



LevelOne

User Manual

WBR-6003/ WBR-6006

150Mbps Wireless Router

Ver. 2.0

Safety

Federal Communication Commission Interference Statement

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 of the following measures:

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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-6003/ WBR-6006) 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

1. INTRODUCTION	6
USER MANUAL OVERVIEW	6
2. UNPACKING AND SETUP	7
FEATURES	7
PACKAGE CONTENTS	7
3. HARDWARE INSTALLATION	7
FRONT VIEW	7
REAR VIEW	8
HARDWARE INSTALLATION STEPS	9
4. CHECK YOUR NETWORK SETTINGS	10
5. CONFIGURATION WIZARD	11
6. ADVANCED SETUP	13
BASIC SETTING	14
Primary Setup	15
DHCP Server	20
Wireless Settings	21
Change Password	33
FORWARDING RULES	34
Virtual Server	35
Special AP	36
Miscellaneous Items	37
SECURITY SETTINGS	38
Packet Filter	39
Domain Filter	41
URL Blocking	42
MAC Address Control	43
Miscellaneous Items	45
ADVANCED SETTINGS	46
System Time	47
System Log	48
Dynamic DNS	49
SNMP Setting	50
Routing	51
Schedule Rule	53
QoS Rule	錯誤! 尚未定義書籤。
TOOLBOX	54
View Log	55
Firmware Upgrade	56
Backup Setting	56
Reset to Default	56
Reboot	56
Miscellaneous Items	57
APPENDIX A 802.1X SETTING	58
APPENDIX B FAQ AND TROUBLESHOOTING	62
TECHNICAL SPECIFICATIONS	68

Default Settings

IP Address	192.168.1.1
Password	admin
Wireless Mode	Enable
Wireless SSID	WBR-6003/ WBR-6006
Wireless Security	None

1. Introduction

Congratulations on your purchase of LevelOne WBR-6003/ WBR-6006 *150Mbps 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

Introduction	Describes the <i>150Mbps Wireless Router</i> .
Unpacking and Setup	Helps user to get started with the basic installation of the <i>150Mbps Wireless Router</i> .
Hardware Installation	Describes the LED indicators of the <i>150Mbps Wireless Router</i> .
Configuration	Describes the functionalities and its settings.
Technical Specifications	Lists the technical (general, physical and environmental) specifications of the <i>150Mbps Wireless Router</i> .

2. Unpacking and Setup

This chapter provides the package contents and setup information for the *150Mbps Wireless Router*.

Features

- Extended and high-speed wireless connectivity with wireless *N* technology
- Advanced QoS Services for Intelligent Internet
- Backward compliant with IEEE802.11g and 11b standards
- Operates on the 2.4GHz frequency band
- Stay Protected with Advanced Network Security
- WEP and WPA/WPA2-PSK encryption supported along with Wi-Fi Protected Setup
- Integrate 4-Port Fast Ethernet Switch with 10/100Mbps MDI-MDI-X auto-sensing
- Built-in NAT function allows multiple PCs and devices to share Internet connection
- Browser-based interface configuration and management
- Quick Setup Wizard provides alternative way to manage device

Package Contents

Open the box of the *150Mbps Wireless Router* and carefully unpack it. The box should contain the following items:

- WBR-6003/ WBR-6006 *150Mbps Wireless Router*
- Power Adapter
- Cat.5 Cable
- Antenna x1
- 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



1) WLAN Button/ WPS Button

- Press and hold for 3 seconds to turn the Wireless LAN on or off.
- Please confirm WLAN status as indicated by WLAN Light
- It is also Wi-Fi Protected Setup push button. Press and hold for 1 seconds to activate WPS pairing with wireless client when WLAN is on.

2) Status

- A steady blinking light indicates the device is ready

3) WAN

- A solid light indicates the WAN port is connected.

4) WLAN Light

- A solid light indicates the Wireless LAN is turned on and ready for use.
- Off indicates Wireless LAN is turned off.
- LED blinks during wireless data transmission.
- Steady blinking indicates WPS function is activated and the router is pairing with wireless client.

5) LAN Lights

- A solid light indicates to an Ethernet enable computer on ports 1 ~ 4.
- LED blinks during data transmission.

Rear View



1) Power Jack

- Receptor for the supplied power adapter

2) LAN Ports (1~4)

- Connect Ethernet devices such as computers, switches or hubs.

3) WAN Port

- The WAN port is the connection for the Ethernet cable to the Cable or DSL Modem.

4) Antenna

- 3dBi fix antenna allows users to have a wider range signal coverage.

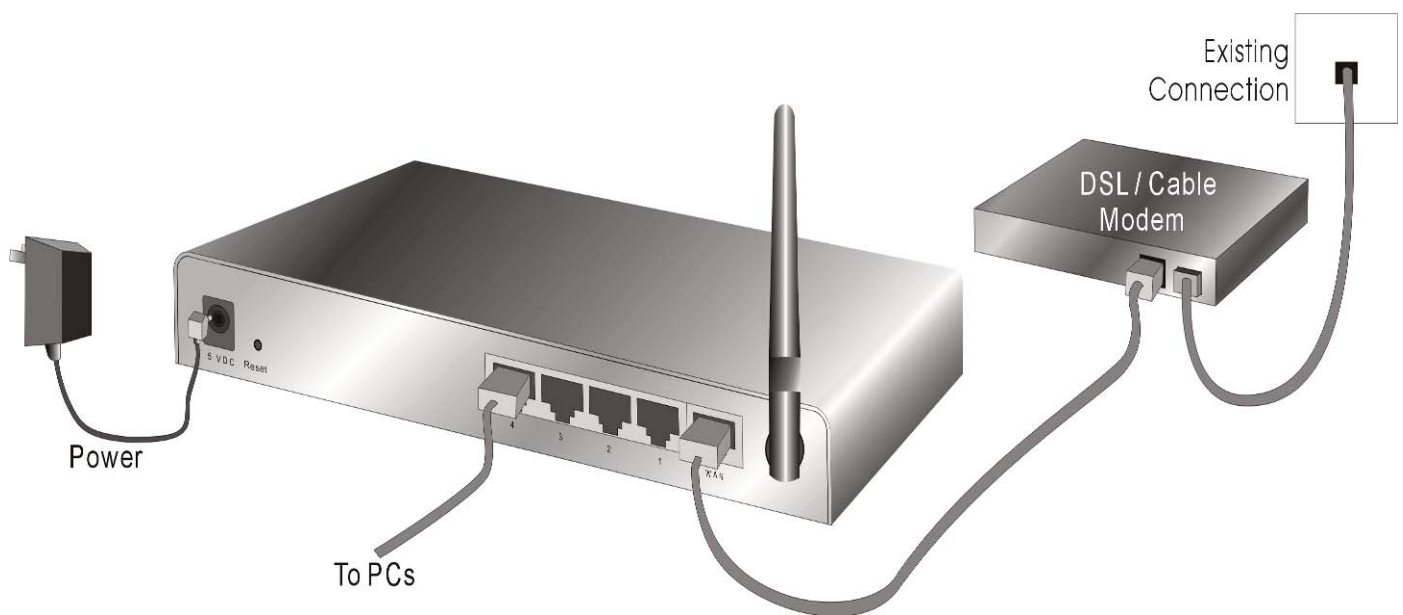
Hardware installation steps

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.

Setup LAN connection

- **Wired LAN connection:** Connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of the Wireless Router.
- **Wireless LAN connection:** Locate the WBR-6003/ WBR-6006 at a proper position to gain the best transmit performance.



3. Setup WAN connection

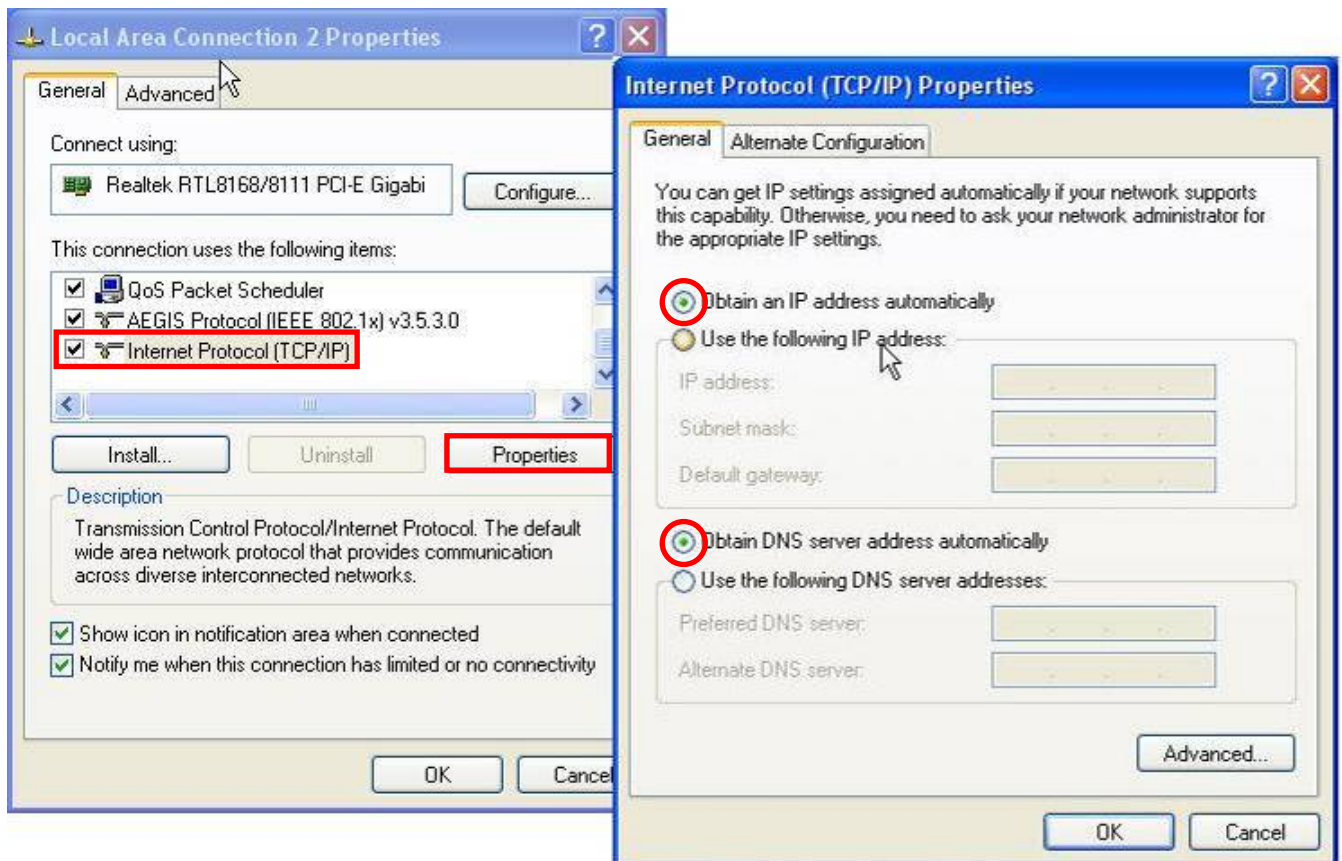
Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone.

4. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the **Status** indicator will be lighted ON for about 10 seconds, and then it will be flashed 3 times to indicate that the self-test operation has finished. Finally, the Status indicator will be continuously flashing once per second to indicate that this product is in normal operation.

4. Check Your Network Settings

1. Please make sure your PC can get IP address automatically so the WBR-6003/ WBR-6006 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-6003/ WBR-6006 *150Mbps Wireless Router* will obtain and assign IP address information automatically. Configuration settings can be established through the Web-Based Configuration Menu.

Open a web browser (Internet Explorer/Firefox/Safari) and type in the IP Address <http://192.168.1.1>

Note:

If you have changed the default IP Address assigned to the WBR-6003/ WBR-6006, ensure you enter the correct IP Address.



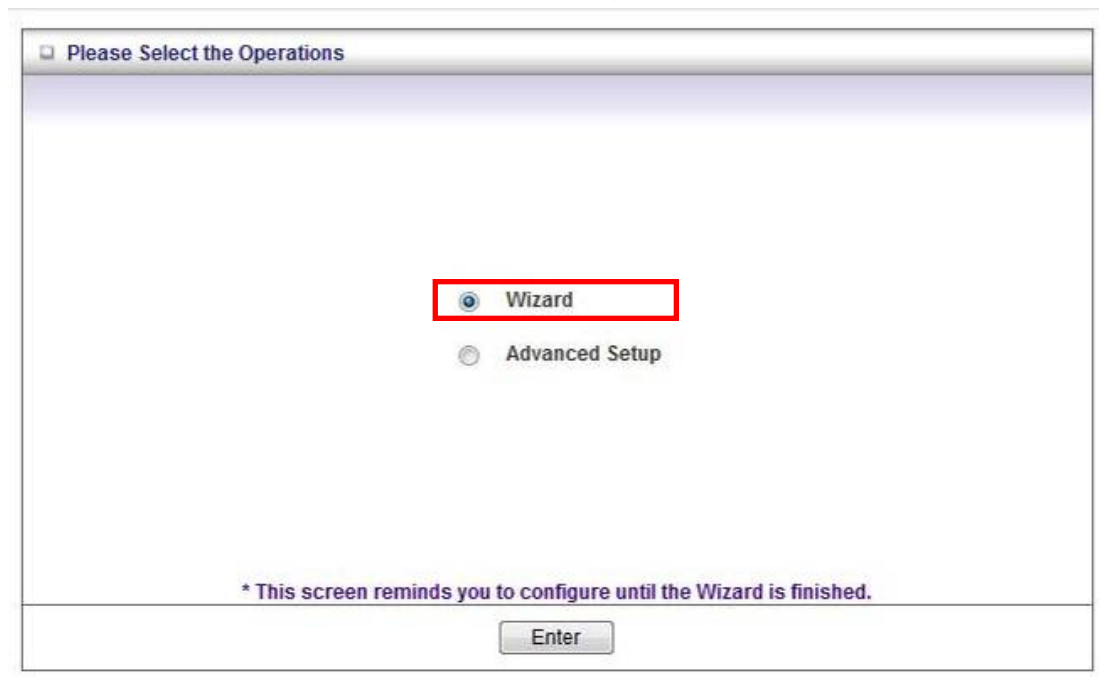
Type in “**admin**” (without quotes) in the Password box, Then click Login

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

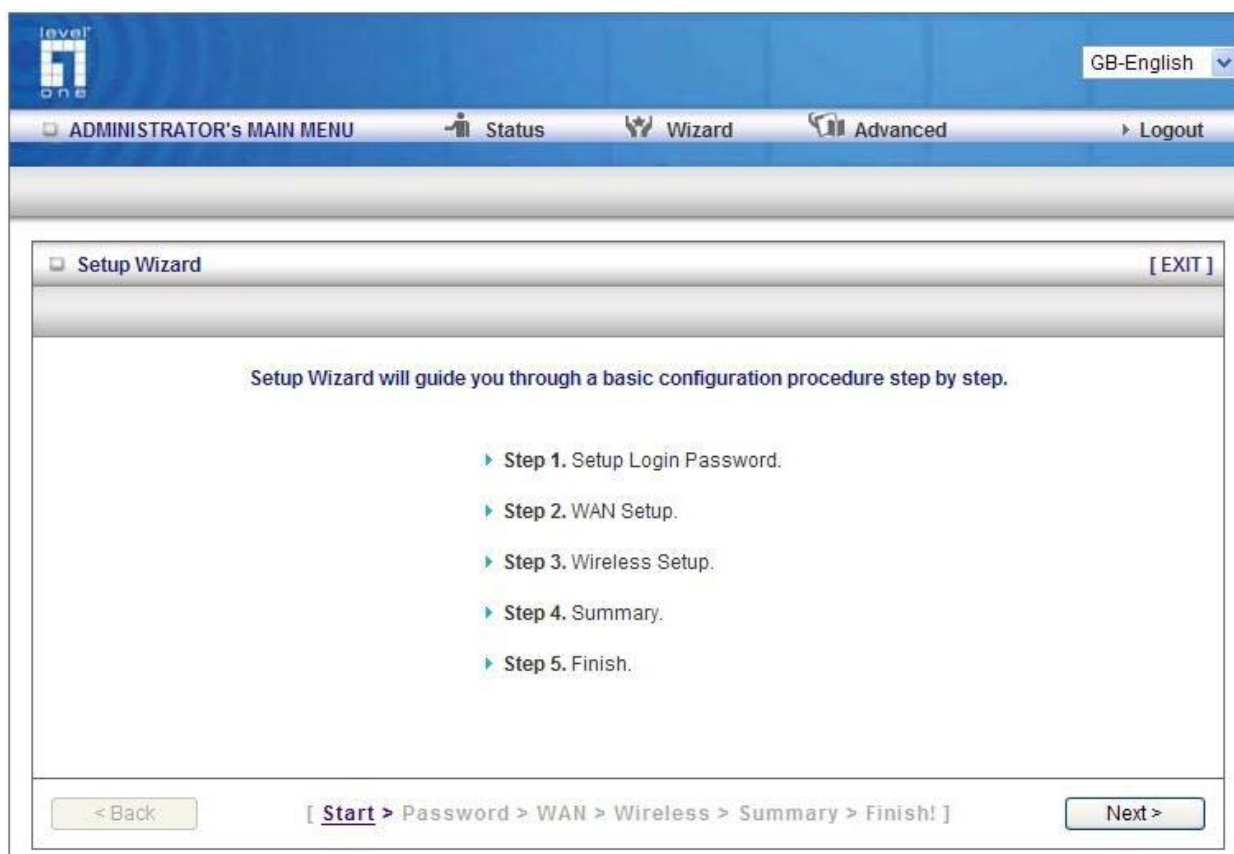


The user can setup step by step to finish the connection with Wizard.

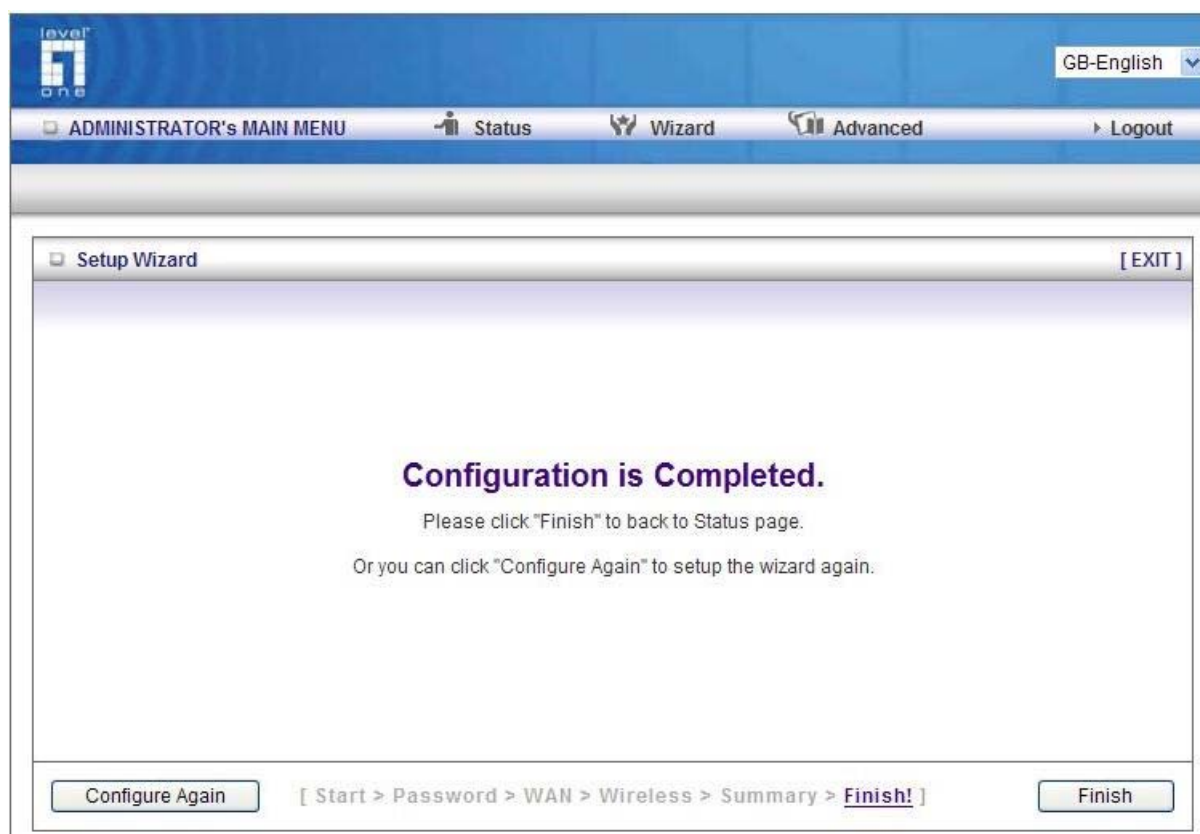
If you are an advanced user, you can access the configurations directly in the Advanced Setup



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

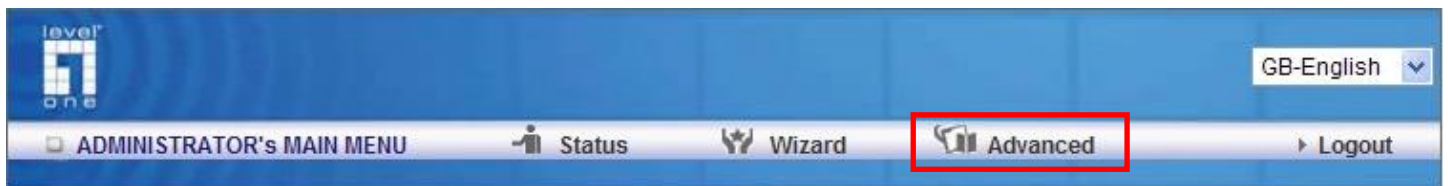


Once the user finishes those steps and the router screen displayed as below. It means that the Internet connection is now established.

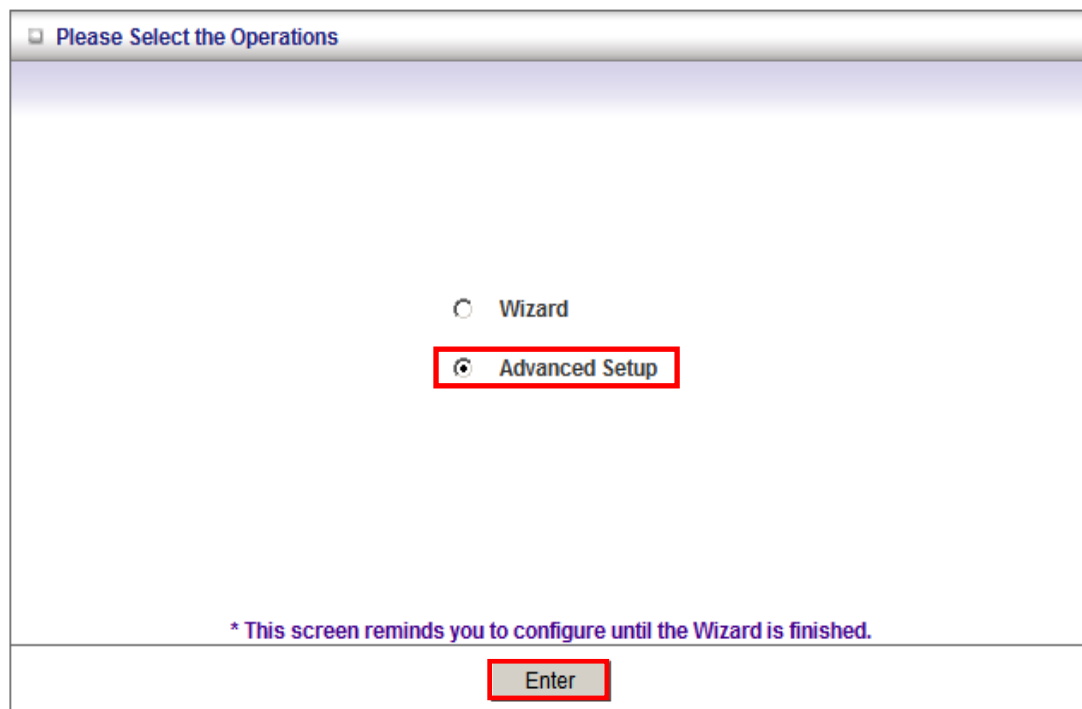


6. Advanced Setup

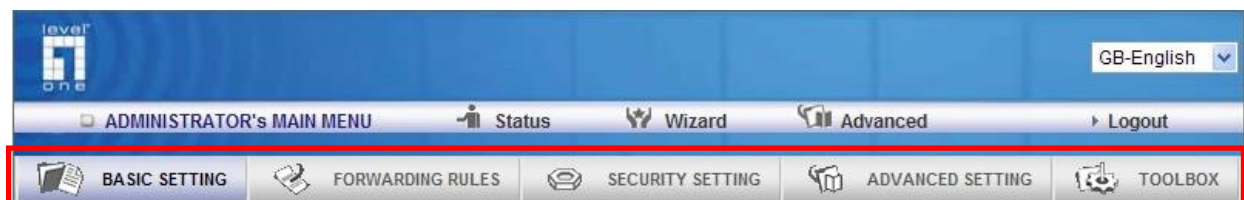
To access the Advanced Setup, click on **Advanced Setup** at the top of the page.



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 Level One administrator web interface. At the top, there is a blue header with the Level One logo on the left and a language dropdown menu set to 'GB-English' on the right. Below the header is a navigation bar with several tabs: '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 sidebar lists four menu items: 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. These items are highlighted with a red rectangular border. The main content area on the right is titled 'Basic Setting' and contains a bulleted list of the same four items, each with a brief description of its function.

level
ONE

GB-English

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Basic Setting

- **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.

Primary Setup

This page lets you change the LAN (Local Area Network) settings on your WBR-6003/ WBR-6006 150Mbps Wireless Router and WAN (Wide Area Network) connection.

Primary Setup [Help]	
Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.1.1"/>
▶ WAN Type	Dynamic IP Address Change...
▶ Host Name	<input type="text" value="WAB-6003"/> (optional)
▶ WAN's MAC Address	<input type="text" value="00-50-18-21-D6-9A"/> Clone MAC
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)
▶ IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Save Undo Virtual Computers...	

1. **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.
2. **WAN Type:** WAN connection type of your ISP. You can click the **Change** button to choose the most suitable one from the following options:

Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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.

Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

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.

Dynamic IP Address with Road Runner Session Management

1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.
2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!
3. Host Name: Optional. Required by some ISPs, e.g. @Home.
4. Renew IP Forever: This feature allows this product renew IP address automatically when the lease time is being expired even the system is in idle state.

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 Status-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

[Help]

DHCP clients

--- Select one ---

Copy to

 ID

--

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>

Save

Undo

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 *150Mbps Wireless Router*

DHCP Server [Help]	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Lease Time	<input type="text" value="0"/> Minutes
▶ IP Pool Starting Address	<input type="text" value="100"/>
▶ IP Pool Ending Address	<input type="text" value="199"/>
▶ Domain Name	<input type="text"/>
▶ Primary DNS	<input type="text" value="0.0.0.0"/>
▶ Secondary DNS	<input type="text" value="0.0.0.0"/>
▶ Primary WINS	<input type="text" value="0.0.0.0"/>
▶ Secondary WINS	<input type="text" value="0.0.0.0"/>
▶ Gateway	<input type="text" value="0.0.0.0"/> (optional)
<div>Save Undo Clients List... Fixed Mapping...</div>	

For more settings click on **More**.

DHCP Server: To either Disable or Enable DHCP Server.

Lease Time: DHCP lease time to the DHCP client

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

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. (see page 35)

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

Wireless Settings

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	None
<div>Save Undo Wireless Client List...</div>	

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

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 **LevelOne**. 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-6003/ WBR-6006 will broadcast beacons that contains SSID and other wireless information so that Computers or other wireless devices can find the WBR-6003/ WBR-6006 when scanning for wireless networks. Disable this function if you want to hide your wireless network.

WMM: Choose to Enable or Disable WMM (WiFi Multimedia) function. This function provides features that improves audio, video and voice applications over the wireless network.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. The default is AUTO which means the WBR-6003/ WBR-6006 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-6003/ WBR-6006 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-6003/ WBR-6006, 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-6003/ WBR-6006. Select the WEP Encryption (64bit or 128bit) and enter the WEP key. Please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	WEP
WEP	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
Key 1	<input checked="" type="radio"/> <input type="text"/>
Key 2	<input type="radio"/> <input type="text"/>
Key 3	<input type="radio"/> <input type="text"/>
Key 4	<input type="radio"/> <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Wireless Client List..."/>	

802.1X

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 [Help]	
Item	Setting
▶ Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	LevelOne
▶ Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	Auto
▶ WDS	Enter...
▶ WPS	Enter...
▶ Security	802.1x and RADIUS
▶ Encryption Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
▶ RADIUS Server IP	0.0.0.0
▶ RADIUS port	1812
▶ RADIUS Shared Key	
<div>Save Undo Wireless Client List...</div>	

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-PSK

This security is more secure compared to WEP. Select which type of encryption to use (either TKIP or AES) and then enter the key in the Passphrase field. The field needs to be between 8 and 63 characters long and can be any combination of letters and numbers if **ASCII** setting is used.

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	WPA-PSK
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Preshare Key Mode	ASCII
Preshare Key	
<div>Save Undo Wireless Client List...</div>	

WPA, WPA2(AES) WPA1/WPA2

Similar to 802.1X security but with TKIP or AES Encryption. You will need a RADIUS server for authentication. Please enter the details of your RADIUS server.

Wireless Setting [Help]	
Item	Setting
▶ Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	LevelOne
▶ Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	Auto
▶ WDS	Enter...
▶ WPS	Enter...
▶ Security	WPA1 / WPA2
▶ Encryption	TKIP + AES
▶ RADIUS Server IP	0.0.0.0
▶ RADIUS port	1812
▶ RADIUS Shared Key	
<div>Save Undo Wireless Client List...</div>	

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.

WPA-PSK, WPA2-PSK(AES), WPA / WPA2-PSK

This security is more secure compared to WEP. It will use either TKIP or AES for enhanced security. Please enter the key in the Passphrase field. The field can be between 8 and 63 characters long and can be any combination of letters and numbers under **ASCII** format.

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	WPA-PSK / WPA2-PSK
Encryption	TKIP + AES
Preshare Key Mode	ASCII
Preshare Key	
<div>Save Undo Wireless Client List...</div>	

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-6003/ WBR-6006 before initializing WPS functions.

Set PIN number of WBR-6003/ WBR-6006

Click the “Generate New PIN” button to randomly create a new PIN number for the WBR-6003/ WBR-6006.

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
▶ Setup	<input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station
▶ Current PIN of the device	19583815 <input type="button" value="Generate New PIN"/>
▶ WPS state	WPS is invalid!
▶ WPS status	Unconfigured

LevelOne WUA-0615

Profile Network Advanced Statistics WMM WPS Radio On/Off About

WPS AP List

ID	Model	MAC	Channel
ID : 0x0004	WBR-6003	00-11-68-53-94-E8	1
ID :	PMWBR-6001	00-11-68-2A-30-C6	7

WPS Profile List

Profile
WBR-6600

WPS Configuration

Pin Code: 13010775

Config Mode: Registrar

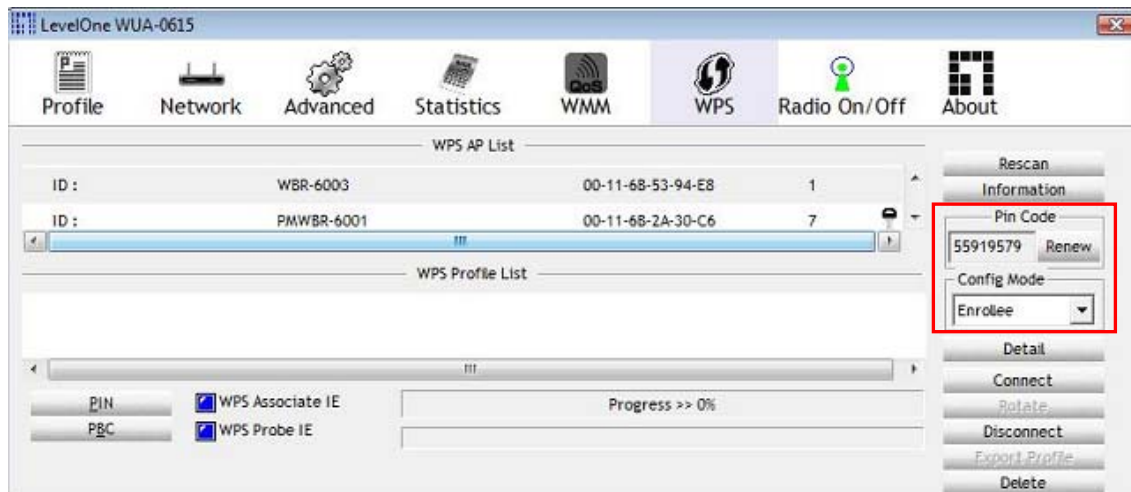
Detail

Connect Rotate Disconnect Export Profile

Progress >> 0%

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 the "Trigger" button to initiate WPS.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Setup	<input type="radio"/> Current AP PIN <input checked="" type="radio"/> Configure Wireless Station
▶ Method	<input checked="" type="radio"/> Enrollee PIN : 55919579 <input type="radio"/> Software button
▶ WPS state	WPS is invalid!
▶ WPS status	Unconfigured
<div>Save Trigger Back</div>	

Push Button Method

Select the “Software Button” mode and click the “Trigger” button.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Setup	<input type="radio"/> Current AP PIN <input checked="" type="radio"/> Configure Wireless Station
▶ Method	<input type="radio"/> Enrollee PIN : 00000000 <input checked="" type="radio"/> Software button
▶ WPS state	WPS is invalid!
▶ WPS status	Unconfigured
<div>Save Trigger Back</div>	

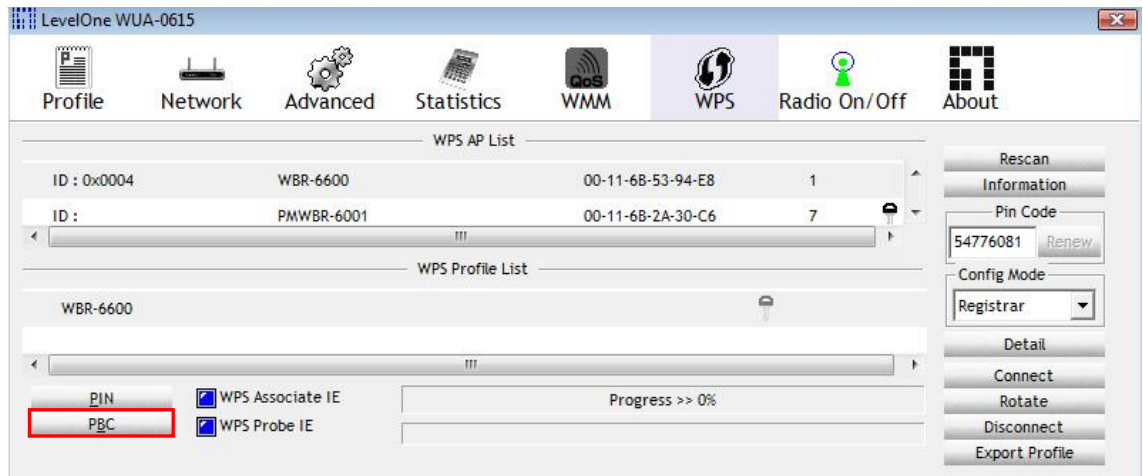
An alternative is to press the WPS button at the front of the router until the WLAN light starts flashing. This indicates that WPS is activated.



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-6003/ WBR-6006. Also note that the standard only supports WEP encryption.

Select the AP Mode that most suites your desired application.

AP Only:

WDS is disabled. WBR-6003/ WBR-6006 functions as normal Access Point mode

WDS - Bridge:

Create a WDS Bridge between multiple Access Points, and bridge to only wired connections. In this mode, the WBR-6003/ WBR-6006 will not provide service to any wireless clients.

WDS - Bridge + AP:

A combination of the AP and Bridge modes can create a WDS Bridge between multiple Access Points, and also accept wireless and wired clients.

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.

WDS Setting

[Help]

Item	Setting	
▶ AP Mode:	WDS - Bridge	
▶ Remote AP MAC MAC 1		
MAC 2		
MAC 3		
MAC 4		
Scanned AP's MAC <div> <div>-- Select one --</div> <div>Copy to</div> </div> Remote AP MAC <div> <div>--</div> </div>		
SSID	Channel	MAC Address
AMG-2000TSD	1	00-11-6B-39-A9-73
wap-0005tsd	1	00-03-7F-FE-00-02
wan-1112	1	00-19-5B-43-29-8E
WBR-6001TSD	6	00-11-6B-29-30-84
WAP-0003	6	00-11-6B-60-6A-C5
8FB1	6	00-09-7C-F1-F3-1B
MeetingRoom	7	00-11-6B-B0-87-9C
QC-6000	11	00-11-6B-17-48-F6
<div> <div>Save</div> <div>Undo</div> <div>Scan AP</div> <div>Back</div> </div>		

Change Password

This page allows you to change the WBR-6003/ WBR-6006 Web Configuration password. Please type in the old password (factory default password is **admin**) and then type in the new password.

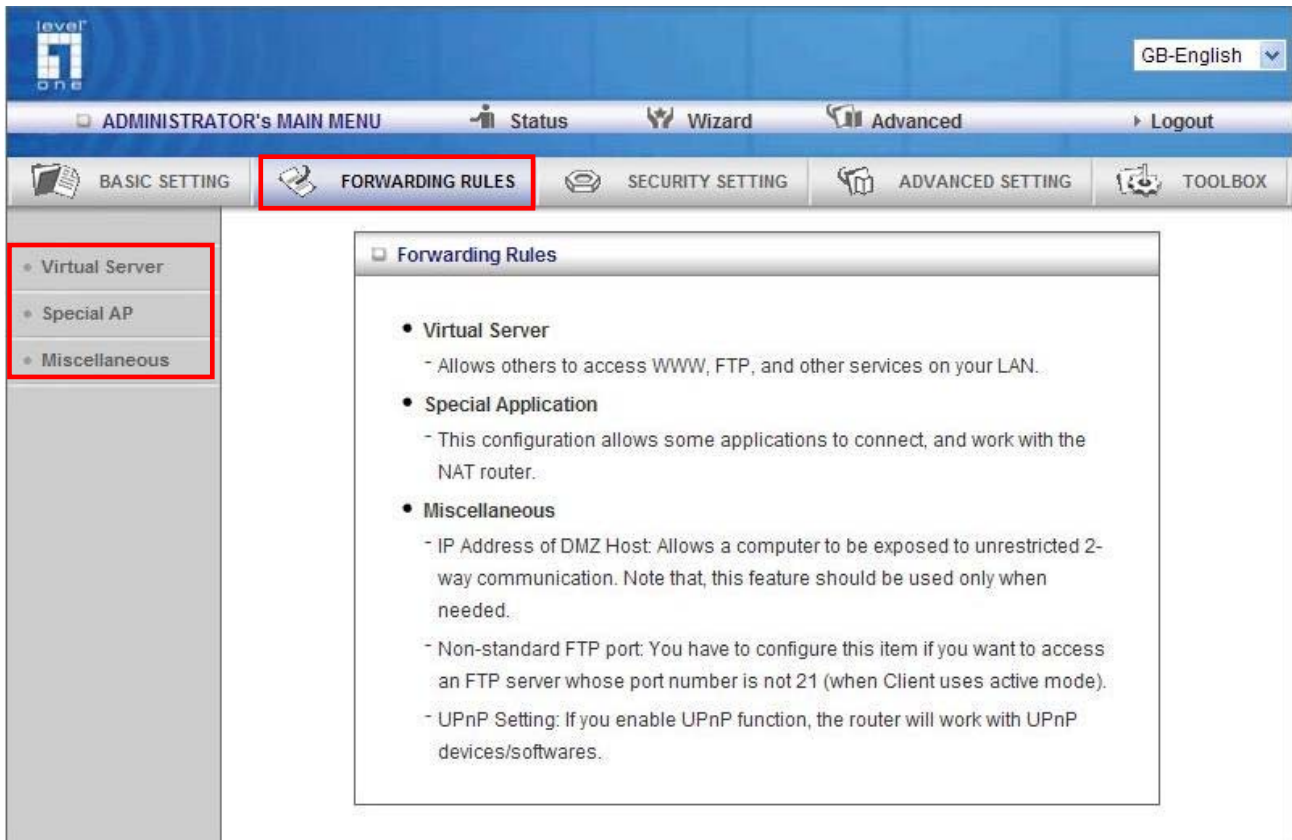
Change Password	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

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-6003/ WBR-6006. 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 --

Schedule rule (00)Always
Copy to ID --

ID	Server IP	Public Port	Private Port	Protocol	Enable	Schedule Rule#
1	192.168.1.			Both	<input type="checkbox"/>	0
2	192.168.1.			Both	<input type="checkbox"/>	0
3	192.168.1.			Both	<input type="checkbox"/>	0
4	192.168.1.			Both	<input type="checkbox"/>	0
5	192.168.1.			Both	<input type="checkbox"/>	0
6	192.168.1.			Both	<input type="checkbox"/>	0
7	192.168.1.			Both	<input type="checkbox"/>	0
8	192.168.1.			Both	<input type="checkbox"/>	0
9	192.168.1.			Both	<input type="checkbox"/>	0
10	192.168.1.			Both	<input type="checkbox"/>	0

Next >>
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 192.168.1.2, a Web server (port 80) at 192.168.1.3, and a VPN server at 192.168.1.6, 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	192.168.1.2	V
80	80	192.168.1.3	V
1721	1723	192.168.1.6	V

Special AP

Special Applications

[Help]

Popular applications

--- Select one ---

Copy to

 ID

--

ID	Trigger	Incoming Ports	Enable
1	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
2	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
3	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
4	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
5	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
6	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
7	<div>65535</div>	<div>0</div>	<input type="checkbox"/>
8	<div>65535</div>	<div>0</div>	<input type="checkbox"/>

Save

Undo

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-6003/ WBR-6006. 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-6003/ WBR-6006 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	192.168.1. <input type="text"/>	<input type="checkbox"/>
▶ Non-standard FTP port	<input type="text"/>	
▶ UPnP setting		<input checked="" type="checkbox"/>
▶ Xbox Support		<input checked="" type="checkbox"/>
▶ VPN PPTP Pass-Through		<input checked="" type="checkbox"/>
▶ VPN IPSec Pass-Through		<input checked="" type="checkbox"/>
<div>Save Undo</div>		

IP Address of DMZ Host

Here you can set the DMZ (Demilitarized Zone) Host. It is a computer that does not have the WBR-6003'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.

Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

UPnP Setting

The WBR-6003/ WBR-6006 supports Universal Plug and Play. However this depends on your operating system.

Xbox Support

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

VPN PPTP Pass-Through

The WBR-6003/ WBR-6006 supports PPTP pass through on VPN connection.

VPN IPSec Pass-Through

The WBR-6003/ WBR-6006 supports VPN IPSec pass through on VPN connection.

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's Main Menu. The top navigation bar includes the Level One logo, a language dropdown set to 'GB-English', and links for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu highlights 'SECURITY SETTING' in red, alongside 'BASIC SETTING', 'FORWARDING RULES', 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, a vertical menu lists 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous', all of which are enclosed in a red rectangular box. The main content area, titled 'Security Setting', contains a list of security features: Packet Filters, Domain Filters, URL Blocking, MAC Address Control, and Miscellaneous. Each feature is accompanied by a brief description of its function.

Security Setting

- **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-6003/ WBR-6006. 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.

Outbound Packet Filter

[Help]

Item	Setting			
▶ Outbound 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.				
Schedule rule (00)Always Copy to ID --				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> 0

Save

Undo

Inbound Filter...

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 (192.168.1.1) or a range of IP addresses (192.168.1.100 – 192.168.1.200). 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 [Help]				
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.				
Virtual Server Rule – IP address : Port (Service) – Schedule rule (00)Always Copy to ID --				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
<div> Save Undo Outbound Filter... MAC Level... </div>				

Domain Filter

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

Domain Filter		[Help]	
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="100"/> To <input type="text" value="199"/>		
▶ Schedule Rule#	<input type="text" value="(00)Always"/> <input checked="" type="radio"/> Enable <input type="radio"/> Disable		
ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input 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"/>
6	<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.
- **Schedule Rule:** You can set your Domain Filter by schedule.
- **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-6003/ WBR-6006 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.100~ X.X.X.199 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	
▶ Schedule Rule#	(00)Always <input type="radio"/> Enable <input type="radio"/> Disable	
ID	URL	Enable
1	<input type="text" value="msn"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="sina"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="cnnsi"/>	<input 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"/>

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

You can set your URL Blocking by schedule.

To enable **Schedule Rule**, 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 [Help]				
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. Note: Association control has no effect on wired clients.		
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="00-12-34-56-78-90"/>	192.168.1. <input type="text" value="100"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="text" value="00-12-34-56-78-92"/>	192.168.1. <input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="text" value="00-98-76-54-32-10"/>	192.168.1. <input type="text" value="101"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" << Previous"/> <input type="button" value=" Next >>"/> <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 control method 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-6003/ WBR-6006. If a client is denied, then it means the client cannot send or receive any data via this WBR-6003/ WBR-6006. 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.

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

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 switch 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 - "00-12-34-56-78-90" --> 192.168.12.100

ID 3 - "00-98-76-54-32-10" --> 192.168.12.101

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 1 tries to use an IP address different from the address listed in the Control Table (192.168.12.100), it will be denied to connect to the WBR-6003/ WBR-6006.

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
▶ Remote Administrator Host / Port	0.0.0.0 / 8080	<input type="checkbox"/>
▶ Administrator Time-out	600 seconds (0 to disable)	
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ SPI mode		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>
▶ VPN PPTP Pass-Through		<input checked="" type="checkbox"/>
▶ VPN IPSec Pass-Through		<input checked="" type="checkbox"/>
<div>Save Undo</div>		

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 0.0.0.0, 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 "/nn" 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 8080. You can change web server port to other port.

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.

Discard PING from WAN side: When enabled, any host on the internet cannot ping this device's from WAN side.

SPI Mode: When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

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.

VPN PPTP Pass-Through: If enabled, the PPTP packet can pass through on VPN connection.

VPN IPSec Pass-Through: If enabled, the IPSec packet can pass through on VPN connection.

Advanced Settings

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

The screenshot displays the Javel One Administrator's Main Menu. The top navigation bar includes links for ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. Below this, a secondary menu highlights BASIC SETTING, FORWARDING RULES, SECURITY SETTING, and ADVANCED SETTING (which is selected and highlighted with a red box). On the left side, a sidebar lists various settings: System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule, all of which are also highlighted with a red box. The main content area, titled 'Advanced Setting', provides detailed descriptions for each of these settings:

- System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- 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).
- 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.
- Schedule Rule**
 - Apply schedule rules to Packet Filters and Virtual Server.

System Time

This page allows you to set the time settings of the WBR-6003/ WBR-6006.

System Time [Help]	
Item	Setting
System Time	Saturday, 1 November 2008 4:47:43 AM
<input type="radio"/> Get Date and Time by NTP Protocol <input type="button" value="Sync Now !"/>	
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
<input type="radio"/> Set Date and Time using PC's Date and Time	
PC Date and Time	Friday, 23 January 2009 2:46:41 PM
<input checked="" type="radio"/> Set Date and Time manually	
Date	Year: 2008 Month: Nov Day: 01
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)
<input type="radio"/> Daylight Saving <input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Start	Month: Jan Day: 01 Hour: 00
End	Month: Jan Day: 01 Hour: 00
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

There are three ways to set up the System Time of the WBR-6003/ WBR-6006.

1. **Get Date and Time by NTP Protocol:** Selected if you want to get the Date and Time from an NTP server. A Time Server and time zone is required. Once entered, click **Sync Now** to sync the time with the Time Server.
2. **Set Date and Time using PC's Date and Time:** Set the Date and Time using the settings from your computer.
3. **Set Date and Time manually:** Selected if you want to Set Date and Time manually.

If required, set the Daylight Saving settings by selecting Enable and define the Start and End dates for daylight savings periods.

System Log

The WBR-6003/ WBR-6006 supports both Syslog (using UDP packets) and E-Mail alert.

System Log		[Help]
Item	Setting	Enable
▶ IP Address for Syslog	192.168.1. <input type="text"/>	<input type="checkbox"/>
▶ IP Address of Outgoing Mail Server	<input type="button" value="Send Mail Now"/>	<input type="checkbox"/>
• SMTP Server IP/Port	<input type="text"/>	
• E-mail address	<input type="text"/>	
• E-mail Subject	<input type="text"/>	
• User name	<input type="text"/>	
• Password	<input type="text"/>	
▶ Log Type	<input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice	
<input type="button" value="View Log..."/> <input type="button" value="Save"/> <input type="button" value="Undo"/>		

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.
- **Sent E-Mail Alert to:** 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)
- **User Name / Password:** Username and Password if your SMTP server requires log in.

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-6003/ WBR-6006, 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 [HELP]	
Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼ Provider website
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>
Save 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.

SNMP Setting

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

SNMP Setting [Help]	
Item	Setting
▶ Enable SNMP	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text" value="public"/>
▶ Set Community	<input type="text" value="private"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2c
<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 public. This will act as a password.
- **Set Community:** Set the community of private. 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-6003/ WBR-6006, 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 [HELP]					
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"/>
<div>Save Undo</div>					

There are two types of routing supported by the WBR-6003/ WBR-6006.

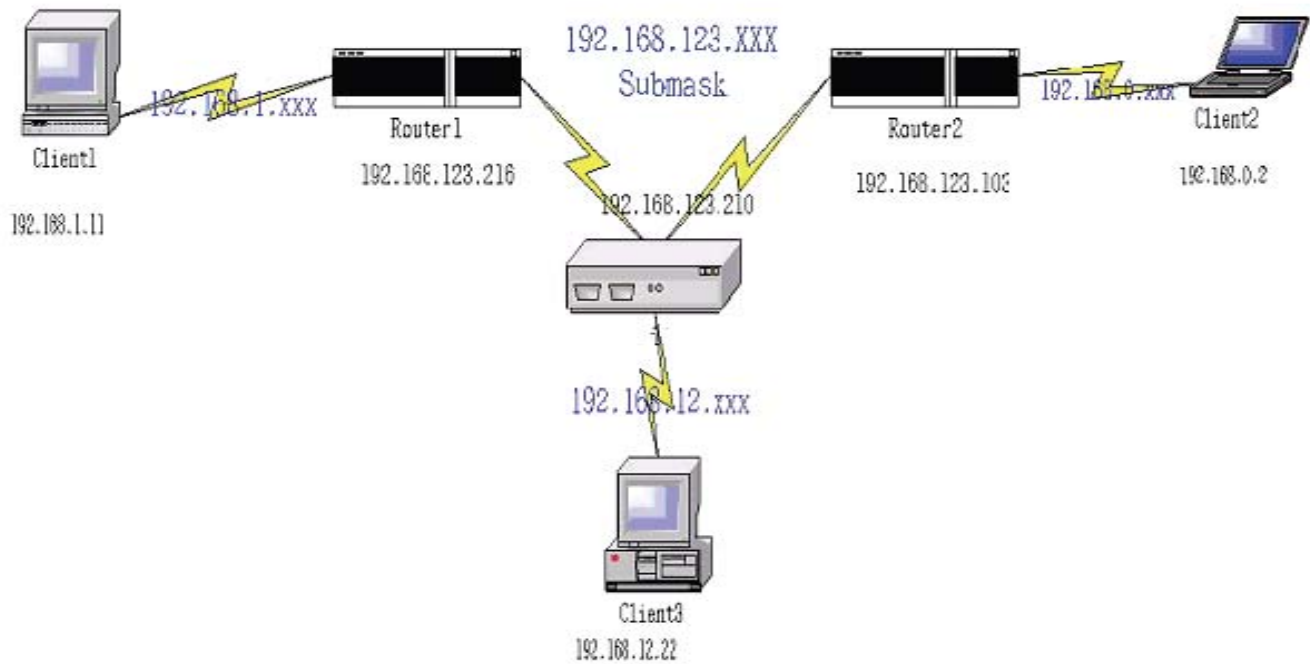
- **Dynamic Routing:** This method uses Routing Information Protocol (RIP) to enable the devices to determine the best route for each packet based on the number of hops between the source and destination.

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-6003/ WBR-6006 to communicate with computers on other LAN segments which are connected to the WBR-6003/ WBR-6006 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.

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 type="checkbox"/> Enable	
Rule#	Rule Name	Action
<div>Save Add New Rule...</div>		

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

Schedule Rule Setting [Help]		
Item	Setting	
▶ Name of Rule 1	<input type="text"/>	
▶ System Time	Saturday, 1 November 2008 12:32:53 AM	
Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
<div>Save Undo Back</div>		

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

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, Packet Filters, and Domain Filters by entering the rule number in the "Schedule Rule#" fields.

Toolbox

This section has some basic tools to maintain the WBR-6003/ WBR-6006's systems.

The screenshot displays the LevelOne administrator web interface. At the top, there is a blue header with the LevelOne logo on the left and a language dropdown menu set to 'GB-English' on the right. Below the header is a navigation bar with several tabs: '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'. The 'TOOLBOX' tab is highlighted with a red border. On the left side of the main content area, there is a vertical sidebar with a list of options: 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. This sidebar is also highlighted with a red border. The main content area features a 'Toolbox' panel with a title bar and a list of tools, each with a brief description:

- **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.

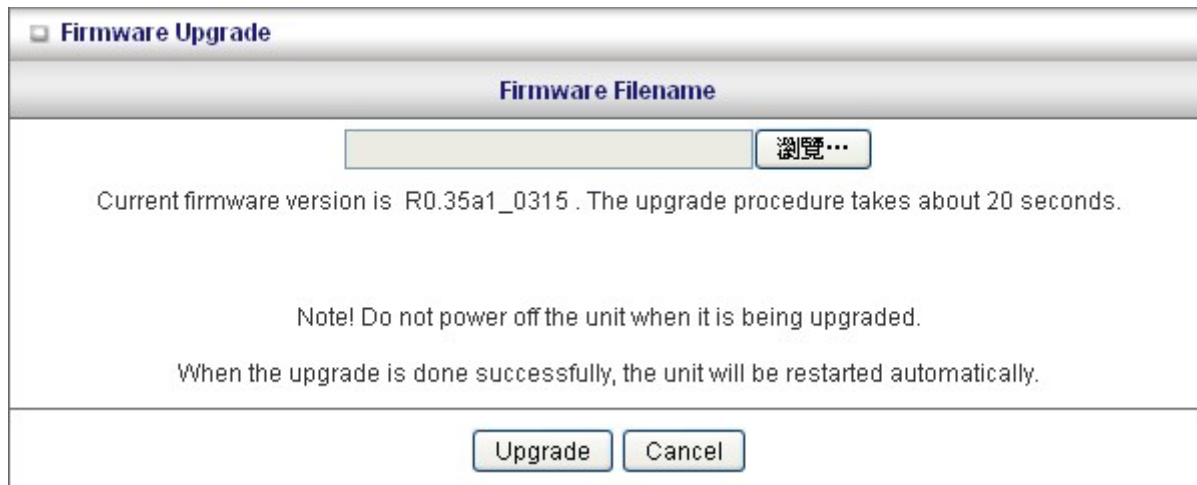
View Log

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

System Log	
Item	Info
WAN Type:	Dynamic IP Address (R0.03b1)
Display time	Sat Nov 01 00:43:33 2008
Time	Log
Saturday, 1 November 2008 12:01:32 AM	Associated: 00-1F-1F-1F-6E-D4 st=0
Saturday, 1 November 2008 12:01:41 AM	DOD:triggered internally
Saturday, 1 November 2008 12:01:41 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:01:51 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:02:05 AM	Admin from 192.168.0.101 login successfully
Saturday, 1 November 2008 12:02:11 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:02:51 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:04:13 AM	DOD:triggered internally
Saturday, 1 November 2008 12:04:13 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:04:23 AM	DHCP:discover(My Host)

Firmware Upgrade

This page allows you to perform updates to the firmware of the WBR-6003/ WBR-6006.



The image shows a web-based dialog box titled "Firmware Upgrade". It has a header bar with the title. Below the header is a section labeled "Firmware Filename" containing a text input field and a "瀏覽..." (Browse...) button. The main body of the dialog contains the text: "Current firmware version is R0.35a1_0315 . 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." At the bottom of the dialog 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-6003/ WBR-6006 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.

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 reboot the device to make the settings effect.

Reboot

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

Miscellaneous Items

Miscellaneous Items [Help]	
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"/>
▶ VPN PPTP Pass-Through	<input checked="" type="checkbox"/>
▶ VPN IPSec Pass-Through	<input checked="" type="checkbox"/>
<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.

VPN PPTP Pass-Through:

If enabled, the PPTP packet can pass through on VPN connection.

VPN IPSec Pass-Through:

If enabled, the IPSec packet can pass through on VPN connection

Appendix A 802.1x Setting

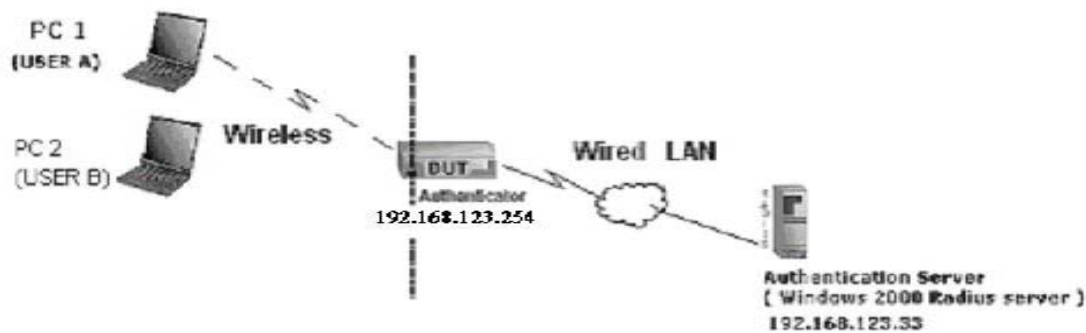


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

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.

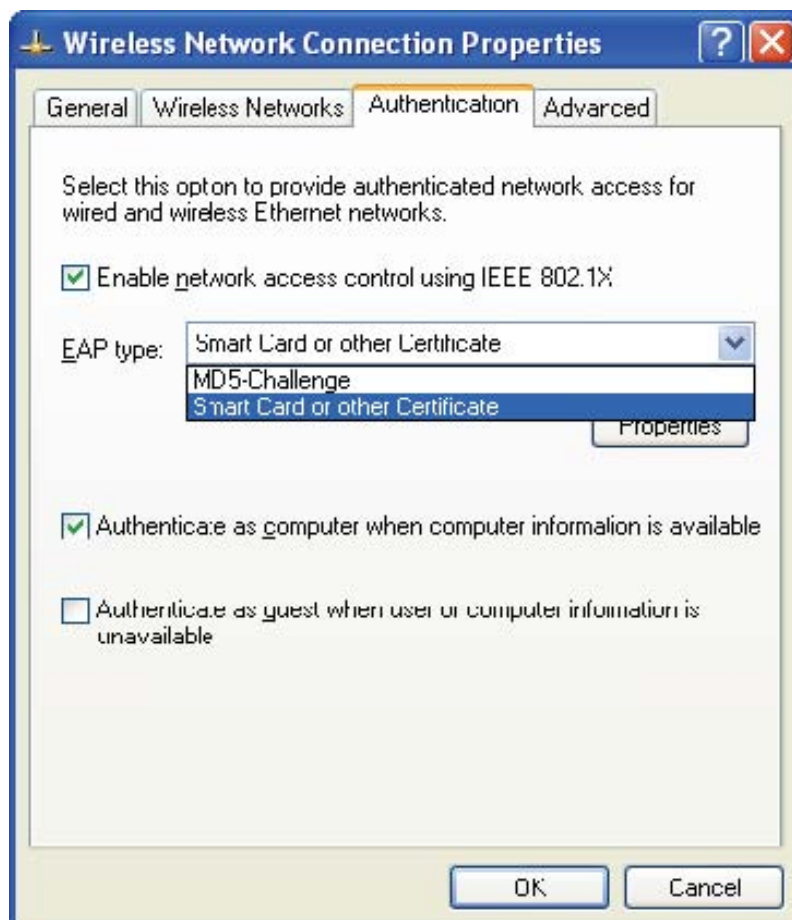


Figure 2: Enable IEEE 802.1X access control / Smart card or certificate properties

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.

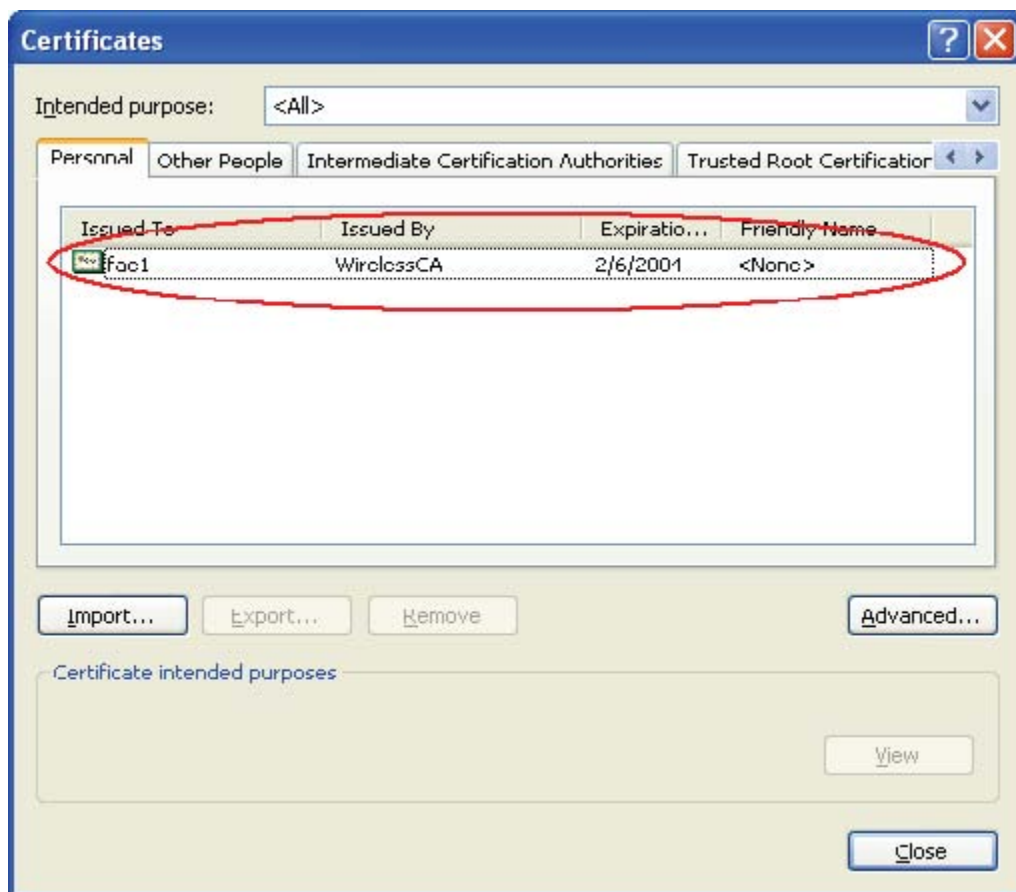


Figure 4: Certificate information on PC1

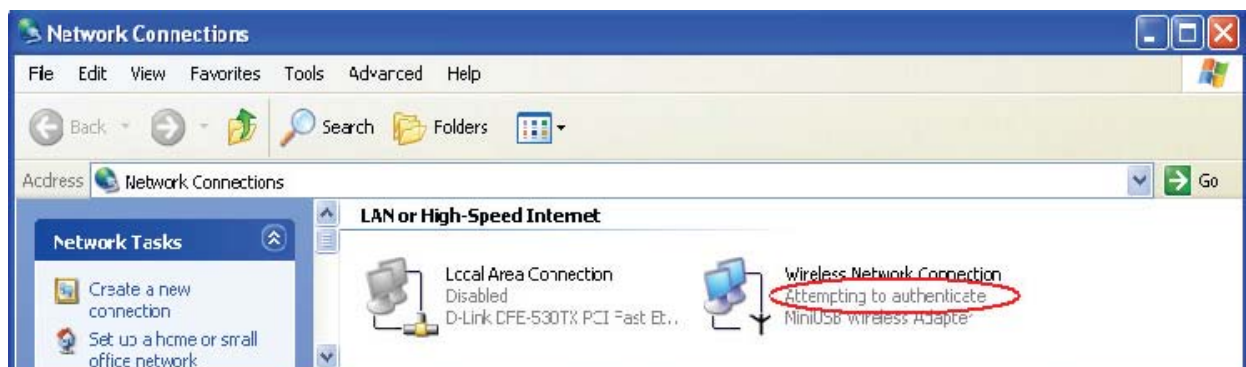


Figure 5: Authenticating

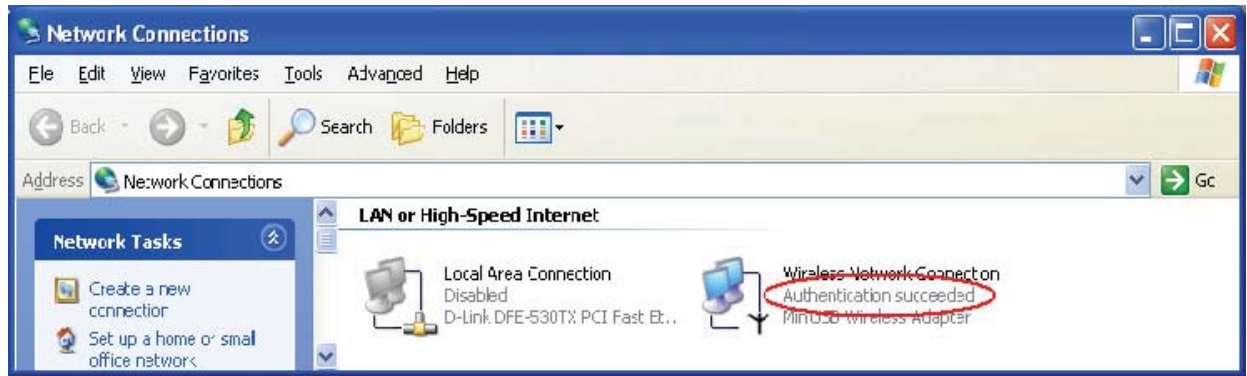


Figure 6: Authentication success

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.

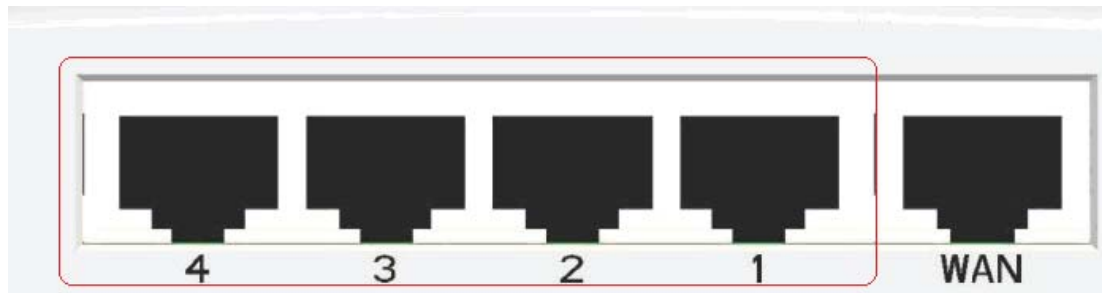
Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.

Appendix B FAQ and Troubleshooting

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

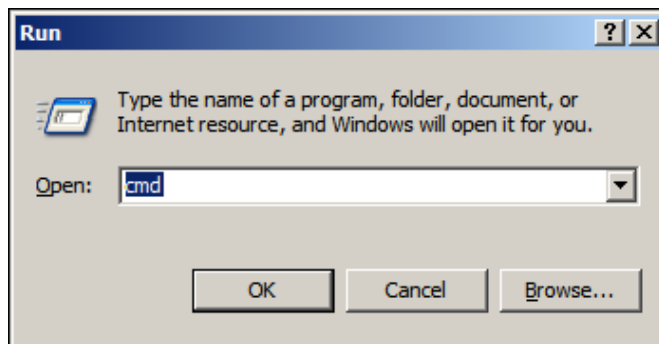
1. Why can't I configure the router even if the cable is plugged in the ports of Router and the LED is also lit?

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. . . . . : 192.168.1.123  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

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: You can Restore the device with RESET button (You can find it on the back of the device). Please make sure the router is power on and ready to use. Use a sharp objects like paper clip to press the reset button, keep the buttons pressed until 8 seconds, and then remove your clip. If the Status LED flashes about 5 times, 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.

Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.

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?

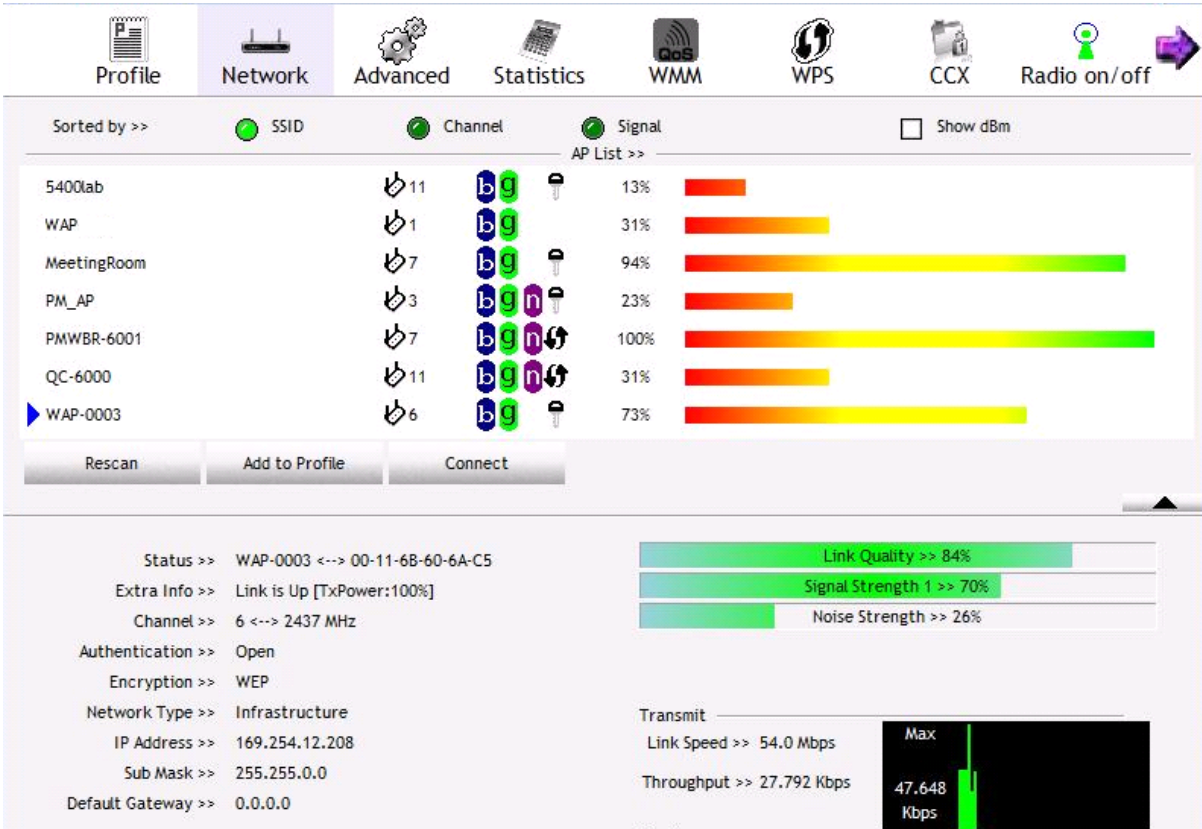
A: First, make sure that you already installed wireless client device in your computer. Then check the configuration of wireless router. The default is below:

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	None
<div>Save Undo Wireless Client List...</div>	

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:

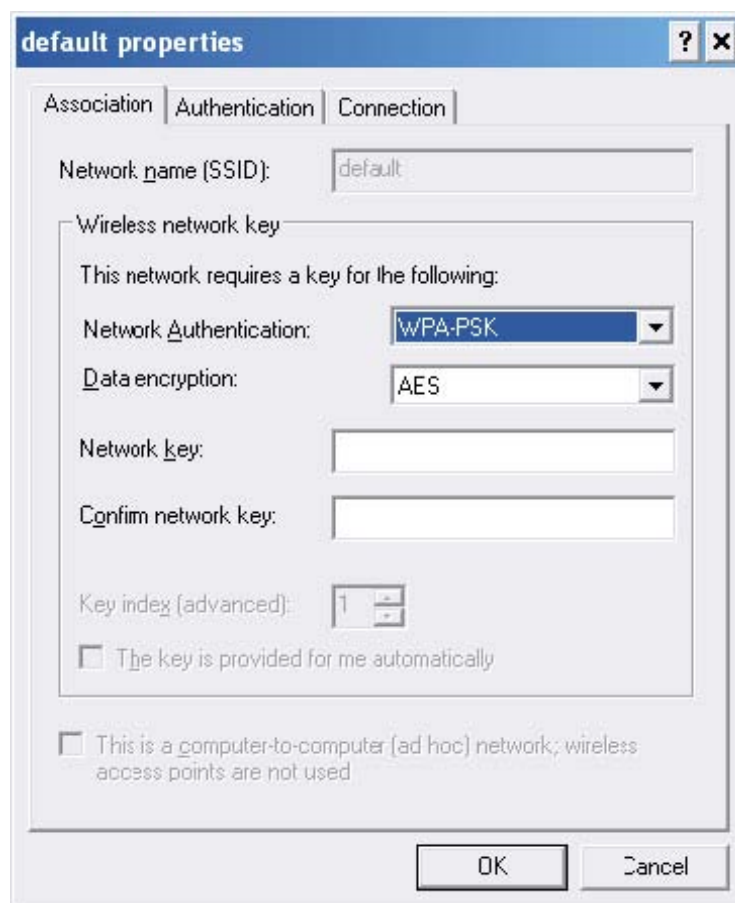
```
Connection-specific DNS Suffix . : 
IP Address. . . . . : 192.168.1.123
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

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

General	
Model	<i>WBR-6003/ WBR-6006 150Mbps Wireless Router</i>
Data Transfer Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps
Transmit Power	802.11b: 21.50dBm 802.11g: 26.58dBm
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	64/128-bits WEP Encryption, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.1x
Diagnostic LED	Status WAN WLAN LAN LEDs
Antenna	Dipole fix antenna
Physical and Environmental	
Operating Systems Supported	Windows 2000, Windows XP, Windows Vista, Windows 7, Linux, MAC OSX
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	10% ~ 95% RH, no condensation
Dimensions	156mm (L) x 110mm(W) x 22mm (D)
Certifications	FCC, CE