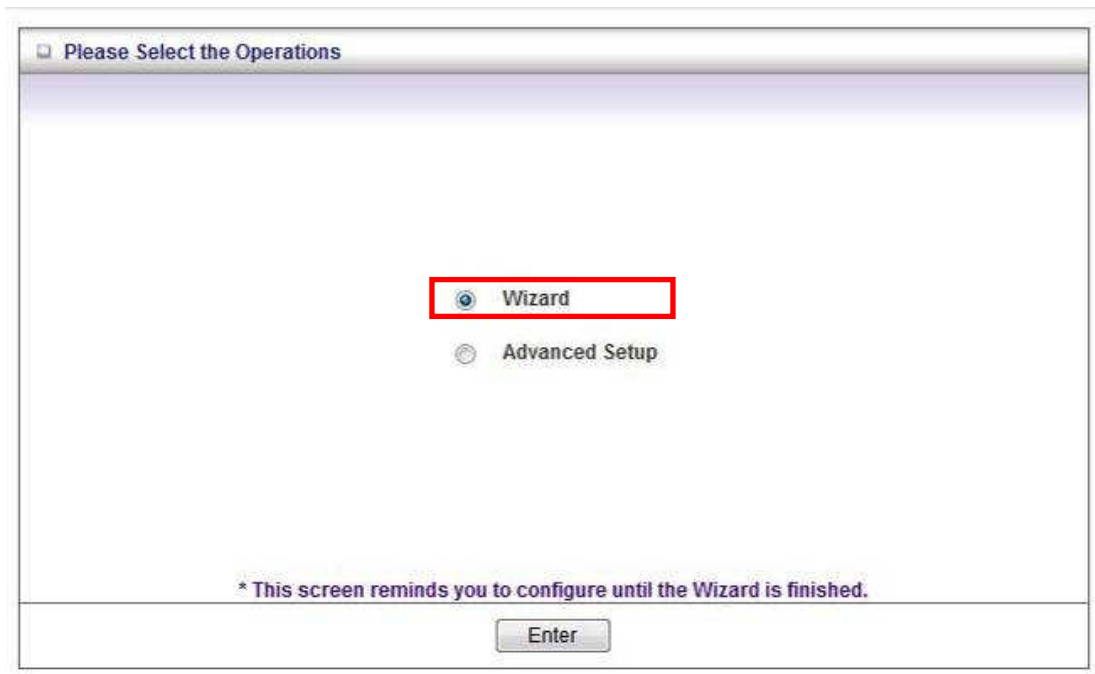
Type in “**password**” (without quotes) in the Password box, Then click Login

**Note:** password is the default login password for the unit.

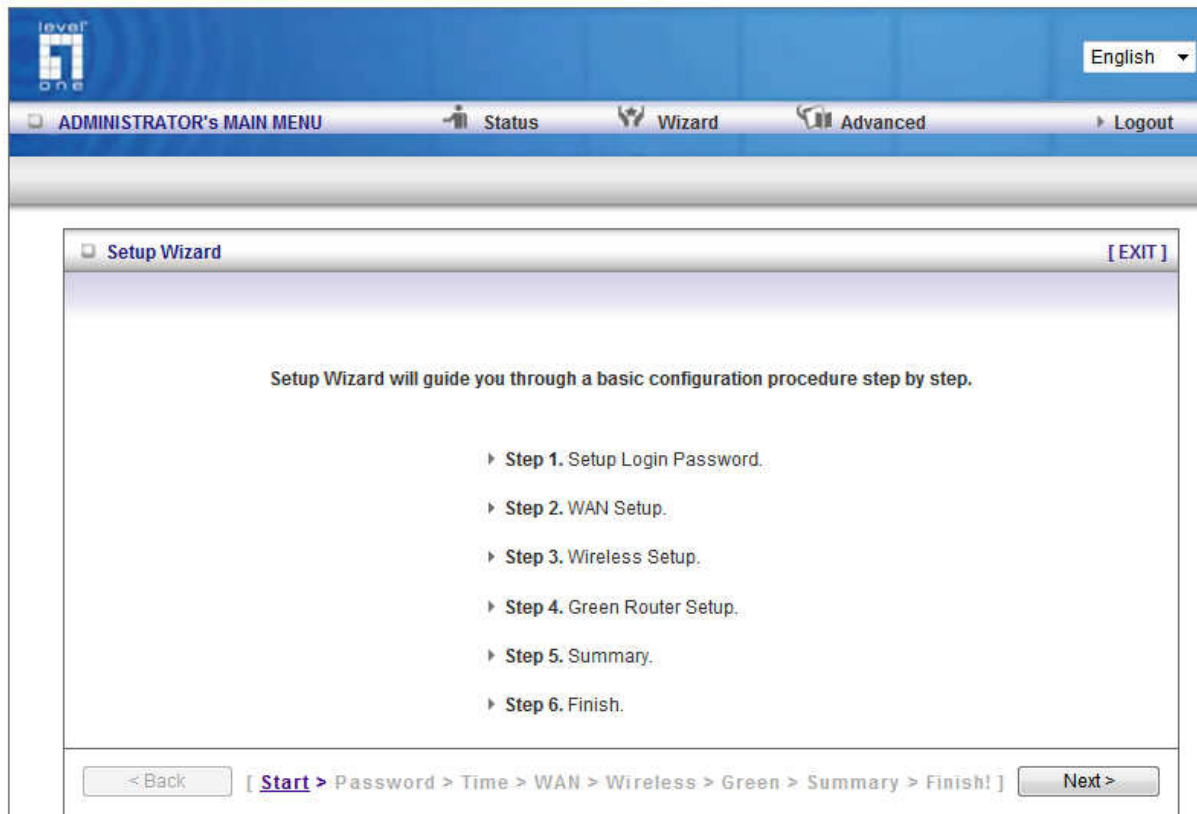


The user can setup step by step to finish the connection with Wizard.

If you are an advanced user, you can access the configurations directly in the Advanced Setup



Setup Wizard will guide you through a basic configuration procedure step by step. Press **Next** to begin.



Remember to set up the Sleep Mode to enable the Power Saving features.

level one

English

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

Setup Wizard - Green Function Setting [EXIT]

Smart Schedule  Enable  
(\* When Smart Schedule is Enabled, the router will first detect whether there is anyone still using the network or Internet before going into Sleep mode.)

Setup Sleep times for **Everyday** or **Monday ~ Friday**  
 Setup Sleep times **Manually**

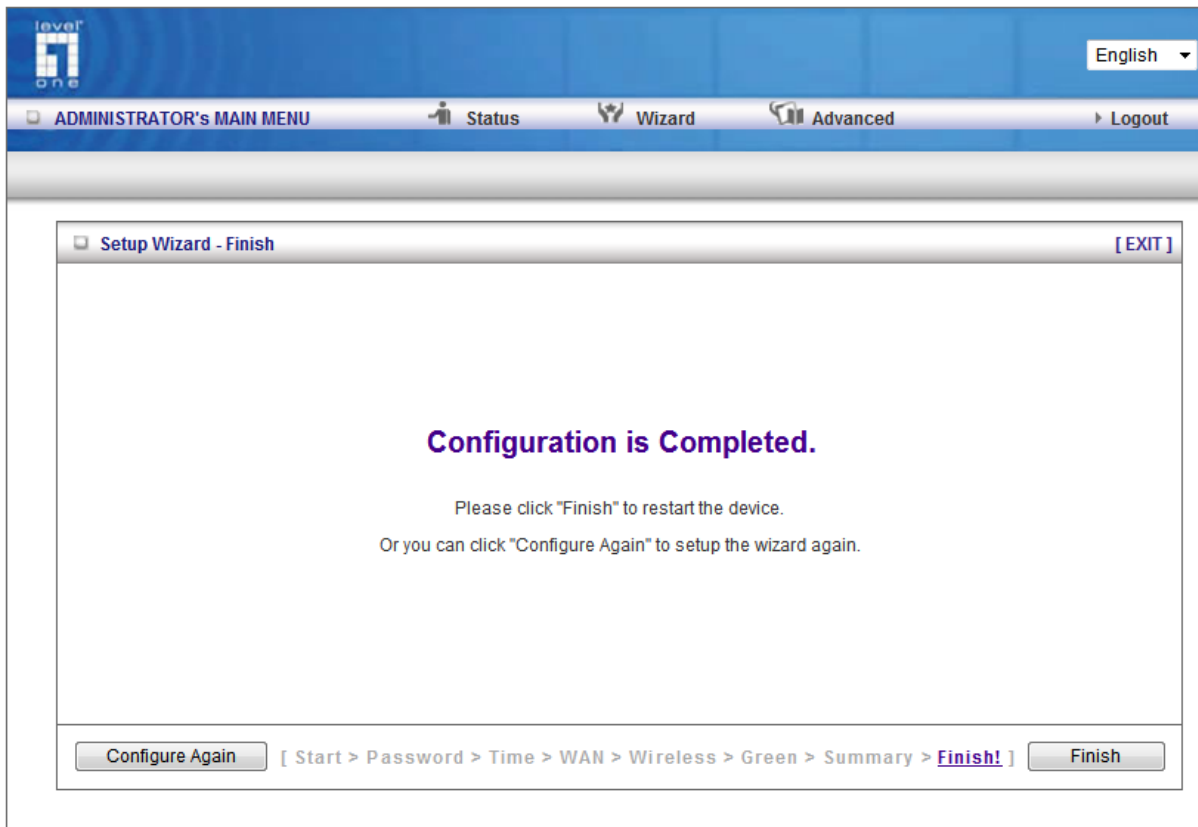
Everyday  Mon~Fri  
From  To  Use 24 Hour Format

ID	Power OFF Days	Power OFF Time(hh:mm)	Power ON Days	Power ON Time(hh:mm)
1	Monday	23:00	Monday	08:00
2	Tuesday	23:00	Tuesday	08:00
3	Wednesday	23:00	Wednesday	08:00
4	Thursday	23:00	Thursday	08:00
5	Friday	23:00	Friday	08:00

< Back   [ Start > Password > Time > WAN > Wireless > **Green** > Summary > Finish! ]   Next >



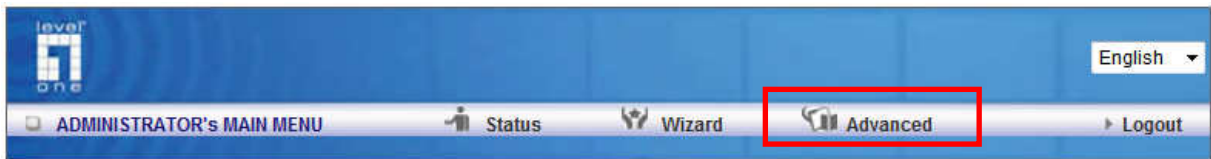
Once the user finishes those steps and the router screen displayed as below. It means that the Internet connection is now established.



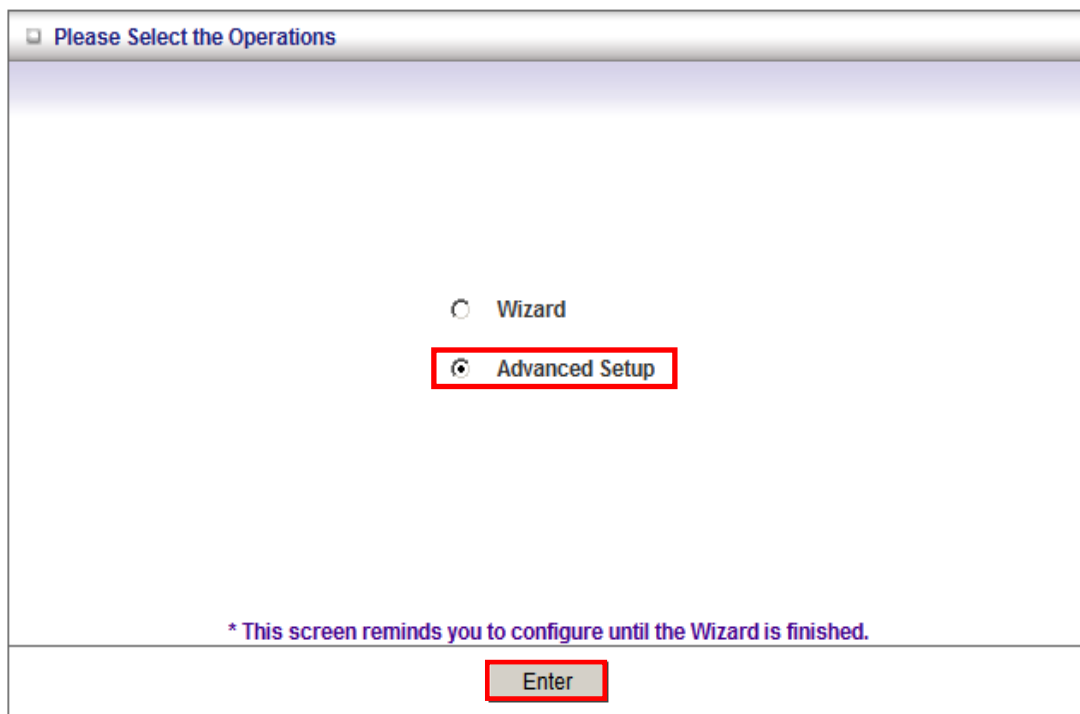
## 6. Advanced Setup

---

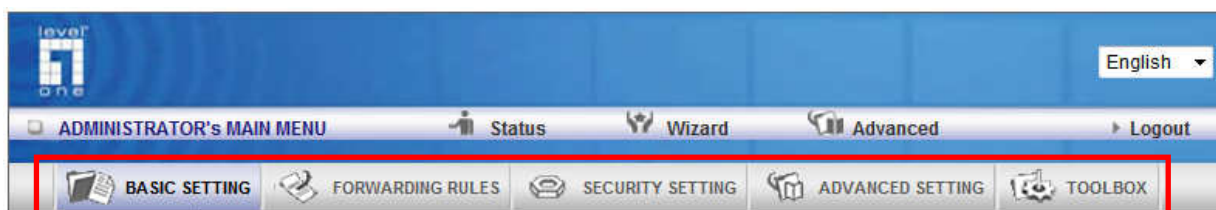
To access the Advanced Setup, click on **Advanced Setup** at the top of the page.



Or, for first time installation, choose Advanced Setup and click **Enter**.



Once in the Advanced Setup, you will be presented with the following menu.



# Basic Setting

These are the basic settings of the unit. Click on the menu on the left to access the respective settings page.

The screenshot displays the web management interface for a Level One WBR-6020 router. At the top, there is a blue header with the Level One logo and a language dropdown menu set to 'English'. Below the header is a navigation bar with tabs for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains icons and labels for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, a vertical menu is highlighted with a red box, listing options: 'Green Function', 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Basic Setting' and contains the following information:

- The WBR-6020 supports 3 modes:**
  - On Mode:** Wireless Router is always on.
  - Low Power Mode:** When no wireless devices are connected to the Wireless Router for 10 minutes, it will automatically switch to Low Power Mode. In this mode, power is reduced to wireless transmissions. When wireless traffic is detect, the Wireless Router will automatically revert to full power status.
  - Sleep Mode:** When the time set in the Schedule is met, then the Wireless Router will enter Sleep Mode when it detects there are no devices using the network or Internet. To wake the Wireless Router from Sleep Mode, press the sleep button.  
**Users cannot use the network or Internet when in Sleep Mode.**
- Primary Setup**
  - Configure LAN IP, and select WAN type.
- DHCP Server**
  - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless**
  - Wireless settings allow you to configure the wireless configuration items.
- Change Password**
  - Allow you to change system password.

## Green Function

The Power Saving function allows you to set the time that the router enters into Sleep Mode. This means that the router can automatically power on and off at user specified times.

Green Function				
Item		Setting		
▶ Low Power Wireless Mode		<input checked="" type="checkbox"/> Enable		
▶ Sleep mode		<input checked="" type="checkbox"/> Enable Warning: Users cannot use the network or Internet when in Sleep Mode.		
▶ Smart Schedule		<input checked="" type="checkbox"/> Enable		
ID	Power OFF Days	Power OFF Time(hh:mm)	Power ON Days	Power ON Time(hh:mm)
1	Monday ▼	23:00	Monday ▼	08:00
2	Tuesday ▼	23:00	Tuesday ▼	08:00
3	Wednesday ▼	23:00	Wednesday ▼	08:00
4	Thursday ▼	23:00	Thursday ▼	08:00
5	Friday ▼	23:00	Friday ▼	08:00
6	-- choose one -- ▼		-- choose one -- ▼	
7	-- choose one -- ▼		-- choose one -- ▼	
8	-- choose one -- ▼		-- choose one -- ▼	
9	-- choose one -- ▼		-- choose one -- ▼	
10	-- choose one -- ▼		-- choose one -- ▼	
11	-- choose one -- ▼		-- choose one -- ▼	
12	-- choose one -- ▼		-- choose one -- ▼	
13	-- choose one -- ▼		-- choose one -- ▼	
14	-- choose one -- ▼		-- choose one -- ▼	
15	-- choose one -- ▼		-- choose one -- ▼	
16	-- choose one -- ▼		-- choose one -- ▼	
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Bootup/Sleep Time Log"/>				

**Low Power Wireless Mode:** When no wireless clients are connected to the router, it will reduce power to the radio to save power. When a device connects wirelessly to the router, it will revert to full power immediately.

**Sleep Mode:** When Enabled, the router will follow the times set in the schedule below to enter Sleep Mode, or wake up to normal mode. When the router is in Sleep Mode, the user will not be able to connect to the Local network, nor the Internet.

**Note:** The Sleep button on the back of the router can override the current router setting. You can force the router to enter Sleep Mode, or revert back to normal mode.

**Smart Schedule:** When Enabled, the router will first check whether there is any network activity on router before entering Sleep Mode. This is to prevent your network usage to be interrupted.

**Bootup / Sleep Time Log:** A log of the times that the router entered Sleep Mode, or woke up back to normal mode.

## Primary Setup

This page lets you change the LAN (Local Area Network) settings on your WBR-6020 *N\_Max Wireless Router* and WAN (Wide Area Network) connection.

Primary Setup <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.0.1"/>
▶ WAN Type	Dynamic IP Address ▾
▶ Host Name	<input type="text" value="WBR-6020"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Connect-on-Demand ▾
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Virtual Computers..."/>	

**LAN IP Address:** The local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

**WAN Type:** WAN connection type of your ISP. You can use the drop-down men to choose the most suitable one from the following options:

**Connection Control:** You can choose the method that the router maintains connection to the internet.

**Connect-on-Demand:** The router will automatically connect to the Internet when a computer in the network requests Internet usage.

**Auto-reconnect (always on):** The router will maintain connection to the Internet at all possible times. It will also reconnect automatically when it detects it has been disconnected.

**Manually:** You will need to connect to the Internet manually each time

Primary Setup <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ LAN IP Address	192.168.0.1
▶ WAN Type	Dynamic IP Address ▼
▶ Host Name	<div style="border: 1px solid red; padding: 2px;">           Static IP Address            Dynamic IP Address            PPP over Ethernet            PPTP            L2TP         </div> <input type="text"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Connect-on-Demand ▼
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Virtual Computers..."/>	

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

**Static IP Address:** ISP assigns you a static IP address.

**Dynamic IP Address:** Obtain an IP address from ISP automatically.

**PPP over Ethernet:** Some ISPs require the use of PPPoE to connect to their services.

**PPTP:** Some ISPs require the use of PPTP to connect to their services.

**L2TP:** Some ISPs require the use of L2TP to connect to their services

### Static IP Address

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

### Dynamic IP Address

1. Host Name: Optional. Required by some ISPs, for example: @Home.
2. Renew IP Forever: This feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

## **PPP over Ethernet**

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
4. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.
5. Connection Control: There are 3 modes to select:
6. Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
7. Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.
8. Manually: The device will not make the link until someone clicks the connect-button in the Staus-page.



## **PPTP**

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

1. My IP Address and My Subnet Mask: The private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: The IP address of the PPTP server.
3. PPTP Account and Password: The account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Connection ID: Optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: The time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
6. Connection Control: There are 3 modes to select:
7. Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
8. Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.
9. Manually: The device will not make the link until someone clicks the connect-button in the Status page.

## **L2TP**

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

1. My IP Address and My Subnet Mask: The private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
6. Connection Control: There are 3 modes to select:
  - Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
  - Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.
  - Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

### Virtual Computers (Only for Static and dynamic IP address WAN type)

Used when WAN is set as DHCP or Static IP, the user can assign a global IP address to a LAN IP Address.

Virtual Computers <span style="float: right;">[ Help ]</span>			
ID	Global IP	Local IP	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- **Global IP:** Enter the global IP address assigned by your ISP.
- **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
- **Enable:** Check this item to enable the Virtual Computer feature.

## DHCP Server

This page allows you to configure the DHCP server on the Router

DHCP Server <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	<input type="text" value="2"/>
▶ IP Pool Ending Address	<input type="text" value="50"/>
▶ Lease Time	<input type="text" value="86400"/> Seconds
▶ Domain Name	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Primary WINS	<input type="text"/>
▶ Secondary WINS	<input type="text"/>
▶ Gateway	<input type="text"/> (optional)

For more settings click on **More**.

**DHCP Server:** To either Disable or Enable DHCP Server.

**IP Pool Starting/Ending Address:** The pool of IP's that can be allocated to clients

**Lease Time:** DHCP lease time to the DHCP client

**Domain Name:** To assign a Domain Name (optional)

**Primary DNS/Secondary DNS:** To assign DNS Servers (optional)

**Primary WINS/Secondary WINS:** To assign WINS Servers (optional)

**Gateway:** The IP address of an alternate gateway (optional)

**Clients List:** Check the DHCP client list.

**Fixed Mapping:** Take you to the Security > MAC Control page.

After you finish your selections click either **Save** to store your settings, or **Undo** to exit.

## Wireless Settings

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	None ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List..."/>	

**Wireless - Enabled** by default. Disabling this will turn off the wireless feature of this unit.

**Wireless Operation Mode:** Select between Access Point or Wireless Client mode.

**Note:** Wireless Client modes supports the following Wireless Encryption modes:  
WEP, WPA-PSK (TKIP), WPA2-PSK (AES)

**Network ID (SSID):** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **WBR-6020**. The SSID can be easily changed to establish a new wireless network.

**Note:** SSID names may contain up to 32 ASCII characters.

**SSID Broadcast:** The WBR-6020 will broadcast beacons that contains SSID and other wireless information so that Computers or other wireless devices can find the WBR-6020 when scanning for wireless networks. Disable this function if you want to hide your wireless network.

**Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The default is AUTO which means the WBR-6020 will find the least used channel to avoid interference.

**Note:** Channel range depends on your regional regulations. Please see specifications for Channel details.

**Wireless Client List:** You can use this function to see the devices connected to the WBR-6020 through the wireless network.

**Security: Security** - You may select from three levels of encryption to secure your wireless network: No Encryption, WEP, 802.1x RADIUS, WPA-PSK, WPA, WPA2-PSK (AES), WPA2 (AES), WPA-PSK / WPA2-PSK and WPA1 / WPA2.

LevelOne recommends **WPA2-PSK (AES)** for simple and secure wireless encryption.

After configuring the wireless security settings on the WBR-6020, you will also need to configure the same settings on your wireless adapter before you attempt a wireless connection.

Please note that not all adapters support all the available security functions.

**No Encryption** is the default (as shown in the screen above).

**WEP:**

WEP (Wired Equivalent Privacy). Enabling the security can protect your data while it is transferred to the WBR-6020. Enter the 10 digit WEP Key.

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	WEP ▼
<input checked="" type="radio"/> WEP Key 1	HEX ▼ 1234567890
<input type="radio"/> WEP Key 2	HEX ▼ 1234567890
<input type="radio"/> WEP Key 3	HEX ▼ 1234567890
<input type="radio"/> WEP Key 4	HEX ▼ 1234567890
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List..."/>	

## WPA-PSK, WPA2-PSK, WPA / WPA2-PSK

This security is more secure compared to WEP. Please enter the key in the Preshare Key field. The field can be between 8 and 63 characters long and can be any combination of letters and numbers.

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	WPA-PSK / WPA2-PSK ▼
▶ Preshare Key	1234567890
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List.."/>	

## 802.1x and RADIUS

To use this security feature, you will need to have a RADIUS server on your network to authenticate access. Please type in the details for your RADIUS server.

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	802.1x and RADIUS ▼
▶ RADIUS Server IP	<input type="text"/>
▶ RADIUS port	1812
▶ RADIUS Shared Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List..."/>	

### *RADIUS Server*

IP Address, or the RADIUS server's domain-name.

### *RADIUS Shared Key*

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

## WPA, WPA2, WPA1/WPA2

Similar to 802.1X security using WPA / WPA2 for encryption. You will need a RADIUS server for authentication. Please enter the details of your RADIUS server.

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	WPA / WPA2 ▼
▶ RADIUS Server IP	<input type="text"/>
▶ RADIUS port	1812
▶ RADIUS Shared Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List..."/>	

### *RADIUS Server*

- IP address or the RADIUS server's domain-name.
- Port number of the RADIUS Server
- Enter the RADIUS Shared Key  
Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



## WPS (WiFi Protected Setup)

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

Please ensure you have wireless security set up on the WBR-6020 before initializing WPS functions.

### Set PIN number of WBR-6020

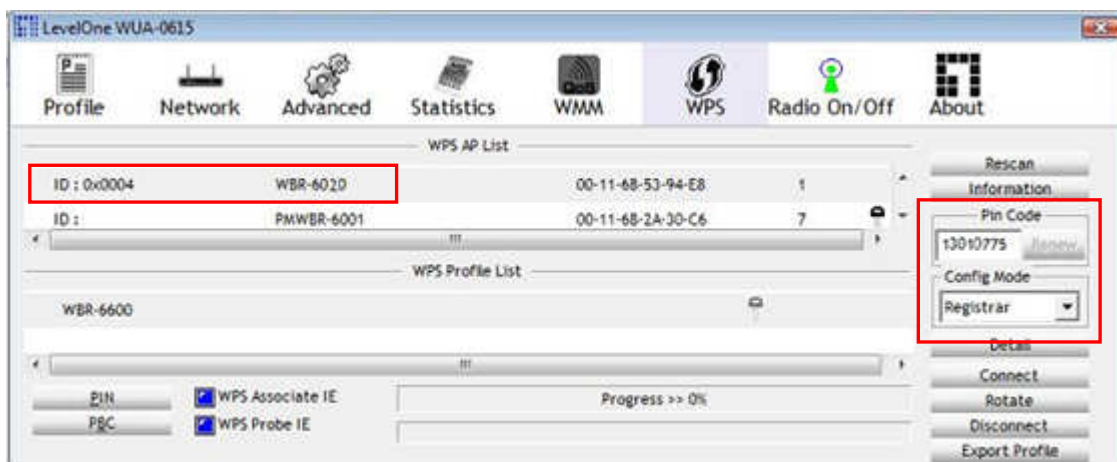
Make sure the Router is set in “Enrollee” mode.

Click the “Generate New PIN” button to randomly create a new PIN number for the WBR-6020. Then click “Save” to apply the settings.

Set your wireless adapter as Registrar and enter this PIN number to initiate the WPS function.

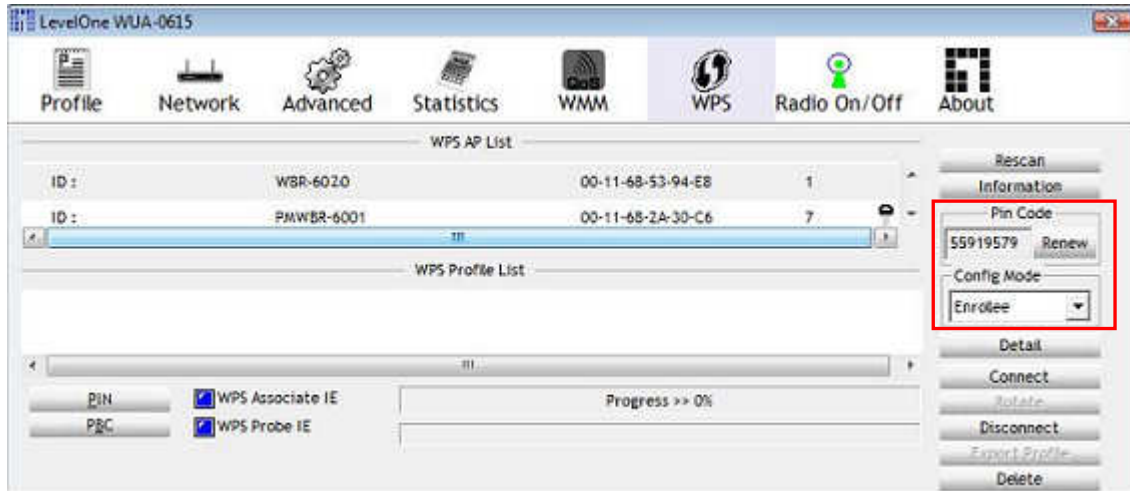
Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	13010775 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Enrollee ▼
▶ Config Status	UNCONFIGURED <input type="button" value="Set"/>
▶ Config Method	PIN Code ▼
▶ WPS status	Not in Use

No change!



### Enter PIN number of Wireless Adapter

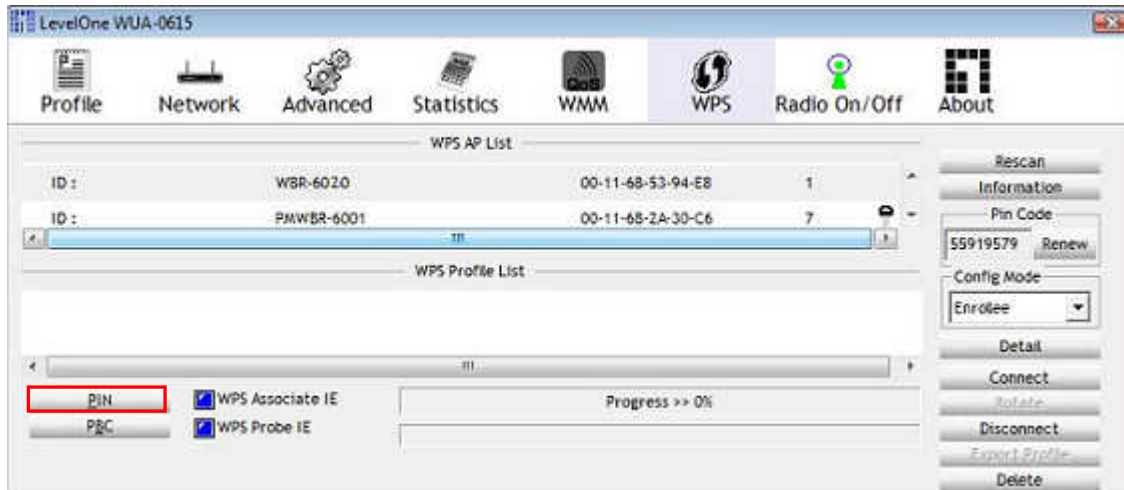
It is also possible to use the PIN number you have set on the wireless adapter. Set the adapter as Enrollee and enter the PIN you want.



Enter the enrollee's (computer's wireless adapter) PIN number and then click "Save."

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	36185641 <input type="button" value="Generate New PIN"/>
▶ Config Mode	<input type="text" value="Registrar"/>
▶ Config Status	UNCONFIGURED <input type="button" value="Set"/>
▶ Config Method	<input type="text" value="PIN Code"/> <input type="text" value="55919579"/>
▶ WPS status	Not in Use
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	
<b>Saved! Changes take effect immediately!</b>	

Now initiate the WPS by clicking the PIN button on the wireless adapter's utility.



## Push Button Method

Change the Config Method to "Push Button."

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	77869241 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Enrollee ▾
▶ Config Status	UNCONFIGURED <input type="button" value="Set"/>
▶ Config Method	<b>Push Button ▾</b>
▶ WPS status	Not in Use

**Saved! Changes take effect immediately!**

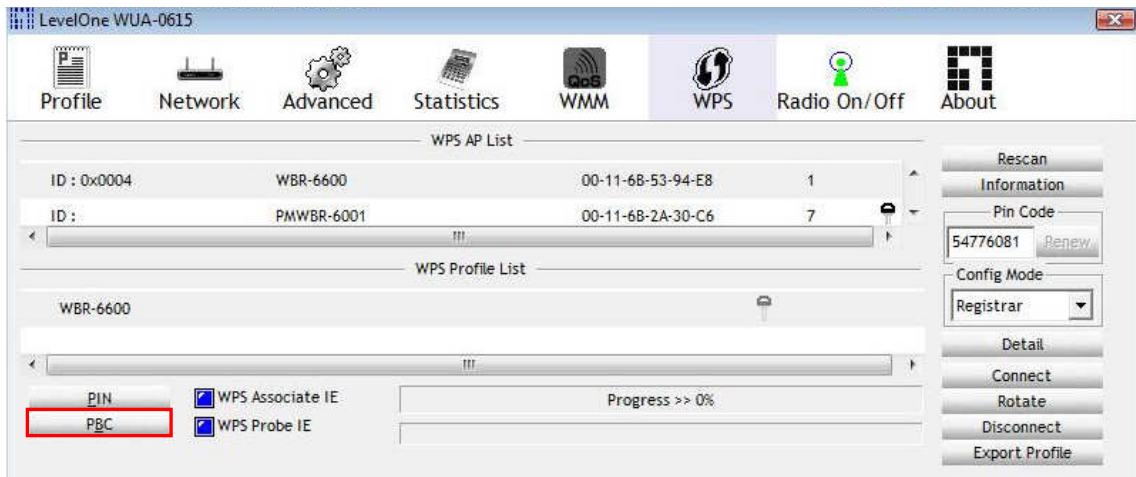
Then press the WPS button at the front of the router until the WLAN light starts flashing. This indicates that WPS is activated.



Then press and hold the WPS button on your wireless client for 1 second.



If your device has no physical WPS push button, then you can push the software button in the utility.



## WDS (Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

For maximum compatibility, it is recommended that WDS be set up using only the same models, in this case, WBR-6020. Also note that the standard only supports WEP encryption.

Click **Enable** to activate the WDS function.

Then type in the MAC addresses of other Access Points in the **Remote AP MAC** fields. Or you can copy the ones from **Scanned AP's MAC** list.

Click **Save** to save the settings and **Undo** to cancel.

**Note:** WDS supports WEP Wireless Encryption mode.

WDS Setting <span style="float: right;">[ Help ]</span>			
Item	Setting		
▶ Wireless Bridging	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
▶ Remote AP MAC 1	<input type="text"/>		
Remote AP MAC 2	<input type="text"/>		
Remote AP MAC 3	<input type="text"/>		
Remote AP MAC 4	<input type="text"/>		
▶ Encryption type	None ▾		
Scanned AP's MAC <span>-- select one --</span> ▾ <input type="button" value="Copy to"/> Remote AP MAC <span>--</span> ▾			
Wireless AP List			
ID	SSID	Channel	MAC Address
1	MeetingRoom	7	00:11:6B:B0:87:9C
2	WAP-0003	6	00:11:6B:60:6A:C5
3	ZyXEL	6	00:13:49:3D:DA:2D
4	QC-6000	11	00:11:6B:17:48:F6
5	WBR-6001TSD	11	00:11:6B:29:30:84
6	8FB1	6	00:09:7C:F1:F3:1B
7	MyPlace	2	00:18:84:A4:DB:06
8	TSD10	11	00:11:6B:39:A9:73
9	WAP-6010	11	00:05:9E:8D:85:C8
10	MyPlace	2	00:18:84:A4:DB:06
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Scan AP"/> <input type="button" value="Back"/>			

## Change Password

This page allows you to change the WBR-6020 Web Configuration password. Please type in the old password (factory default password is **password**) and then type in the new password.

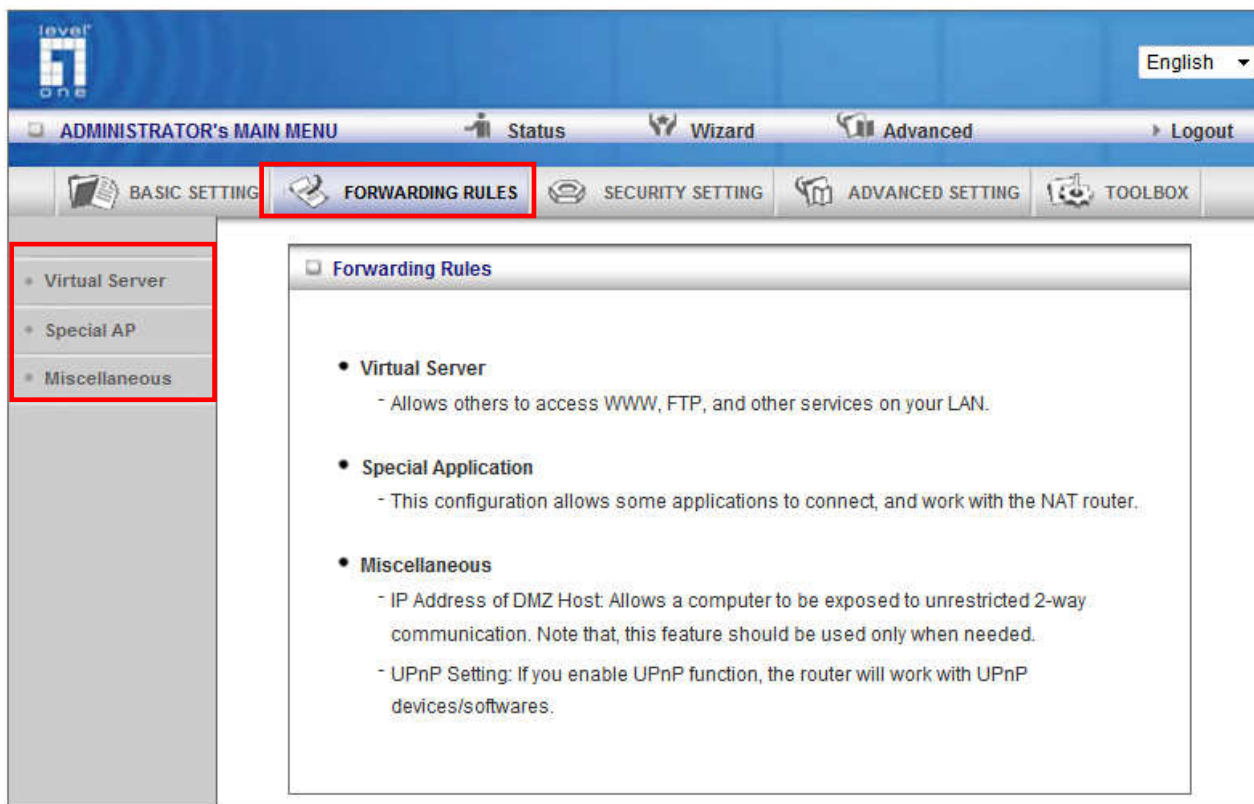
Change Password	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

If you change the password, make sure you use the new password next time you log into the web configuration.

Click **Save** to save the settings and **Undo** to cancel.

# Forwarding Rules

This page allows you to configure the port forwarding management of the WBR-6020. Use the menu on the left to access the setting pages.



The port forwarding feature is required because the Wireless Router's NAT (Network Address Translation) will block incoming traffic from the Internet to the LAN if the specific port mapping is not set up in the NAT table.

This is to provide a level of protection to computers on your LAN, however as a result creates connectivity problems when you want to make LAN resources available on the Internet. These include FTP servers, network game servers or other server applications.

There are three ways to work around the NAT and enable LAN resources on the Internet. Port Forwarding (Virtual Server), Port Triggering (Special AP page) and DMZ Host (Miscellaneous page).



## Virtual Server

Virtual Server
[ Help ]

Well known services -- select one -- Copy to ID --

ID	Server IP	Public Port	Private Port	Protocol	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
17	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
18	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
19	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always
20	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both	<input type="checkbox"/>	(0) Always

Save Undo

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule (Advanced Setting > Schedule).

For example, if you have an FTP server (port 21) at 192.168.0.1, a Web server (port 80) at 192.168.0.2, and a VPN server at 192.168.0.6, then you need to specify the following virtual server mapping table:

You can specify different ports to be used for Public and Private source and destinations.

Public Port	Private Port	Server IP	Enable
20	21	192.168.0.2	V
80	80	192.168.0.3	V
1721	1723	192.168.0.6	V

## Special AP

Special Applications <span style="float: right;">[ Help ]</span>			
Popular applications <span>--- Select one ---</span> <span>Copy to</span> ID <span>--</span>			
ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<span>Save</span> <span>Undo</span>			

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with the WBR-6020. The **Special Applications** feature allows some of these applications to work with this product. If this fails to make an application work, try setting that computer as the **DMZ host** instead. Please refer to Forwarding Rules > Miscellaneous section.

1. **Trigger:** The outbound port number that will be triggered by the application.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers and are allowed to pass through the firewall.

The WBR-6020 also comes with predefined settings for some popular applications. To use the predefined settings, select your application from the list, select an unused ID and then click **Copy** to add the predefined setting to your list.

**Note:** At any given time, only one PC can use each Special Application tunnel.

## Miscellaneous Items

Miscellaneous Items		[ Help ]
Item	Setting	Enable
▶ IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
▶ UPnP setting		<input checked="" type="checkbox"/>
▶ IGMP setting		<input type="checkbox"/>

### IP Address of DMZ Host

Here you can set the DMZ (Demilitarized Zone) Host. It is a computer that does not have the WBR-6020's built-in firewall applied. It allows the computer to be exposed to unrestricted communication to the Internet.

This setting is most commonly used for Internet gaming, Video conferencing, Internet telephony and other special applications.

To enable DMZ, enter the IP address of the PC and tick on Enable.

### UPnP Setting

The WBR-6020 supports Universal Plug and Play. However this depends on your operating system.

### IGMP setting

IGMP is a protocol used for multicasting applications where the content data is transmitted from one source to a number of recipients. This function must be enabled if any applications in your LAN are in a multicast group.

# Security Settings

This section allows you to configure the security management of the unit. Click on the menu on the left to access the respective setting page.

The screenshot displays the Level One administrator interface. At the top, there is a blue header with the Level One logo and a language dropdown set to 'English'. Below the header is a navigation bar with 'ADMINISTRATOR'S MAIN MENU' and icons for 'Status', 'Wizard', and 'Advanced', along with a 'Logout' link. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (highlighted with a red box), 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, a vertical menu is highlighted with a red box, listing 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Security Setting' and contains a list of security features:

- **Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- **Domain Filters**
  - Let you prevent users under this device from accessing specific URLs.
- **URL Blocking**
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- **MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- **Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

## Packet Filter

Packet Filters allows you to control what packets are allowed to pass through the WBR-6020. The Outbound Filter applies to all outbound packets and the Inbound Filter only applies to packets that are destined to Virtual Servers or the DMZ Host only.

The screenshot shows the 'Outbound Packet Filter' configuration window. At the top, there is a title bar with a close button and a '[ Help ]' link. Below the title bar is a table with two columns: 'Item' and 'Setting'. The 'Item' column contains 'Outbound Filter' and the 'Setting' column contains an 'Enable' checkbox, which is highlighted with a red box. Below this table are two radio buttons: 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. Below the radio buttons is a table with 5 columns: 'ID', 'Source IP', 'Destination IP : Ports', 'Enable', and 'Use rule#'. The table has 8 rows, each with an 'ID' from 1 to 8, empty input fields for 'Source IP' and 'Destination IP : Ports', an 'Enable' checkbox, and a 'Use rule#' dropdown menu set to '(0) Always'. At the bottom of the window, there are four buttons: 'Save', 'Undo', 'Inbound Filter...' (highlighted with a red box), and 'MAC Level...'.

To enable the Outbound Filter, tick the **Enable** tick box.

There are two types of filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound.

For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.0.1). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). You also need to add prefix "T" or "U" to specify TCP or UDP protocol, for example T80, U53, U20002999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses.

Packet Filter can also work with Scheduling Rules and give users more flexibility on Access control. For more detail, please refer to Scheduling Rule (Advanced Setting > Scheduling).

Each rule can be enabled or disabled individually.

### Inbound Filter:

To access the Inbound Packet Filter page, click on **Inbound Filter** on the bottom of the page. All settings on this page are similar to Outbound Filters.

Inbound Packet Filter <span style="float: right;">[ Help ]</span>				
Item		Setting		
▶ Inbound Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/>				

## Domain Filter

The Domain Filter enables you to prevent users from accessing specific domain addresses (web sites).

Domain Filter <span style="float: right;">[ Help ]</span>			
Item		Setting	
▶ Domain Filter		<input checked="" type="checkbox"/> Enable	
▶ Log DNS Query		<input checked="" type="checkbox"/> Enable	
▶ Privilege IP Addresses Range		From <input type="text" value="101"/> To <input type="text" value="105"/>	
ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text" value="www.sina.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text" value="www.google.com"/>	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

To enable Domain Filter, make sure to tick the **Enable** tick box.

- **Log DNS Query:** Check if you want to log the action when someone accesses the specific URLs.
- **Privilege HOST / Netmask:** Setting a group of computers that have privilege to access the internet without any restrictions.
- **Domain Suffix:** A suffix of URL to be restricted; For example, ".com", "xxx.com".
- **Action:** When someone is accessing the URL that meets the domain suffix, what kind of action you want the WBR-6020 to take. Tick on **Drop** to block the access and/or tick on **Log** to log this access.

In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.
2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.
3. URL include "www.google.com" will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

## URL Blocking

URL Blocking will block LAN computers from connecting to a pre-defined Web Site. The major difference between Domain Filter and URL Blocking is that Domain Filter requires the user to input suffixes (eg: xxx.com, ttt.net) while URL Blocking only requires user to input a keyword.

In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

URL Blocking [ Help ]		
Item	Setting	
▶ URL Blocking	<input checked="" type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text" value="msn"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="cnn"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="cnn"/>	<input checked="" type="checkbox"/>
4	<input type="text" value="espn"/>	<input checked="" type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>

To enable URL Blocking, make sure to tick **Enable**.

To set an URL Blocking rule, you will require:

- **URL:** If any part of the Website's URL matches the predefined word, the connection will be blocked.
- **Enable:** Tick to enable the rule.

In this example:

1. URL include "msn" will be blocked, and the action will be record in log-file.
2. URL include "sina" will be blocked, but the action will be record in log-file
3. URL include "cnnsi" will not be blocked, but the action will be record in log-file.
4. URL include "espn" will be blocked, but the action will be record in log-file



## MAC Address Control

The Domain Filter enables you to prevent users from accessing specific domain addresses (web sites).

MAC Address Control <span style="float: right;">[ Help ]</span>				
Item	Setting			
▶ MAC Address Control	<input checked="" type="checkbox"/> Enable			
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and <input type="text" value="allow"/> ▾ unspecified MAC addresses to connect.			
<input checked="" type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and <input type="text" value="deny"/> ▾ unspecified MAC addresses to associate. <b>Note: Association control has no effect on wired clients.</b>			
DHCP clients <input type="text" value="-- select one --"/> ▾ <input type="button" value="Copy to"/> ID <input type="text" value="--"/> ▾				
ID	MAC Address	IP Address	C	A
1	<input type="text" value="00:50:B6:05:B2:B1"/>	<input type="text" value="192.168.0.2"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="00:12:F0:13:B0:50"/>	<input type="text" value="192.168.0.3"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="00:0E:35:96:2E:32"/>	<input type="text" value="192.168.0.5"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" &lt;&lt; Previous"/> <input type="button" value=" Next &gt;&gt;"/> <input type="button" value=" Save"/> <input type="button" value=" Undo"/>				

To enable MAC Address Control, make sure to tick on **Enable**.

There are two types of controls available:

- **Connection Control:** To control which wired and wireless clients can connect to this device. If a client is denied access, it means the client cannot access the Internet either. Choose “allow” or “deny” to allow or deny the clients whose MAC addresses are not in the list.
- **Association Control:** To control which wireless client can be associated with this WBR-6020. If a client is denied, then it means the client cannot send or receive any data via this WBR-6020. Choose “allow” or “deny” to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless network.

<b>MAC Address</b>	MAC address indicates a specific client.
<b>IP Address</b>	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
<b>C</b>	When " <b>Connection control</b> " is checked, check " <b>C</b> " will allow the corresponding client to connect to this device.
<b>A</b>	When " <b>Association control</b> " is checked, check " <b>A</b> " will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combo box and button to help you to input the MAC address.

DHCP clients   ID

You can select a specific client in the DHCP clients Combo box, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combo box.

### Previous and Next Page

To make this setup page simple and clear, we have divided the "Control Table" into several pages. You can use these buttons to navigate to different pages.

### Example:

In this scenario, there are three clients listed in the Table. Clients 1 and 2 are wireless, and client 3 is wired.

1. The MAC Address Control" function is enabled.
2. **Connection Control** is enabled and all the wired and wireless clients not listed in the Control table are "Allowed" to connect to this device.
3. **Association control** is enabled, and all of the wireless clients not listed in the Control table are "Denied" to associate to the wireless LAN.
4. Clients 1 and 3 have fixed IP address either from the DHCP server of this device or manually assigned:

ID 1 - "00-50-B6-05-B2-B1" --> 192.168.0.2

ID 3 - "00-0E-35-96-2E-32" --> 192.168.0.5

Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

For example, Client 3 tries to use an IP address different from the address listed in the Control Table (192.168.0.5), it will be denied to connect to the WBR-6020.

5. Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.
6. Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

## Miscellaneous Items

This page allows you to change various miscellaneous security settings.

Miscellaneous Items		[ Help ]
Item	Setting	Enable
▶ Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)	
▶ Remote Administrator Host : Port	<input type="text"/> : <input type="text" value="8080"/>	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>

**Administrator Timeout:** The amount of time with no activity before the user will be logged out of the web configuration pages. Set to zero to disable this feature.

**Remote Administrator Host/Port:** By default, only LAN user can browse the built-in web configuration pages to perform administration task. This feature enables you to perform administration task from the Internet. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is blank, any host can connect to this product to perform administration task.

For better security, you can specify just one IP address or use subnet mask bits “/n” notation to specify a group of trusted IP addresses. For example, "10.1.2.0/24".

**NOTE:** When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port.

**Discard PING from WAN side:** When enabled, any host on the WAN cannot ping this MobilSpot™.

### DoS Attack Detection:

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

# Advanced Settings

These pages allow you to configure the more advanced settings on the unit.

The screenshot displays the Level One administrator interface. At the top, there is a blue header with the Level One logo on the left and a language dropdown menu set to 'English' on the right. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU' and icons for 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains icons and labels for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (highlighted with a red box), and 'TOOLBOX'. On the left side, a vertical sidebar menu lists several options: 'Status', 'System Log', 'Dynamic DNS', 'QoS Rule', 'SNMP', 'Routing', 'System Time', and 'Schedule Rule'. The 'Status' option is highlighted with a red box. The main content area is titled 'Advanced Setting' and contains a list of configuration options, each with a brief description:

- **System Log**
  - Send system log to a dedicated host or email to specific receipts.
- **Dynamic DNS**
  - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- **QoS Rule**
  - Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- **SNMP**
  - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- **Routing**
  - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- **System Time**
  - Allow you to set device time manually or consult network time from NTP server.
- **Schedule Rule**
  - Apply schedule rules to Packet Filters and Virtual Server.

## System Log

The WBR-6020 supports both Syslog (using UDP packets) and E-Mail alert.

System Log		[ Help ]
Item	Setting	Enable
▶ IP Address for Syslog	<input type="text"/>	<input type="checkbox"/>
▶ Setting of Email alert		<input type="checkbox"/>
• SMTP Server IP/Port	<input type="text"/> : <input type="text"/>	
• SMTP User name	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail address	<input type="text"/>	
• E-mail Subject	<input type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="View Log..."/> <input type="button" value="Email Log Now"/>		

For Syslog, you will need to enter the IP address of the host computer that will be receiving the syslog messages and tick on **Enable**.

For E-Mail alert, you will need to define the following:

- **E-Mail Alert:** Tick **Enable** to enable this feature.
- **SMTP Server IP and Port:** Enter the IP address and port of the SMTP server, separated by “.” (no quotes). If you do not specify the port number, the default value of 25 will be used.
- **SMTP User Name / Password:** Username and Password if your SMTP server requires log in.
- **E-mail address:** Enter the e-mail addresses of the recipients for the email logs. To assign more than one recipient, use “;” or “,” (no quotes) to separate the e-mail addresses.
- **E-Mail Subject:** Enter the subject for the e-mail (optional)

## Dynamic DNS

Dynamic DNS is a feature that allows users to set up a static domain name even when they have a dynamic internet IP address. So even if your IP address changes every time you connect to your ISP, the IP address can be mapped to a host name so that anyone who wants to connect to the WBR-6020, or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP address which might change.

Dynamic DNS <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Before you enable **Dynamic DNS**, you need to register an account on one of the supported Dynamic DNS providers in the list. After successfully registering the account, the Dynamic DNS provider would provide you with the following details:

- Host Name
- Username/Email
- Password

To enable Dynamic DNS click the check box next to Enable in the DDNS field and choose the respective Dynamic DNS provider. Enter the required details and then click **Save** to save the settings or **Undo** to cancel.

## QoS Rule

Here you can set the parameters for QoS (Quality of Service). This function allows you to specify which types of data packets are given priority. For example you can increase the priority of Voice Over IP or gaming packets so that they are handled first by WBR-6020.

QoS Rule					
Item			Setting		
▶ QoS Control			<input type="checkbox"/> Enable		
▶ Bandwidth of Upstream			<input type="text"/> kbps (Kilobits per second)		
ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

To enable QoS Control, tick **Enable**.

**Local IP:** Please input Client IP, Example: 192.168.12.33. This is the computer that the rule applies.

**Remote IP:** Please input Global IP and port, Example: 168.96.2.3 and port 21. This is so that the QoS Rule only applies to packets from this Internet source.

**Priority:** Please set whether this particular rule should be given a High, Normal or Low priority.

**Schedule Rule #:** Specify which schedule this rule will follow. Eg: What times the rule applies.

## SNMP Setting

SNMP (Simple Network Management Protocol) is designed to give users the ability to remotely manage a computer or network device.

SNMP Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

To enable SNMP, please set the following:

- **Enable SNMP:** You must check either Local or Remote or both to enable SNMP function. If Local is checked, this unit will respond to requests from LAN. If Remote is checked, the unit will respond to requests from WAN.
- **Get Community:** Set the community of GetRequest. This will act as a password.
- **Set Community:** Set the community of SetRequest. This will act as a password.
- **IP 1,IP 2,IP 3,IP 4:** Enter the IP addresses of the managed PCs. The unit will send SNMP Trap messages only to the IP addresses listed.
- **SNMP Version:** Please select the SNMP Version of your SNMP Management software.

Click on **Save** to save the settings or **Undo** to cancel.



## Routing

When you have more than one WBR-6020, or router with different subnets on the network, you will need to enable this function to allow the different subnets to communicate with each other.

Routing Table <span style="float: right;">[ Help ]</span>					
Item		Setting			
▶ Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
▶ Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

There are two types of routing supported by the WBR-6020.

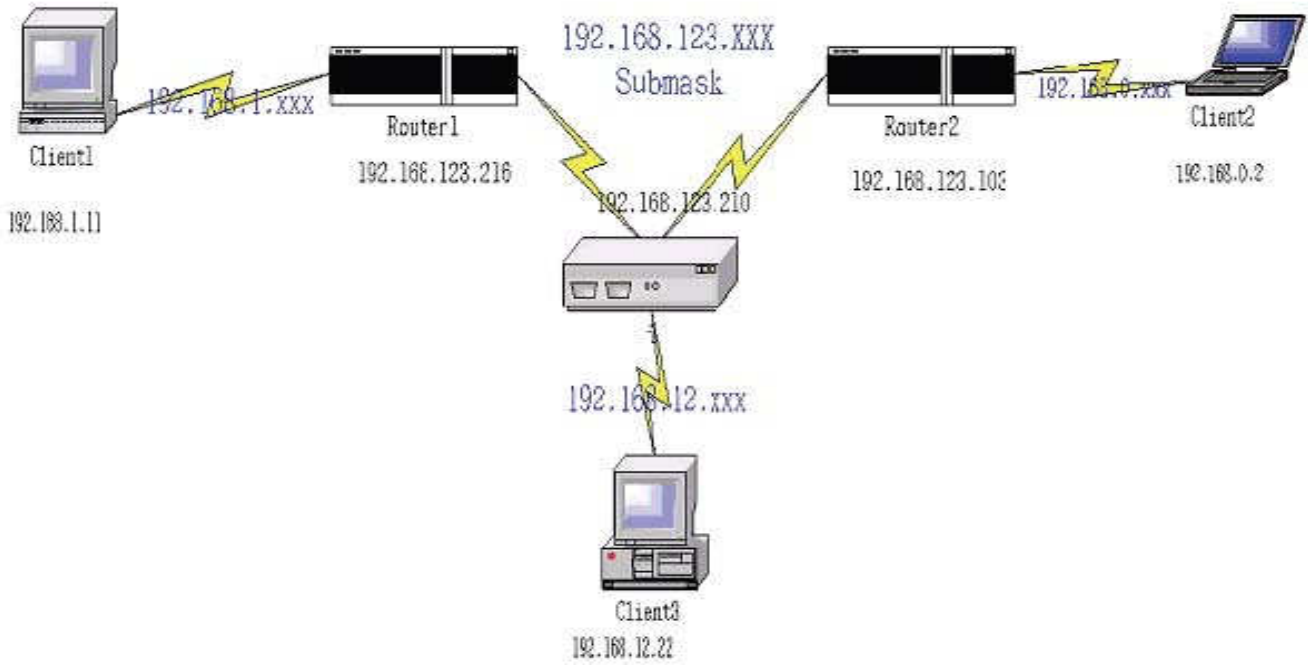
- **Dynamic Routing:** This method uses Routing Information Protocol (RIP) to enable the devices to determine the best route for each packet based on the number of hops between the source and destination.

Tick the **Enable** box to enable Dynamic Routing. Use RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

- **Static Routing:** Allows computers that are connected to the WBR-6020 to communicate with computers on other LAN segments which are connected to the WBR-6020 using a different router. You can specify up to eight routing rules.

The details below are required to set the routing rules:

- IP Address
- Subnet Mask
- Gateway
- Hop, number of hops
- Tick **Enable** for each rule.



Destination	Subnet Mask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

So if, for example, Client3 wants to send an IP data packet to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (Router 2)

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216 (Router 1)  
 Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

## System Time

This page allows you to set the time settings of the WBR-6020.

System Time <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi ▼
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/>	
<input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Tuesday July 28, 2009 15:44:46)"/>	

**Time Zone:** Select the time zone for your location.

**Auto-Synchronization:** The router will automatically keep sync with a NTP Time Server.

**Sync with Time Server:** Force the router to sync with a Time Server.

**Sync with my PC:** The router will use the time set on your computer.

## Schedule Rule

This feature allows you to define the time schedule of Virtual Server and Packet Filter rules.

Schedule Rule		[ Help ]
Item	Setting	
▶ Schedule	<input checked="" type="checkbox"/> Enable	
Rule#	Rule Name	Action
1		New Add
2		New Add
3		New Add
4		New Add
5		New Add
6		New Add
7		New Add
8		New Add
9		New Add
10		New Add
<input data-bbox="507 1115 667 1144" type="button" value=" &lt;&lt; Previous "/> <input data-bbox="687 1115 778 1144" type="button" value=" Next &gt;&gt; "/> <input data-bbox="799 1115 858 1144" type="button" value=" Save "/> <input data-bbox="863 1115 1086 1144" type="button" value=" Add New Rule..."/>		

To enable Scheduling, tick **Enable** and click **Save**.

Then create new rules by pressing the **New Add** button.

Schedule Rule Setting <span style="float: right;">[ Help ]</span>			
Item		Setting	
▶ Name of Rule 1		<input type="text"/>	
▶ Policy		Inactivate <input type="button" value="v"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Sunday <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
2	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
3	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
4	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
5	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
6	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
7	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
8	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>			

Enter the Rule's Name and set the Start and End Times for each day. Then click **Save** to save the new rule.

Once defined, you can use it for Virtual Server and Packet Filters by entering the rule number in the "Schedule Rule#" fields.

# Toolbox

This section has some basic tools to maintain the WBR-6020's systems.

The screenshot displays the Level One WBR-6020 web interface. At the top, there is a blue header with the Level One logo and a language dropdown set to 'English'. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX', with 'TOOLBOX' highlighted by a red box. On the left side, a sidebar menu is visible, with 'System Info', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous' listed, all of which are also highlighted by a red box. The main content area is titled 'Toolbox' and contains a list of tools with their descriptions:

- **View Log**
  - View the system logs.
- **Firmware Upgrade**
  - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
  - Save the settings of this device to a file.
- **Reset to Default**
  - Reset the settings of this device to the default values.
- **Reboot**
  - Reboot this device.
- **Miscellaneous**
  - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
  - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

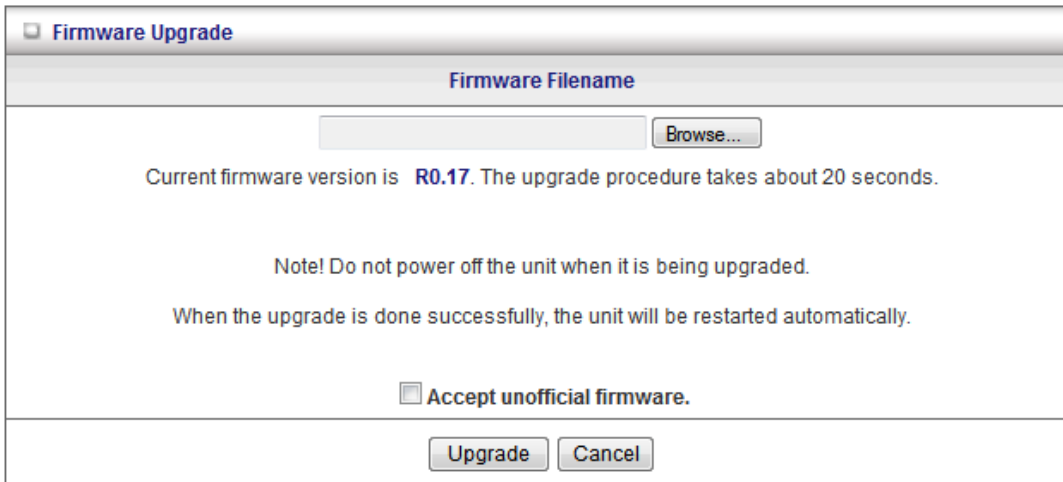
# System Info

View the Log of the router. It can also be exported to a text file.

System Information	
Item	Setting
▶ WAN Type:	Dynamic IP Address
▶ Display time	2009/01/02 09:45:29
System Log	
Time	Log
Jan 2 02:45:47	commander: CMD_DHCP_renew: ip=0.0.0.0 nm=0.0.0.0
Jan 2 02:45:48	udhcpd[17816]: udhcpd (v0.9.9-pre) started
Jan 2 03:11:25	udhcpd[18090]: Sending discover...
Jan 2 03:11:28	udhcpd[18090]: Sending discover...
Jan 2 03:11:31	udhcpd[18090]: Sending discover...
Jan 2 03:11:34	udhcpd[18090]: No lease, failing.
Jan 2 03:11:34	udhcpd[18115]: udhcpd (v0.9.9-pre) started
Jan 2 03:11:36	udhcpd[18391]: Received SIGTERM
Jan 2 03:11:38	commander: CMD_DHCP_renew: ip=0.0.0.0 nm=0.0.0.0
Jan 2 03:11:38	udhcpd[18426]: udhcpd (v0.9.9-pre) started
Jan 2 03:24:21	udhcpd[18700]: Sending discover...
Jan 2 03:24:24	udhcpd[18700]: Sending discover...
Jan 2 03:24:27	udhcpd[18700]: Sending discover...
Jan 2 03:24:30	udhcpd[18700]: No lease, failing.
Jan 2 03:24:31	udhcpd[18721]: udhcpd (v0.9.9-pre) started
Page: 1/67 (Log Number: 1000)	
<input data-bbox="517 1279 676 1312" type="button" value=" &lt;&lt; Previous "/> <input data-bbox="687 1279 783 1312" type="button" value=" Next &gt;&gt; "/> <input data-bbox="799 1279 927 1312" type="button" value=" First Page "/> <input data-bbox="943 1279 1070 1312" type="button" value=" Last Page "/>	
<input data-bbox="600 1319 703 1352" type="button" value=" Refresh "/> <input data-bbox="715 1319 847 1352" type="button" value=" Download "/> <input data-bbox="858 1319 995 1352" type="button" value=" Clear logs "/>	

## Firmware Upgrade

This page allows you to perform updates to the firmware of the WBR-6020.



The screenshot shows a dialog box titled "Firmware Upgrade". At the top, there is a header bar with the title. Below the header, the text "Firmware Filename" is centered. Underneath, there is a text input field followed by a "Browse..." button. The main body of the dialog contains the following text: "Current firmware version is R0.17. The upgrade procedure takes about 20 seconds." followed by a "Note! Do not power off the unit when it is being upgraded." and "When the upgrade is done successfully, the unit will be restarted automatically." Below this text is a checkbox labeled "Accept unofficial firmware." At the bottom of the dialog, there are two buttons: "Upgrade" and "Cancel".

To use, click **Browse** and locate the firmware image file, then click **Upgrade**.

**Note:** Please connect to the WBR-6020 using a wired LAN connection as if the connection breaks during the update, it will render the unit unworkable. Also disable any anti-virus or firewall program before beginning the update.

**Accept unofficial firmware:** Force the router to accept unofficial firmware files. LevelOne does NOT recommend this function be used.

### Backup Setting

You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

### Reset to Default

You can also reset the unit back to factory default settings by clicking the **Reset to Default** button and click OK. Please wait while the unit reboots.

### Reboot

To reboot the unit manually, click the **Reboot** button and click OK.



## Miscellaneous Items

Miscellaneous Items <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

### MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

### Domain Name or IP Address for Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

# Appendix A 802.1x Setting

---

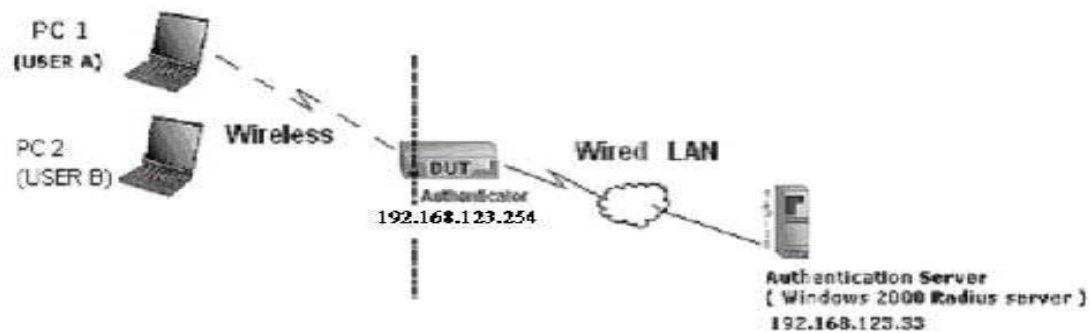


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

## Equipment Details

**PC1:** Microsoft Windows XP Professional without Service Pack 1 and LevelOne Wireless PCI Card

**PC2:** Microsoft Windows XP Professional with Service Pack 1a or later and LevelOne Wireless PCI Card.

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.



Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 (You can get more information from <http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>)

## DUT Configuration:

1. Enable DHCP server.
2. WAN setting: static IP address.
3. LAN IP address: 192.168.123.254/24.
4. Set RADIUS server IP.
5. Set RADIUS server shared key.
6. Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP\_TLS, PEAP\_CHAPv2(Windows XP with SP1 only), and PEAP\_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

## DUT and Windows 2000 Radius Server Setup

### Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5\_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

### Setup DUT

1. Enable the 802.1X (check the “Enable checkbox”).
2. Enter the RADIUS server IP.
3. Enter the shared key. (The key shared by the RADIUS server and DUT).
4. We will change 802.1X encryption key length to fit the variable test condition.

### Setup Network adapter on PC

1. Choose the IEEE802.1X as the authentication method. (Fig 2)
2. Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
3. If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer.
4. We will change EAP type to fit the variable test condition.



Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

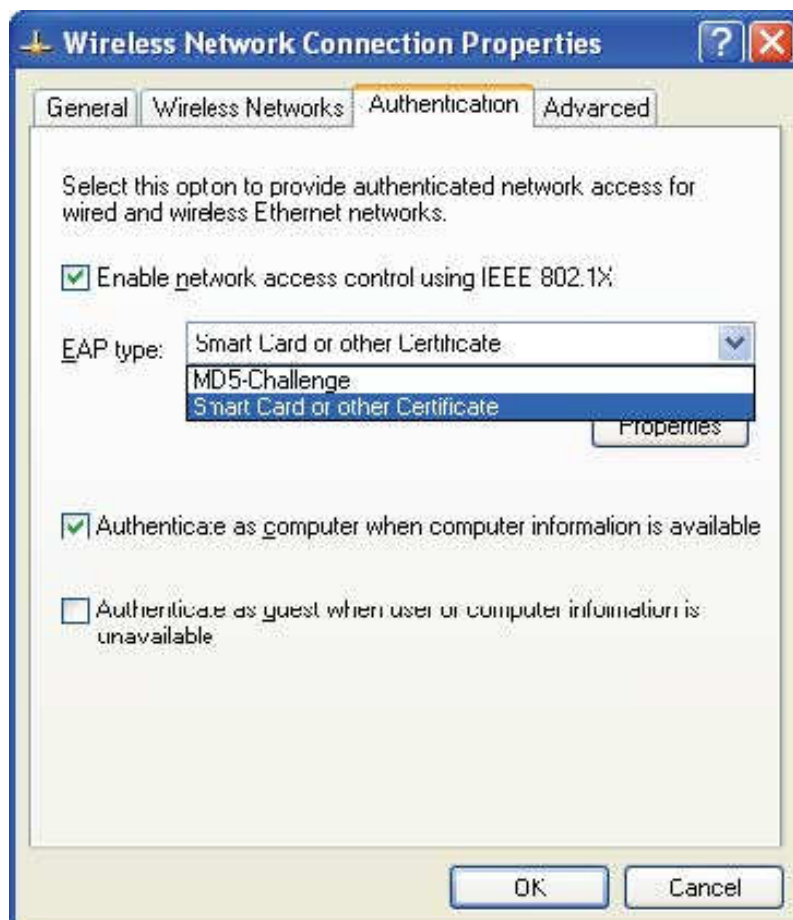


Figure 2: Enable IEEE 802.1X access control / Smart card or certificate properties

## Windows 2000 RADIUS server Authentication testing:

DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 chooses the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP\_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. ( Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

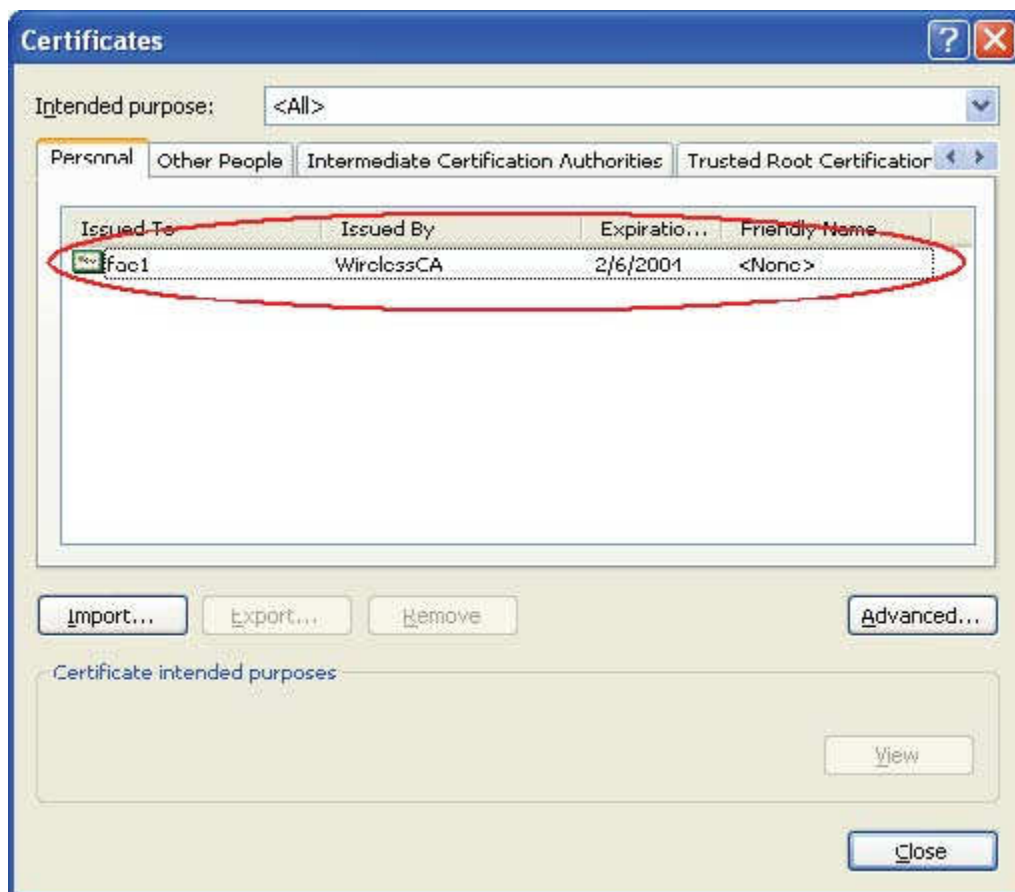


Figure 4: Certificate information on PC1

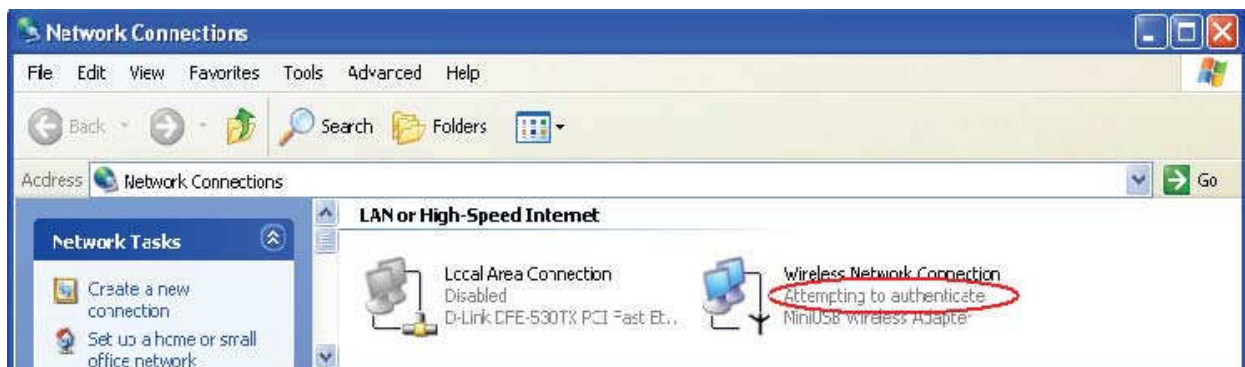


Figure 5: Authenticating

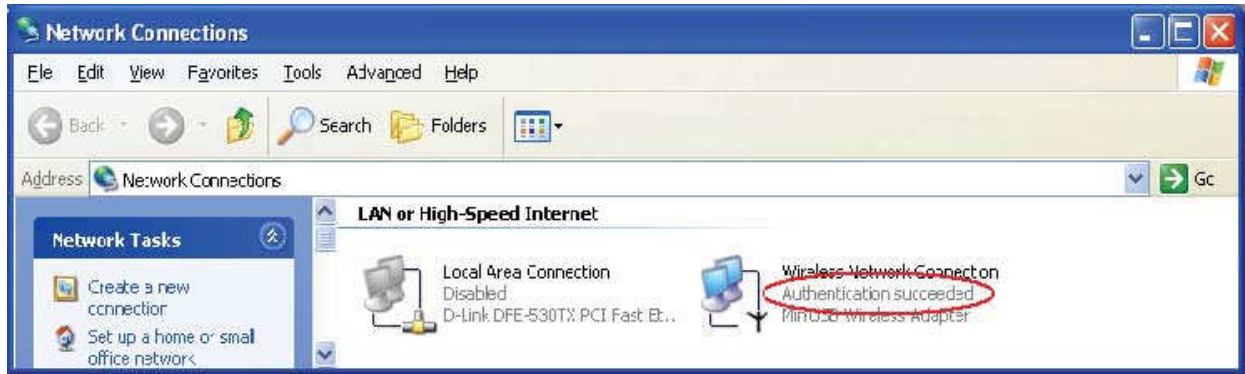


Figure 6: Authentication success

DUT authenticate PC2 using PEAP-TLS.

1. PC2 chooses the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP\_TLS.
3. Disable the wireless connection and enable again.
4. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

**Support Type:** The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.

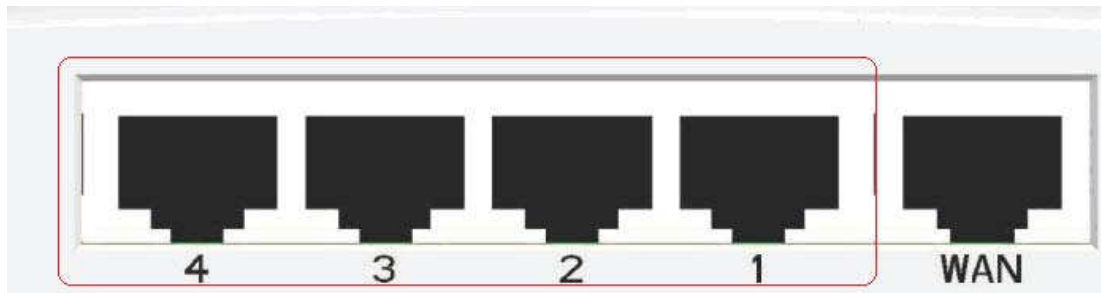
# Appendix B FAQ and Troubleshooting

---

## What can I do when I have some trouble at the first time?

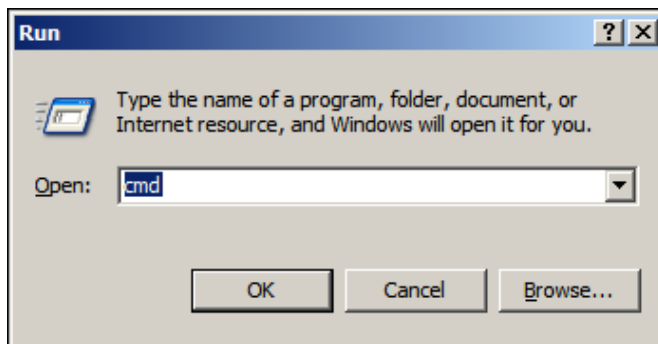
1. Why can't I configure the router even if the cable is plugged in the ports of Router and the LED is also lit?

A: First, make sure that which port is plugged. If the cable is in the WAN port, please change to plug in LAN port 1 or LAN port 4:



Then, please check if your PC can get an IP address from the Router.

Click Start, Run



Type **CMD** and then click “OK”

Type **ipconfig** in the command prompt as shown below.

```
Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.0.169
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

If you see that your PC has an IP address, then open your Web-Browser, and type 192.168.0.1 in the address bar.

If not, please type **ipconfig /release**, then **ipconfig /renew**, to update your IP address.

## 2. Why can't I connect the router even if the cable is plugged in LAN port and the LED is light?

**A:** First, please check Status LED. If the device is normal, the LED will blink once per second. If not, please check the blinking Status LED as shown:

### **Status LED stays constantly on or off:**

The system is frozen. Suggest powering off and on the router. If this symptom continues to occur, please reset to default settings or upgrade to the latest firmware and try again.

**Status LED flashes irregularly:** There is an error in the system. Please reset to default settings and reboot the router.

## 3. How to reset to factory default?

**A:** There are 2 methods to reset to default.

### **Method 1) Restore with RESET button (WLAN and WPS together)**

First, turn off the router. Then press the WLAN and WPS buttons together and power on the router. Keep the buttons pressed until the Status LED starts flashing, and then remove your fingers. If the Status LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat steps and try again.

### **Method 2) Restore directly when the router power on**

First, push the WLAN and WPS buttons for about 5 seconds (Status will start flashing about 5 times), remove the finger. The RESTORE process is completed.

4. Why can I not connect to the Internet even though the cables are plugged in WAN port and LAN port and the LEDs are blink? In addition, the Status LED is also normal and I can configure the web management?

A: Make sure that the network cable from DSL or Cable modem is plugged in WAN port of Router and that the network cable from LAN port of router is plugged in Ethernet adapter. Then, please check which WAN type you use. If you are not sure, please call the ISP. Then please go to this page to input the information given to you by your ISP.

Primary Setup <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.0.1"/>
▶ WAN Type	Dynamic IP Address ▾
▶ Host Name	Static IP Address Dynamic IP Address (optional)
▶ ISP registered MAC Address	PPP over Ethernet PPTP L2TP <input type="button" value="Clone"/>
▶ Connection Control	Connect-on-Demand ▾
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Virtual Computers..."/>	

5. When I use Static IP Address to connect to the Internet, I can access or ping global IP addresses such as 202.93.91.218. However, I cannot access the a website by using its domain name, for example <http://espn.com> ?

A: Please check the DNS configuration of Static IP Address. Please refer to the information of ISP and assign one or two DNS servers.



## How do I connect router by using wireless?

### 1. How to start to use wireless?

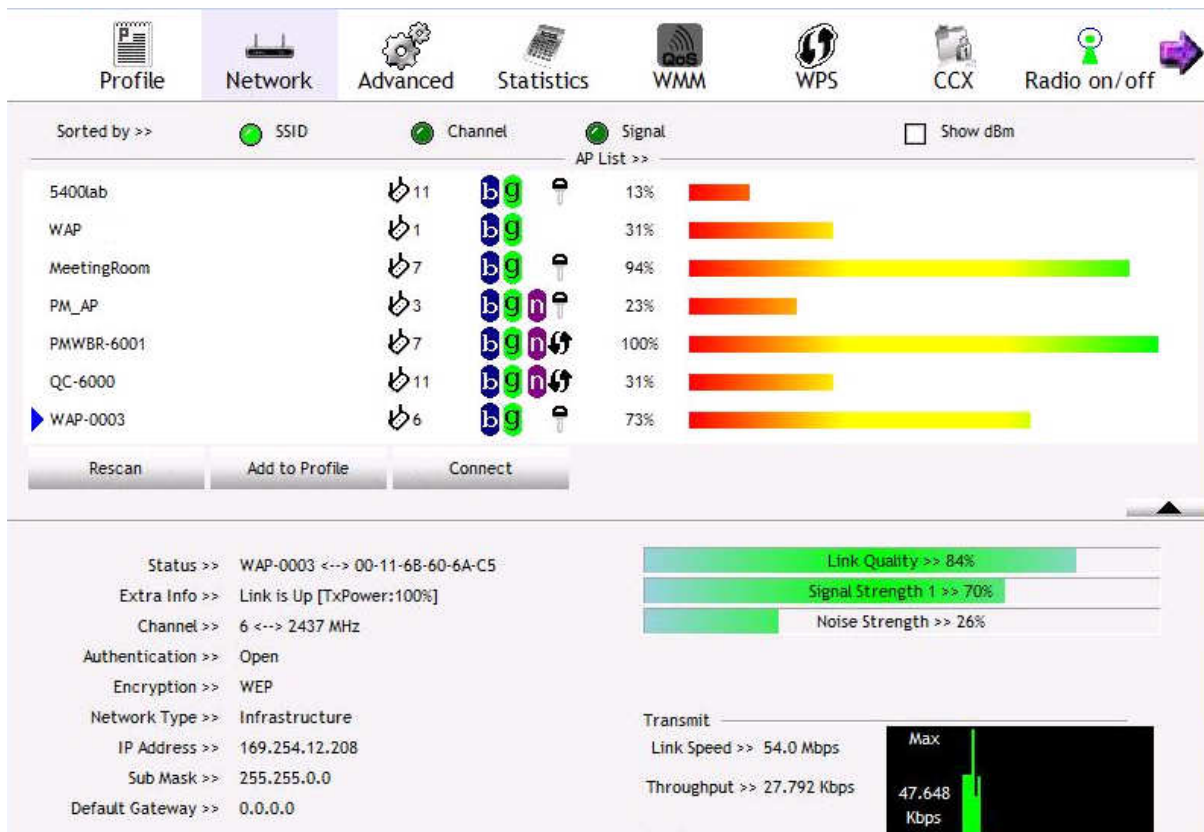
**A:** First, make sure that you already installed wireless client device in your computer. Then check the configuration of wireless router. The default is below:

Wireless Setting <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Wireless Operation Mode	AP mode ▼
▶ Network ID(SSID)	WBR-6020
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Channel	Auto ▼
▶ Wireless Mode	11 B/G/N mixed ▼
▶ Security	None ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS..."/> <input type="button" value="Wireless Client List..."/>	

About wireless client, you will see wireless icon:

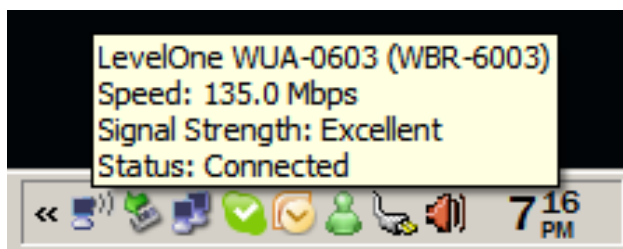


Then click and will see the AP list that wireless client can be accessed:



If the client cannot find your wireless router, please refresh network list again. Choose the one that you will want to connect and connect:

If successfully, the computer will show something similar.



User will also retrieve IP from router, for example:

```

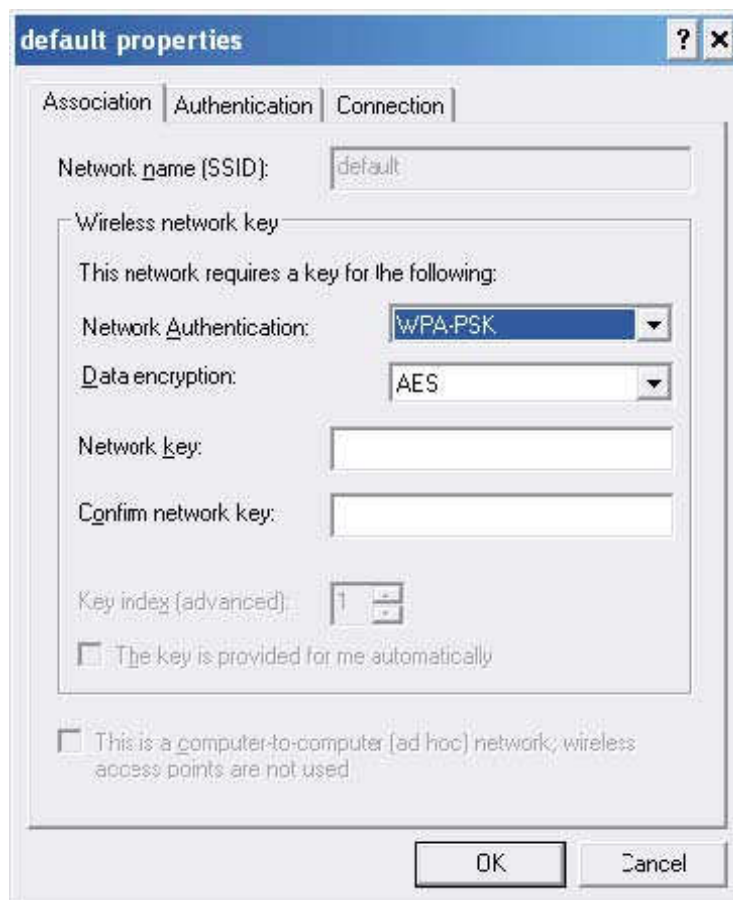
Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.0.169
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
  
```

## 2. How can I use AES encryption of WPA-PSK to connect?

**A:** First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:



If SSID is default and click “Properties” to check if the driver of wireless client supports AES encryption.



## 3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?

**A:** Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.

# Technical Specifications

<b>General</b>	
Model	WBR-6020 <i>N_Max Wireless Router</i>
Data Transfer Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps Max physical rate up to 300 Mbps in 802.11n mode
Transmit Power	802.11b: 17±2dBm 802.11g: 15±2dBm 802.11n: 14±2dBm
Frequency Range	America/ FCC: 2.412~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Channels	1~11 channels (FCC), 1~13 channels (ETSI),
Security	WEP Encryption, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.1x
Diagnostic LED	Sleep Status WAN WLAN LAN
Antenna	2x 2dbi Removable and 1x 2dbi Internal Antennas
<b>Physical and Environmental</b>	
Operating Systems Supported	Windows 2000, Windows XP, Windows Vista, Linux, MAC OSX
Temperature	Operating: 0° ~ 40° C, Storage: -20° ~ 70° C
Humidity	10% ~ 85% RH, no condensation
Dimensions	187mm (L) x 112mm(W) x 29mm (D)
Certifications	FCC, CE