



LevelOne

User Manual

WBR-3800
MobilSpot™ Portable Wireless Hotspot

V1.0 – 0805

FCC 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WBR-3800) 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 Contents

Package Contents	1
System Requirements	1
Chapter 1 - Introduction	2
Front LED Indicators	3
Back Panel Ports	4
Features	5
Chapter 2 - Installation.....	6
Chapter 3 - The Configuration Menu	9
Chapter 4 - Advanced Setup	15
Basic Setting	16
Basic Settings > Primary Setup.....	17
Basic Setting > DHCP Setup.....	19
Basic Setting > Wireless	20
Basic Setting > Change Password.....	24
Forwarding Rules	25
Forwarding Rules > Virtual Server	26
Forwarding Rules > Special AP	27
Forwarding Rules > Miscellaneous	28
Security Setting	29
Security Setting > Packet Filters	30
Inbound Filter:	31
Security Setting > Domain Filters	32
Security Setting > URL Blocking	33
Security Setting > MAC Control	34
Security Setting > Miscellaneous	35
Advanced Setting	36
Advanced Setting > System Log	37
Advanced Setting > Dynamic DNS	38
Advanced Setting > SNMP.....	39
Advanced Setting > Routing.....	40
Advanced Setting > System Time	42
Advanced Setting > Scheduling	43
Advanced Setting > Performance	44

Tool Box	45
Tool Box > System Info	46
Tool Box > Firmware Upgrade	47
Tool Box > Backup Setting.....	47
Tool Box > Reset to Default	47
Tool Box > Reboot	47
Tool Box > Miscellaneous	48
Troubleshooting	49
Technical Specifications	53
3G/3.5G Modem Compatibility List	54

Default Settings

IP Address	192.168.0.1
Password	password
Wireless Mode	Enable
SSID	WBR-3800
Security	None

Package Contents

Important: Check your product package contents FIRST.

The Level One WBR-3800 MobilSpot™ package should contain the items listed below. If any of the items are missing, please contact your reseller immediately.

1. Level One WBR-3800 MobilSpot™ Portable Wireless Hotspot
2. 1x Antenna
3. Rubber Pad and Sponge
4. Power Adapter 5V 3.0A
5. RJ-45 Cable
6. Quick Installation Guide
7. User Manual on CD
8. Cradle Stand

Caution: Using a power supply with a different voltage rating than the one included with the LevelOne WBR-3800 will cause damage and void the warranty for this product.

System Requirements

- A compatible either 16bit or 32bit PCMCIA or USB 3G modem card with service for 3G Broadband access.
Note: Subject to services and service terms available from your carrier.
- Computers with Windows, Macintosh, or Linux based operating systems with an installed Ethernet adapter.
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.
- For Wireless Networking, a computer with working 802.11b, or 802.11g wireless adapter.

Chapter 1 - Introduction

The LevelOne WBR-3800 MobilSpot™ Portable Wireless Hotspot is a high performance tool that supports wireless networking at home, work, or public place usage. The MobilSpot™ uses either a 16bit or 32bit PC card or USB 3G/3.5G modem adapter, for either WCDMA, EDGE or EVDO and even HSDPA 3G Broadband services to connect and distribute the Internet to multiple computers. It also has a WAN port to connect the WBR-3800 to an ADSL/Cable modem or existing gateway router.

Included is also a Wireless Access Point that supports wireless data transfers up to 54 Mbps. The LevelOne WBR-3800 is compatible with industry security features such as WEP, WPA and WPA2 to eliminated exposure to unwanted access.

The LevelOne WBR-3800 MobilSpot™ also comes equipped with solid firewall features to defend against hackers which is even active when VPN is being used. Port Forwarding and UPnP functions make is much simpler to configure and setup a series of port rules required by many online games, P2P file sharing and server applications.

Front LED Indicators



Label	Status	Indicators
3G	Flashing	Flashes when unit is ready
	Off	Power is Off
LAN	Flashing	Flashes when data is being transferred
	On	Indicates link is active
	Off	Indicates no active link
WAN	Flashing	Flashes when data is being transferred
	On	Indicates WAN link is active
	Off	Indicates no WAN link
WLAN	Flashing	Indicates Wireless is enabled
	Off	Indicates Wireless is disabled

Back Panel Ports



Antenna	To connect the supplied antenna
WAN	10/100 RJ-45 Ethernet Port to connect to a modem or router
LAN	10/100 RJ-45 to connect to Ethernet network card or Hub/Switch
Reset	To reset the WBR-3800 to factory default settings (All your customized settings will be lost)
Power	Connect to the included Power Adapter

Features

- Automatic take over back up with 3G connection as ADSL/Cable WAN failover.
- Implementation within 3 minutes allows the network to go where wires cannot go, even outside the home or office.
- Fully compatible with the 802.11g standard to provide a wireless data transfer rate of up to 54Mbps.
- Backwards compatible with the 802.11b standard to provide a wireless data rate of up to 11Mbps.
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing).
- User friendly configuration and diagnostic utilities.
- Operates in the 2.4GHz frequency range.
- Advanced Firewall features.
- Supports NAT with VPN pass-through, providing added security.
- MAC Filtering
- IP Filtering
- Port Scheduling
- DHCP server enables all networked computers to automatically receive IP addresses.
- Web-based interface for Managing and Configuring.
- Access Control to manage users on the network.
- Supports special applications that require multiple connections.
- Equipped with 2x 10/100 Ethernet ports for LAN and WAN access, and a Type II PC card (for both 16Bit and 32Bit) Slot and USB port for 3G network connection.
- Connects multiple computers to a Broadband either WCDMA or EVDO even HSDPA modem to share the Internet connection.

Note: The WBR-3800 MobilSpot™ is designed to work with either EVDO, EDGE or WCDMA (UMTS) even up to HSDPA 3G Modem Adapters.

Please refer to your service provider for detailed feature information.

Chapter 2 - Installation

Note: DO NOT connect the LevelOne WBR-3800 MobilSpot™ to power before performing the installation steps below.

Step 1:

Attach the antenna



1. Remove the antenna from its plastic wrapper.
2. Screw the antenna in a clockwise direction to the back panel of the unit.
3. Once secured, position the antenna upward at its connecting joint.
This will ensure optimal reception.

Step 2:

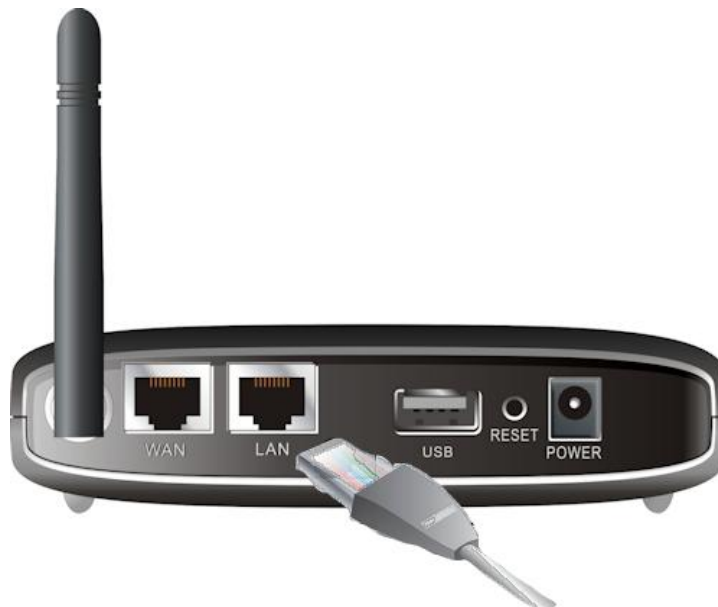
Insert your wireless 3G PC card (either 16bit or 32bit) into the WAN PCMCIA Card Slot or plug your 3G USB modem into the USB interface.



Note: The WBR-3800 MobilSpot™ is designed to work with either UMTS, EDGE or EVDO and even HSDPA 3G modem. Please refer to your service provider for detailed feature information.

Step 3:

Insert the Ethernet cable into LAN Port on the back panel of the WBR-3800 MobilSpot™ and an available Ethernet port on the computer you will use to configure the unit.



Note: The WBR-3800 MobilSpot™ LAN Port is “AutoMDI/MDIX.” This provides Ethernet cable LAN Port access.

Step 4:

1. Connect the power adapter to the receptor on the back panel of your WBR-3800 MobilSpot™.
2. Then plug the other end of the power adapter into a wall outlet or power strip



- The 3G LED will turn ON to indicate power has been applied.
- Other LEDs will flash ON and OFF as the WBR-3800 MobilSpot™ performs initialization and Internet connection processes. This will take a few minutes.
- When complete, the following LEDs will illuminate green:
3G, WAN, LAN, and WLAN.

Chapter 3 - The Configuration Menu

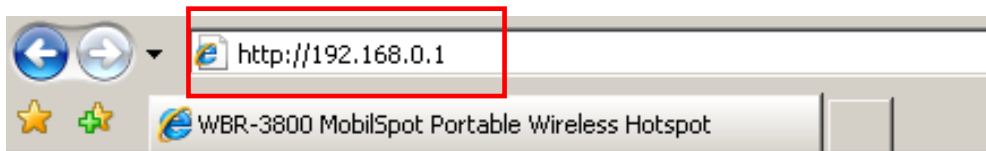
Once properly configured, the WBR-3800 MobilSpot™ will obtain and assign IP address information automatically. Configuration settings can be established through the Web-Based Configuration Menu.

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

Note:

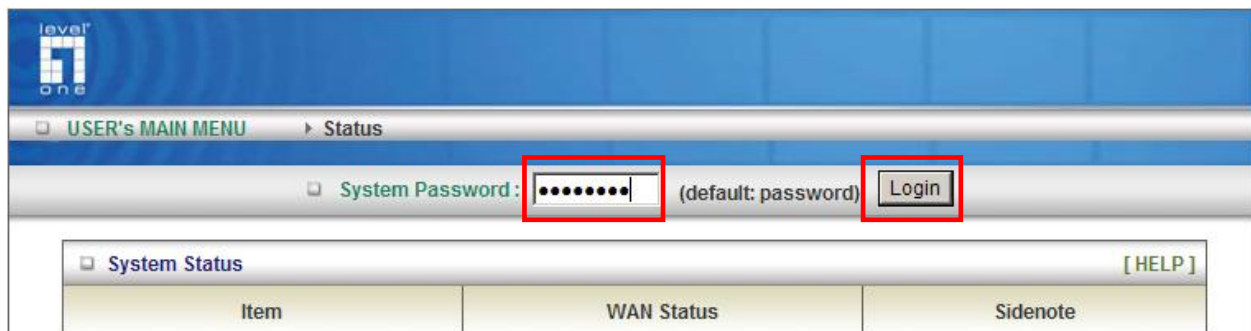
Browser will automatically add port 2005 on the IP Address (eg: http://192.168.0.1:2005)

If you have changed the default IP Address assigned to the WBR-3800, ensure you enter the correct IP Address.



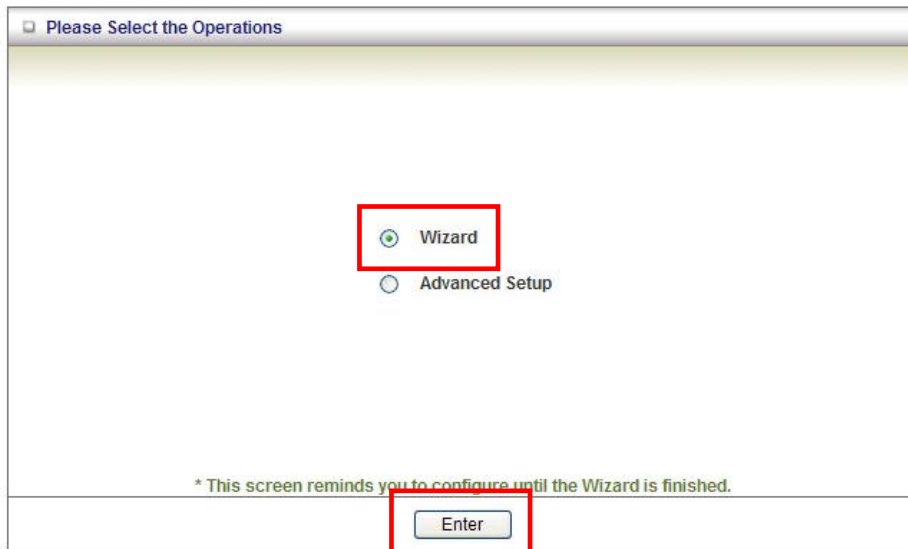
2. Type in “password” (without quotes) in the Password box, Then click Login

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

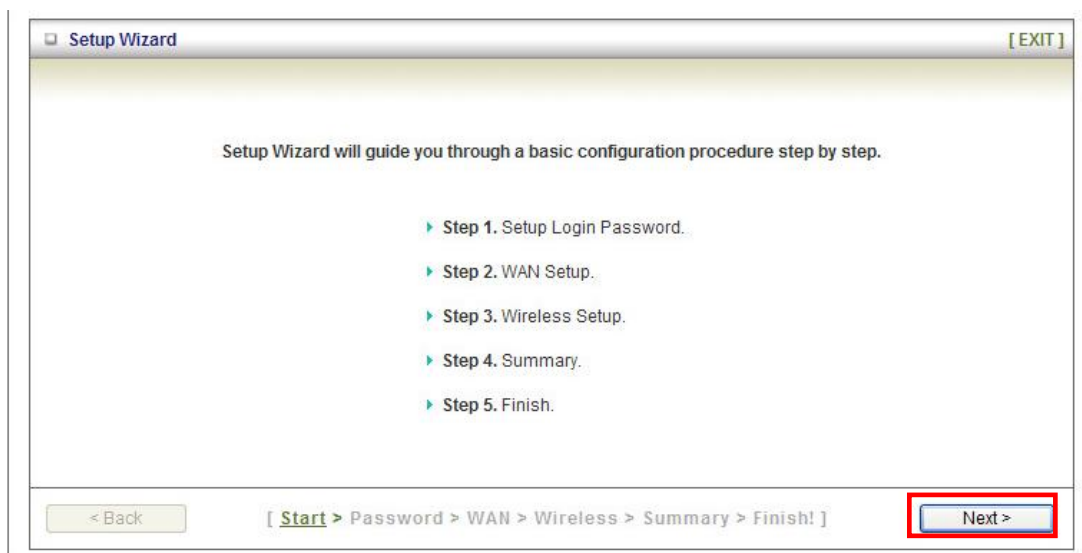


3. Click on **Wizard**, then click **Enter** to start the Setup Wizard.

Or you may click on “**Advanced Setup**” for advanced settings, Please check Chapter 4.



4. The Wizard steps help you to configure the MobilSpot™ in 5 easy steps. Press **Next** button to start configuration.



5. This page allows you to change the MobilSpot's web configuration login password. To change password, enter the old password (default is "password"), then enter new password. Type the new password again in the **Reconfirm** field, then click **Next**.

Or, you can just click **Next** to keep the default password.

It is recommended that you change the system password from the default for extra security.

6. Select the type of WAN connection you want to use, then click **Next**.

Note: Please use the login details supplied by your broadband ISP or 3G Provider.

7. You may change the LAN IP Address of the MobilSpot™ if needed. The LAN IP Address is private to your internal network and cannot be seen on the Internet

Setup Wizard - WAN Settings - Dynamic IP Address [EXIT]

▶ LAN IP Address

▶ Host Name (optional)

▶ WAN's MAC Address Save Clone MAC

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

8. This page allows you to disable the wireless function, set the wireless network name (SSID) and change the wireless channel. Click **Next** when finished.

Setup Wizard - Wireless settings [EXIT]

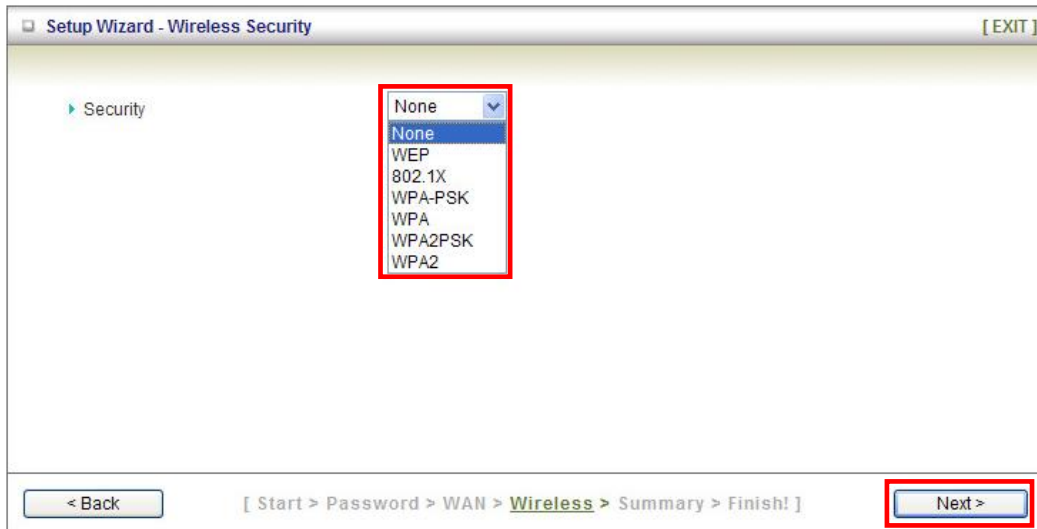
▶ Wireless Radio Enable Disable

▶ Network ID (SSID)

▶ Channel

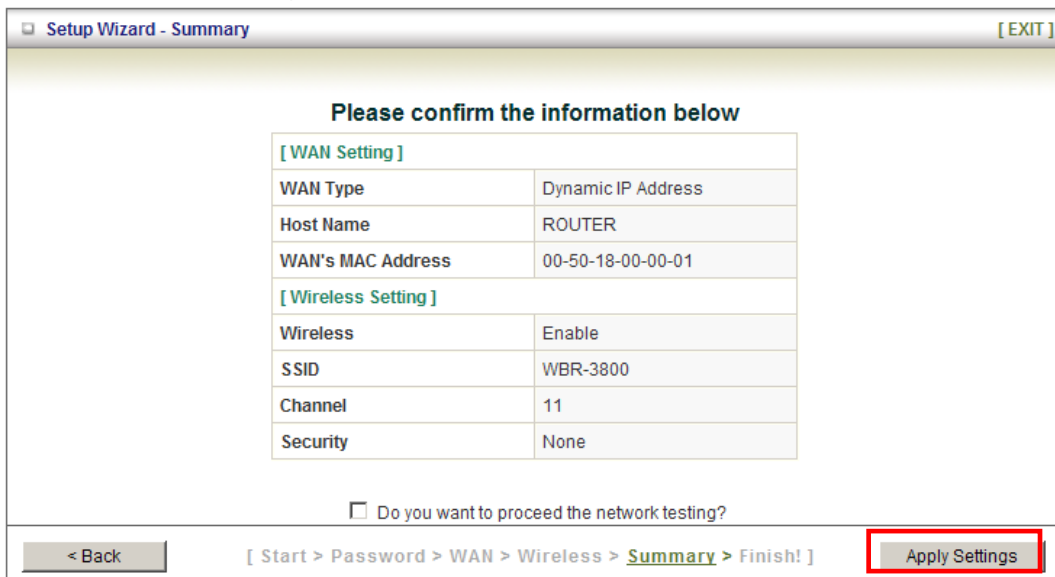
< Back [Start > Password > WAN > Wireless > Summary > Finish!] Next >

9. Select the Wireless security method of your wireless configuration. Click “Next” to continue.

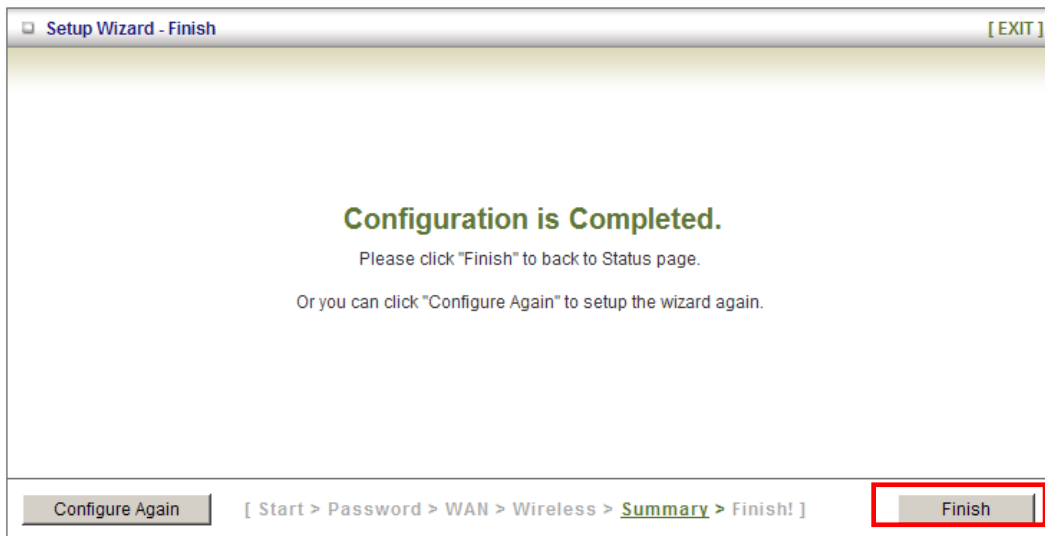


Note: It is strongly recommended that you set up Wireless Security such as WEP or WPA in order to secure your network. Please refer to page 21.

10. Please review the settings, and then click **Apply Settings** to save. If there are mistakes, use **Back** to go back and make corrections.



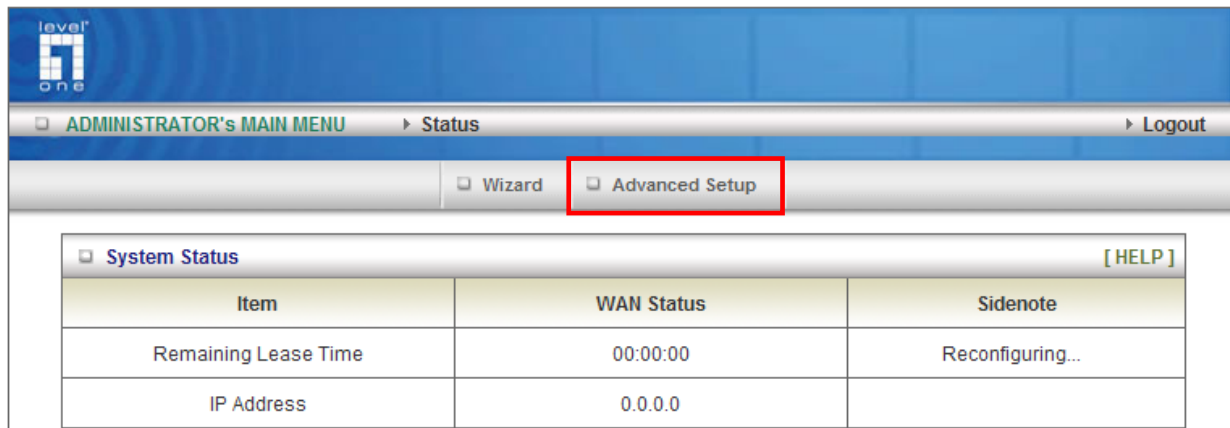
11. Once settings are saved, click **Finish** to go back to the Status page.



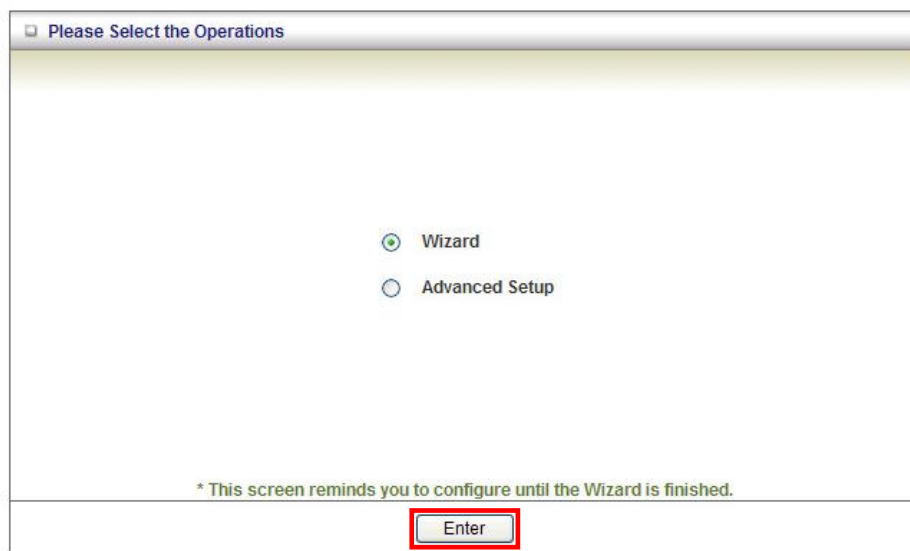
12. If everything is properly configured, the Status page will show WAN or 3G service is online and IP's are assigned.

Chapter 4 - Advanced Setup

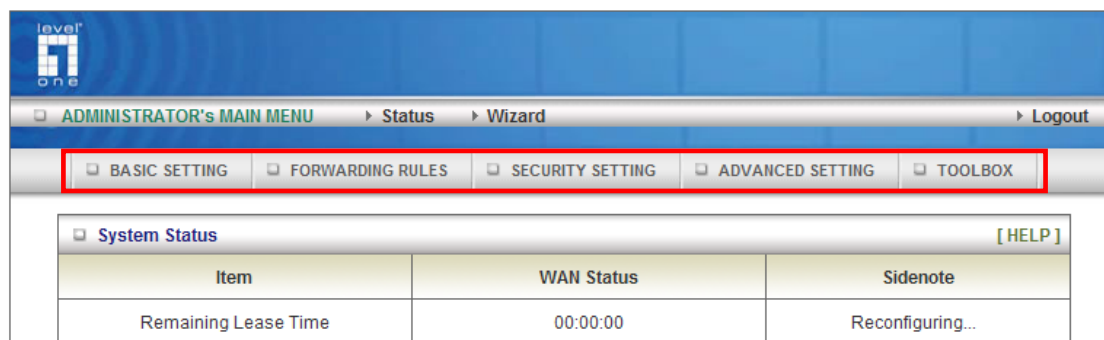
To access the Advanced Setup, click on **Advanced Setup** at the top of the page.



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

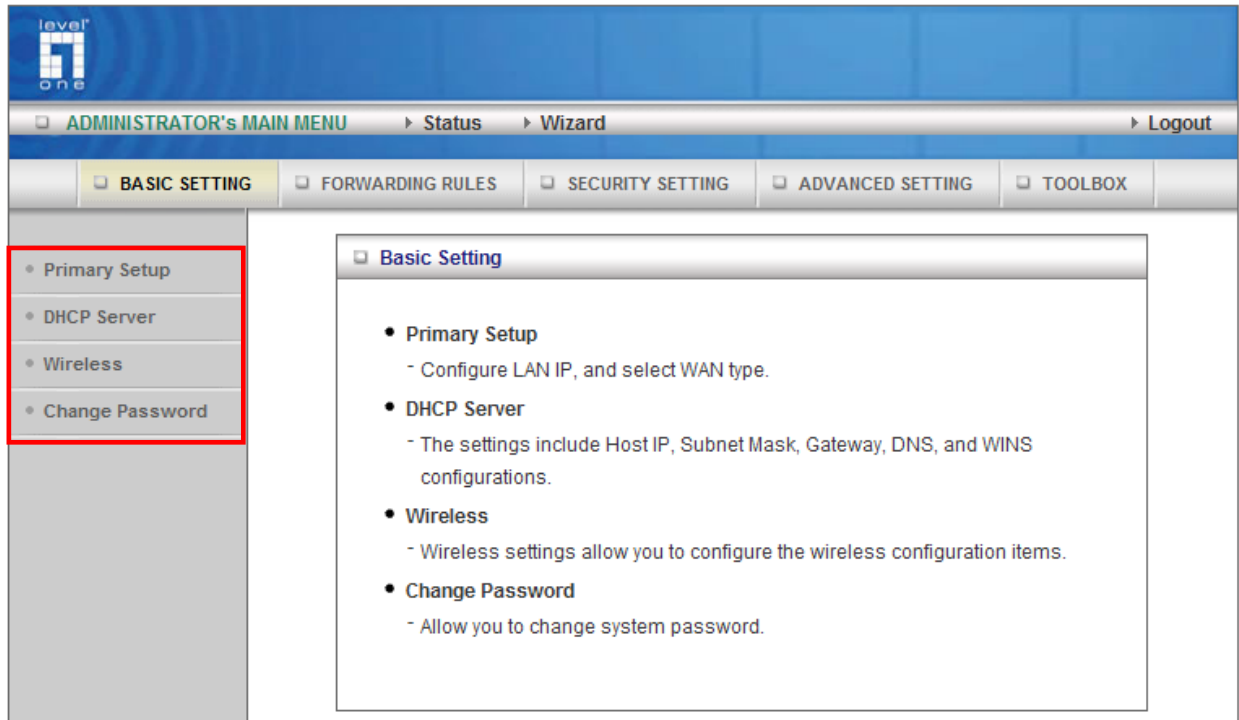


Once in the Advanced Setup, you will be presented with the following menu.



Basic Setting

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



Basic Settings > Primary Setup

This page lets you change the LAN (Local Area Network) settings on your WBR-3800 MobilSpot™ and WAN (Wide Area Network) connection.

Primary Setup [HELP]	
Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.0.1"/>
▶ LAN NetMask	<input type="text" value="255.255.255.0"/>
▶ WAN's MAC Address	<input type="text" value="00-50-18-00-00-01"/> <input type="button" value="Save"/> <input type="button" value="Clone MAC"/>
▶ Auto-Backup	<input type="checkbox"/> Enable checking wired-WAN alive Internet host: <input type="text"/>
▶ WAN Type	
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia. (eg. Telstra BigPond)
<input checked="" type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> 3G	3G
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ MTU	<input type="text" value="1492"/>
▶ Primary DNS	<input type="text" value="0.0.0.0"/>
▶ Secondary DNS	<input type="text" value="0.0.0.0"/>
▶ Maximum Idle Time	<input type="text" value="300"/> seconds <input checked="" type="checkbox"/> Auto-reconnect
▶ PPPoE Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text" value="0.0.0.0"/> (optional)
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Virtual Computers..."/>	

- I. **LAN IP Address:** The local IP address of this device
- II. **LAN Netmask:** The Netmask of the local IP address
- III. **WAN's MAC Address:** The WAN's MAC of this device. If you want to clone the MAC address from your NIC, just click the Clone MAC and Save
- IV. **Auto-Backup:** Checks whether your WAN port connection is active. When WAN port is disconnected, it will automatically switch to 3G internet.
- V. **WAN Type:** WAN connection type of your ISP. You can select a correct one from the following options
 - a) *Static IP Address:* For connections with static IP Addresses
 - b) *Dynamic IP Address:* For connection with Dynamic IP Addresses.
 - c) *Dynamic IP Address with Road Runner Session Management:* When using the WBR-3800 with Telstra Bigpond Cable service.
 - d) *PPP over Ethernet:* For connection with PPPoE service, mostly when used with ADSL modem.
 - e) *L2TP:* For connection with L2TP service
 - f) *PPTP:* For connection with PPTP
 - g) *3G:* For connection with 3G service.

Note: All the above connection types are used with a modem or router connected to the WAN port. Only 3G requires a 3G USB or CardBus modem.

For 3G services, you may need the following information from your 3G provider.

- APN – Enter the APN for your 3G provider.
 - Pin Code – Enter the PIN code for your 3G modem.
 - Dial-Number – No change is usually required, unless required by provider.
 - User Name – Enter your 3G username.
 - Password – Enter your 3G password.
- VI. **Maximum Idle Time:** Enter the number of seconds without any activity before your connection will be terminated automatically.
 - VII. **Auto-Reconnect:** When disconnected, the MobilSpot™ will attempt to automatically reconnect to the ISP.
 - VIII. **Primary DNS/Secondary DNS:** To assign DNS Servers (optional)
 - IX. **Primary WINS/Secondary WINS:** To assign WINS Servers (optional)
 - X. **Maximum idle Time:** If no Internet activity for the set period, then the Internet connection will be dropped.
 - XI. **Auto-Reconnect:** When Internet connection is dropped, the MobilSpot will attempt to reconnect.
 - XII. **Virtual Computer:** Used when WAN is set as DHCP or Static IP, the user can assign a global IP address to a LAN IP address.

Basic Setting > DHCP Setup

This page allows you to configure the DHCP server on the MobilSpot™.

DHCP Server [HELP]	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Lease Time	<input type="text" value="1440"/> Minutes
▶ IP Pool Starting Address	<input type="text" value="50"/>
▶ 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 Server	<input type="text" value="0.0.0.0"/>
▶ Secondary WINS Server	<input type="text" value="0.0.0.0"/>
▶ Gateway	<input type="text" value="0.0.0.0"/> (optional)
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Clients List..."/> <input type="button" value="Fixed Mapping..."/>	

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.

Basic Setting > Wireless

This page allows you to configure the wireless feature of the unit.

Wireless Settings [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID	<input type="text" value="WBR-3800"/>
Channel	<input type="text" value="11"/>
Security	<input type="text" value="None"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting"/>	

1. **Wireless - Enabled** by default. Disabling this will turn off the wireless feature of this unit.
2. **WMM Capable** - Choose Enable or Disable WMM (WiFi Multimedia) function. This function provides features that improves audio, video and voice applications over the wireless network.
3. **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-3800**. The SSID can be easily changed to establish a new wireless network.

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

4. **Channel** - Channels 1-13 are available to choose from, 11 is the default. Devices on the network must share the same channel. Changing the channel may improve signal quality.

Note:

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

Wireless adapters automatically scan and match the wireless settings. You may also select the channel you wish to use.

5. **Security** - You may select from three levels of encryption to secure your wireless network: No Encryption, WEP.802.1x, WPAPSK, WPA, WPA2PSK, or WPA2.
 - a) **No Encryption** is the default (as shown in the screen above).

- b) **WEP Security:** WEP (Wired Equivalent Privacy). Enabling the security can protect your data while it is transferred to the WBR-3800. 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 Settings [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID	WBR-3800
Channel	11
Security	WEP
WEP Encryption	<input checked="" type="radio"/> 64 bit <input type="radio"/> 128 bit
Key 1	<input checked="" type="radio"/> HEX <input type="text"/>
Key 2	<input type="radio"/> HEX <input type="text"/>
Key 3	<input type="radio"/> HEX <input type="text"/>
Key 4	<input type="radio"/> HEX <input type="text"/>
<p>5 or 13 ascii characters eg: passwd or thisisapasswd 10 or 26 hexadecimal characters eg: 0123456789 or 01234567890123456789012345</p> <p>Save Undo WDS Setting</p>	

- c) **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 Settings [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID	WBR-3800
Channel	11
Security	802.1X
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	
<p>Save Undo WDS Setting</p>	

- d) **WPA-PSK / WPA-PSK2:** 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. ASCII.

Wireless Settings [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID	<input type="text" value="WBR-3800"/>
Channel	<input type="text" value="11"/>
Security	<input type="text" value="WPA-PSK"/>
Encryption Type	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
Passphrase	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting"/>	

- e) **WPA / 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 Settings [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID	<input type="text" value="WBR-3800"/>
Channel	<input type="text" value="11"/>
Security	<input type="text" value="WPA2"/>
Encryption Type	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
RADIUS Server IP	<input type="text" value="0.0.0.0"/>
RADIUS port	<input type="text" value="1812"/>
RADIUS Shared Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting"/>	

After configuring the wireless security settings on the WBR-3800 MobilSpot™, 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 supports all the available security functions.

To configure WDS, click on **WDS Setting** button.

WDS Setting		[HELP]
Item	Setting	
▶ Wireless Bridging	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
▶ Remote AP MAC	MAC 1	<input type="text"/>
	MAC 2	<input type="text"/>
	MAC 3	<input type="text"/>
	MAC 4	<input type="text"/>
	MAC 5	<input type="text"/>
	MAC 6	<input type="text"/>
Scanned AP's MAC <input type="text"/> --- Select one --- <input type="button" value="Copy to"/> Remote AP MAC <input type="text"/>		
SSID	Channel	MAC Address
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Scan AP"/>		

WDS is used to wirelessly connect multiple Access Points, to extend the range of the wireless network without using cables. Please note that not all Access Points support WDS functions

To enable WDS, Enable **Wireless Bridging**.

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. This MobilSpot™ can support up to 6 remote MAC addresses.

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

Basic Setting > Change Password

This page allows you to change the WBR-3800 Web Configuration password. Please type in the old password (factory default password is **password**) and then type in the new password.

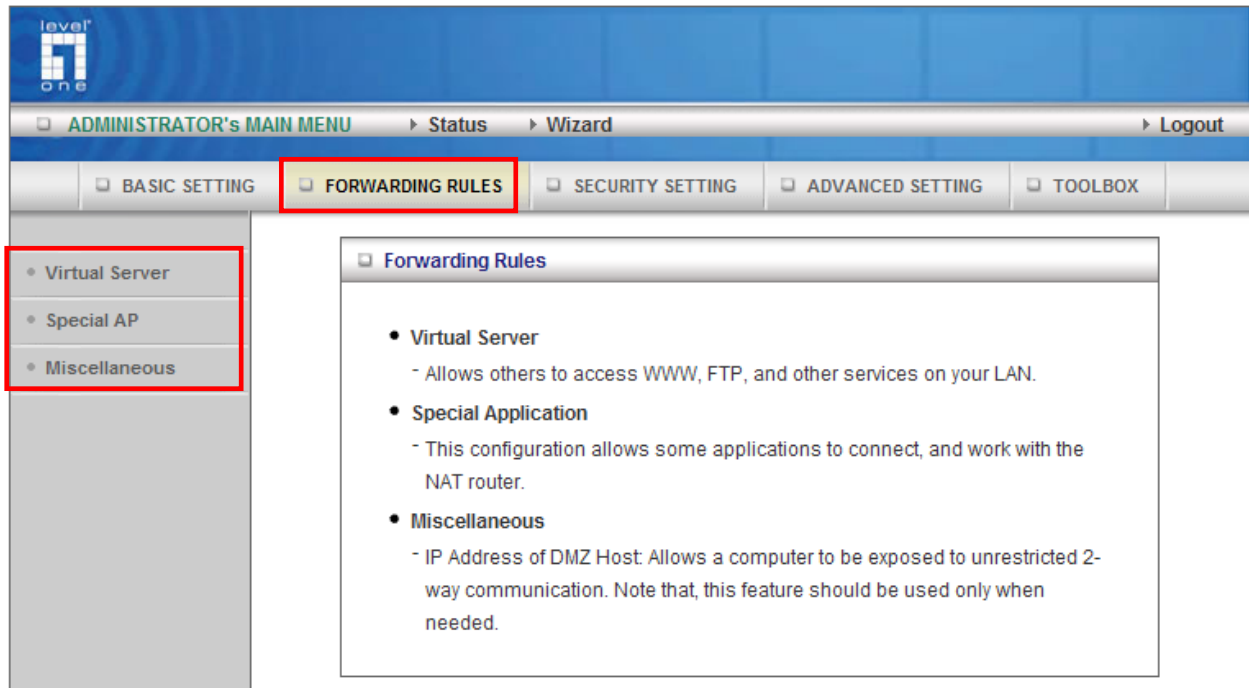
Change Password	
Item	Setting
▶ Old Password	<input type="password" value="....."/>
▶ New Password	<input type="password"/>
▶ Reconfirm	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

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-3800. Use the menu on the left to access the setting pages.



The port forwarding feature is required because the MobilSpot'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).

Forwarding Rules > Virtual Server

Virtual Server
[HELP]

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

Use schedule rule ---ALWAYS ON---

ID	Service Ports	Server IP	Enable	Schedule Rule#
1	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
11	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
12	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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:

Service Port	Server IP	Enable
21	192.168.0.1	V
80	192.168.0.2	V
1723	192.168.0.6	V

Note: You can only bind one IP address to a Service Port at a given time.

Forwarding Rules > Special AP

Special Applications [HELP]			
Popular applications -- select one -- Copy to ID --			
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"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="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-3800. 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-3800 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.

Forwarding Rules > Miscellaneous

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

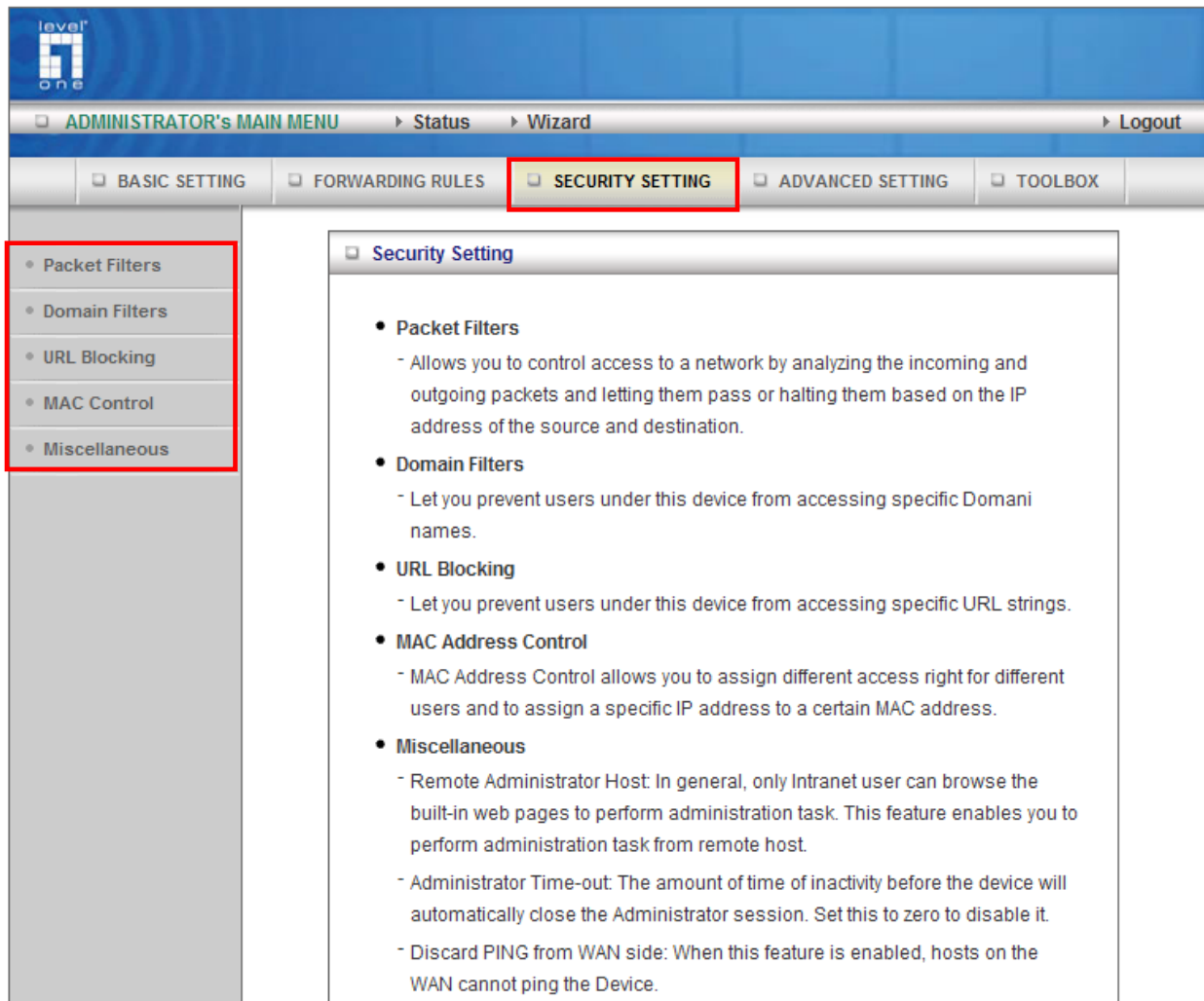
This setting is most commonly used for Internet gaming, Video conferencing, Internet telephony and other special applications.

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

Miscellaneous Items		[HELP]
Item	Setting	Enable
▶ IP Address of DMZ Host	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

Security Setting

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.



Security Setting > Packet Filters

Packet Filters allows you to control what packets are allowed to pass through the MobilSpot™. 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.				
Use schedule rule: ALWAYS ON <input type="button" value="Copy to"/> ID: --				
ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="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) or a range of IP addresses (192.168.0.100 – 192.168.0.200). 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.				
Use schedule rule ---ALWAYS ON--- <input type="button" value="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"/>
<input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/>				

Security Setting > Domain Filters

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

Item		Setting	
▶ Domain Filter		<input type="checkbox"/> Enable	
▶ Log DNS Query		<input type="checkbox"/> Enable	
▶ Privilege IP Addresses Range		192.168.0.[0] ~ [0]	
ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input 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"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

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 MobilSpot™ to take. Tick on **Drop** to block the access and/or tick on **Log** to log this access.

Security Setting > URL Blocking

URL Blocking will block LAN computers from connecting to a pre-defined Web Sites. 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.

Http URL Blocking [HELP]		
Item	Setting	
▶ URL Blocking	<input type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

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.

Security Setting > MAC Control

The MAC Control allows you to assign different access rights for different users, and to assign a specific IP address to a certain MAC address.

MAC Address Control [HELP]					
Item	Setting				
▶ MAC Address Control	<input type="checkbox"/> Enable				
<input 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 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.				
DHCP clients <input type="text" value="-- select one --"/> Copy to ID <input type="text" value="--"/>					
ID	MAC Address	IP Address	Wake On Lan	C	A
1	<input type="text"/>	192.168.0. <input type="text"/>	<input type="text" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.0. <input type="text"/>	<input type="text" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.0. <input type="text"/>	<input type="text" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.0. <input type="text"/>	<input type="text" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Previous page"/> <input type="button" value="Next page"/> <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 MobilSpot™. If a client is denied, then it means the client cannot send or receive any data via this MobilSpot™. 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.

Security Setting > Miscellaneous

This page allows you to change various miscellaneous security settings.

Miscellaneous Items [HELP]		
Item	Setting	Enable
▶ Remote Administrator Host / Port	0.0.0.0 / 80	<input type="checkbox"/>
▶ Administrator Time-out	600 seconds (0 to disable)	
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ Disable UPnP		<input type="checkbox"/>

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 80. 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 WAN cannot ping this MobilSpot™.

Disable UPnP: When enabled, UPnP will be disabled for security reasons.

Advanced Setting

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

The screenshot displays the Level One Administrator's Main Menu. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this, a secondary menu contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (highlighted with a red box), and 'TOOLBOX'. On the left side, a vertical sidebar lists various settings: 'System Log', 'Dynamic DNS', 'QoS', 'SNMP', 'Routing', 'System Time', 'Scheduling', and 'Performance'. The 'Advanced Setting' page is active, showing a list of settings with brief descriptions:

- **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**
 - Gives a user the capability to control network traffic with different priority.
- **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**
 - Let you set up the system time of this device through NTP, PC's timer, or manually.
- **Scheduling**
 - You can set the scheduling rules here, and select the rule number in Virtual Server and Packet Filter, the functions will be active with your scheduling rules.

Advanced Setting > System Log

The WBR-3800 MobilSpot™ supports both Syslog (using UDP packets) and E-Mail alert.

System Log		[HELP]
Item	Setting	Enable
▶ IP Address for System Log	192.168.0. <input type="text"/>	<input type="checkbox"/>
▶ E-mail Alert		<input type="checkbox"/>
▶ SMTP Server IP and Port	<input type="text"/>	
▶ Send E-mail alert to	<input type="text"/>	
▶ E-mail Subject	<input type="text"/>	

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)

Advanced Setting > 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 MobilSpot™, or any services behind the MobilSpot™ 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) ▼
▶ 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.

Advanced Setting > SNMP

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 type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text" value="0.0.0.0"/>
▶ IP 2	<input type="text" value="0.0.0.0"/>
▶ IP 3	<input type="text" value="0.0.0.0"/>
▶ IP 4	<input type="text" value="0.0.0.0"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input 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 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.

Advanced Setting > Routing

When you have more than one MobilSpot™, 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			
▶ RIP		<input type="checkbox"/> Enable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
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-3800.

- **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-3800 to communicate with computers on other LAN segments which are connected to the WBR-3800 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.

Advanced Setting > System Time

This page allows you to set the time settings of the WBR-3800.

System Time [HELP]	
Item	Setting
▶ <input checked="" 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, 21 March 2008 5:07:39 PM
▶ <input type="radio"/> Set Date and Time manually	
Date	Year: 2002 Month: Jan Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)
▶ Daylight Saving	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Start	Jan 1
End	Jan 1
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

There are three ways to set up the System Time of the WBR-3800.

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.

Advanced Setting > Scheduling

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
<input type="button" value="Save"/> <input type="button" value="Add New Rule..."/>		

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

Schedule Rule Setting [HELP]		
Item	Setting	
▶ Name of Rule 1	<input type="text"/>	
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"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>		

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

Advanced Setting > Performance

This page allows you to change the settings of advanced wireless functions.

Wireless Performance Settings [HELP]	
Item	Setting
▶ Beacon interval	100 (msec,range:1~1000,default 100)
▶ DTIM interval	3 (range: 1~65535,default 3)
▶ Wireless Mode	<input checked="" type="radio"/> mixed mode <input type="radio"/> G mode
▶ TX Rates	Auto ▼
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Speed Enhanced Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Antenna Transmit Power	100% (17dBm) ▼

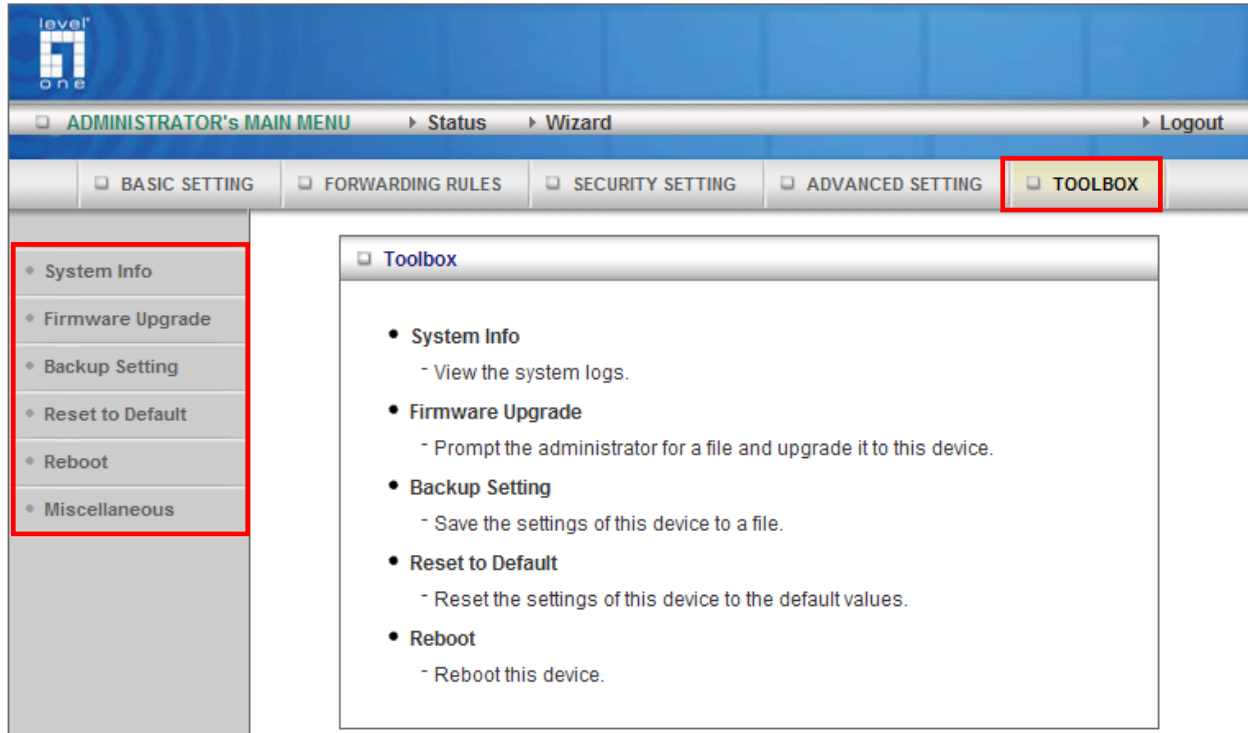
1. **Beacon Interval:** Beacons are packets sent by the unit to synchronize with wireless adapters. The default value is set to 100 milliseconds and the acceptable range is 1 to 1000.
2. **DTIM Interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the unit has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages.

The default value is 3, and the acceptable range is between 1 and 65535.

3. **Wireless Mode:** Select whether to only allow 11g connections, or mixed mode to allow both 11b and 11g connections.
4. **TX Rates:** Depending on signal strength and the capacity of the wireless client, the transmission speed operates at 5Mbps and may drop to lower rates when necessary. The default setting is Auto.
5. **SSID Broadcast:** Choose whether to broadcast this unit's SSID. Turning it off will make your wireless network nearly invisible.
6. **Speed Enhanced Mode:** This TX Burst function is only available for Ralink wireless clients to increase the speed of the wireless connection.
7. **Antenna Transmit Power:** You can either increase or decrease the antenna transmission power. The default setting is 100% (17dBi).

Tool Box

This section has various tools that are available to maintain the WBR-3800's systems.



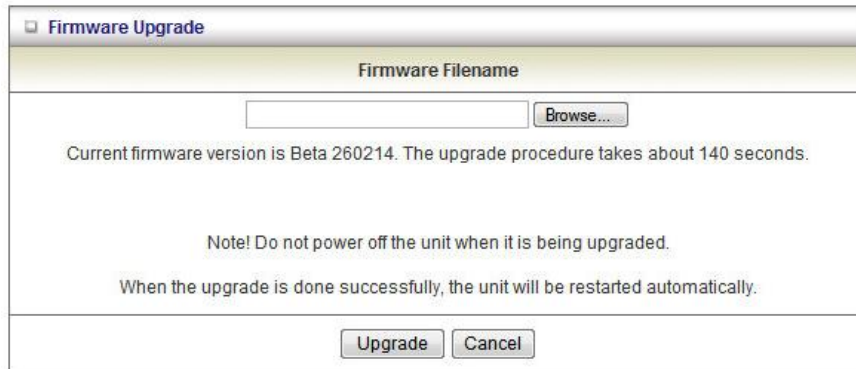
Tool Box > System Info

This page shows the user the System Log and Routing Table of the WBR-3800.

System Information	
Item	Info
▶ WAN Type	Dynamic IP Address (Beta 260214)
▶ Display Time	Tue Nov 30 00:35:13 1999
▶ Log Message	<input checked="" type="radio"/> System Log <input type="radio"/> Routing Table
System Log	
Time	Log
Nov 30 00:00:12	syslogd: syslogd started
Nov 30 00:00:12	boot: Machine restarting
Nov 30 00:00:12	boot: LAN MAC address: 00:50:18:21:c4:f9
Nov 30 00:00:12	boot: WAN MAC address: 00:50:18:21:c4:fa
Nov 30 00:00:16	dhcpd: Listening on LAN 192.168.123.0
Nov 30 00:00:29	dhcpd: already acking lease 192.168.123.50
Nov 30 00:00:29	dhcpd: offer 192.168.123.50 to 00:18:de:8a:6a:9c
Nov 30 00:01:18	httpd: 192.168.123.50 logins successful
Nov 30 00:02:19	dhcpd: inform from 192.168.123.50
Nov 30 00:02:24	dhcpd: inform from 192.168.123.50
Nov 30 00:24:15	httpd: 192.168.123.50 logins successful
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>	

Tool Box > Firmware Upgrade

This page allows you to perform updates to the firmware of the WBR-3800.



The screenshot shows a dialog box titled "Firmware Upgrade". At the top, there is a header bar with the text "Firmware Upgrade". Below this, there is a section labeled "Firmware Filename" which contains a text input field and a "Browse..." button. The main body of the dialog contains the following text: "Current firmware version is Beta 260214. The upgrade procedure takes about 140 seconds." Below this is a note: "Note! Do not power off the unit when it is being upgraded." and another line: "When the upgrade is done successfully, the unit will be restarted automatically." 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-3800 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.

Tool Box > 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.

Tool Box > 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.

Tool Box > Reboot

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

Tool Box > Miscellaneous

This page allows you to set up the Wake-on-LAN feature. It allows you to power up a network device remotely. To use this feature, the network device must be Wake-on-LAN enabled and you will need to know the MAC address of the device.

Miscellaneous Items [HELP]	
Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text" value="00-00-00-00-00-00"/> <input type="button" value="Wake up"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

By entering the network device's MAC address and click **Wake Up**, the WBR-3800 will send a wake-up command to the network device.

Note: This feature only works for computers connected locally to the WBR-3800.

Troubleshooting

This section provides an overview of common issues, and possible solutions for the installation and operation of the WBR-3800 MobilSpot™.

1. Unable to access the Configuration Menu when I use my computer to configure the MobilSpot™. Why?

Note: It is recommended that you use an Ethernet connection to configure the WBR-3800.

Ensure that the Ethernet LED on the WBR-3800 MobilSpot™ is ON.

If the LED is NOT ON, check to see if the cable for the Ethernet connection is securely connected.

Note: Ensure that the IP Address of the computer is in the same range and subnet as the WBR-3800 MobilSpot™. The default IP Address of the WBR-3800 is *192.168.0.1*. All the computers on the local area network must have a unique IP Address within the same range (e.g., *192.168.0.x*). All computers must also have the same subnet mask (e.g., *255.255.255.0*). Any computers that have the identical IP Address will not be visible on the network.

Do a Ping test to make sure that the WBR-3800 is responding.

- Click on Start > Run.
- Type cmd.
- Press Enter.
- Type "ping 192.168.0.1". A successful ping shows four replies.

Note: If you have changed the default IP Address, ensure you ping the correct IP Address assigned to the WBR-3800 MobilSpot™.

2. Why my wireless client can NOT access the Internet?

When the WBR-3800 is configured to use either **WEP** or **WPA-PSK** encryption, ensure encryption settings match that of your wireless adapter settings. Please refer to your wireless adapter documentation for additional information.

Ensure that the wireless client is associated and joined with the correct Access Point. To check this connection (Windows XP), follow the steps below:

- Click on Start > Control Panel > Network Connection
- Right-click on the Wireless Network connection

- Select View Available Wireless Networks in Wireless Configure. The Connect to Wireless Network screen appears.
- Ensure you have selected the correct wireless network.

Ensure that the IP Address of the computer is in the same range and subnet as the WBR-3800 MobilSpot™. The default IP Address of the WBR-3800 is *192.168.0.1*. All the computers on the local area network must have a unique IP Address within the same range (e.g., *192.168.0.x*). All computers must also have the same subnet mask (e.g., *255.255.255.0*). Any computers that have the identical IP Address will not be visible on the network.

To check the IP Address assigned to the wireless adapter, follow the steps below:

- Click on Start > Run
- Type in **cmd** and press Enter.
- Enter **ipconfig /all** and press Enter
- Enter **ping 192.168.0.1** to check if you can access the WBR-3800.

3. Why does my wireless connection keep dropping?

You may try following steps to solve.

- Antenna Orientation
Try different antenna orientations for the WBR-3800 MobilSpot™
Try to keep the antenna at least 6 inches away from the wall or other objects.
- Changing the Wireless Channel
Try changing the channel on the WBR-3800 to a different channel to avoid interference. Please refer to Basic > Wireless section on page 21.

4. Why I am unable to achieve a wireless connection?

Note: An Ethernet connection is required to troubleshoot the WBR-3800 MobilSpot™.

- If you have enabled Encryption (WEP, WPA/WPA2) on the WBR-3800, you must also enable encryption on all wireless clients in order to establish a wireless connection. Please refer to your wireless adapter manual for more information.
- Move the WBR-3800 and the wireless client into the same room, and then test the wireless connection.

- Try disabling all security settings such as **WEP**, and **MAC Address Control**.
- Try turning off the unit and the wireless client. Then turn both back on again.
- Ensure that all devices are set to **Infrastructure** mode.
- Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
- Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically, or drop altogether.
- To avoid interference, change the wireless channel on the WBR-3800, and all devices in your network.
- Try to keep your product at least 3-6 feet away from electrical devices that generate RF noise. Examples include: microwaves, monitors, electric motors etc.

5. I just do not remember my encryption key. What should I do?

If you forgot your encryption key, the Wireless client will be unable to establish a connection.

To reset the encryption key, log into the WBR-3800 using a wired Ethernet connection. Refer to Basic > Wireless on page 21 for more information.

6. How do I reset my WBR-3800 MobilSpot™ to its factory default settings?

If other troubleshooting methods have failed, you may choose to Reset the MobilSpot™ to its factory default settings.

To hard reset the MobilSpot™ to its factory default settings, follow the steps listed below:

- Ensure the MobilSpot™ is powered on (for at least 20 seconds).
- Use a paper clip or pencil tip to press the reset button for ten seconds, and then release.
- Do not power off the unit while it is rebooting.
- Once rebooted, the default settings will be restored.
- Remember to access the web configuration page using default IP of 192.168.0.1 and password "password".

7. What is VPN?

VPN stands for "Virtual Private Networking." VPNs create a "tunnel" through an existing Internet connection using PPTP (Point-to-Point Tunneling Protocol) or IPSec (IP Security) protocols with various encryption schemes including Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

This feature allows you to use your existing Internet connection to connect to a remote site with added security.

Technical Specifications

3G Access	1*PC card Type II Slot and USB 2.0 port
Standards	IEEE 802.11b/g IEEE 802.3 IEEE 802.3u
Wireless Standard	IEEE 802.11b/g Turbo
Data Rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps per Channel Auto Fall-Back
Frequency	2.4 – 2.462 GHz, CCK / OFDM modulation
Range Coverage	Transmit / Reception Power - 18dBm/Per Cell Indoors approx. 35-100 meters; Outdoors up to 100-300 meters
# of Channels	1-11 for N. America (FCC); 1-11 for Canada (DOC) 1-13 Europe (Except Spain and France) (ETSI) 1-14 Japan (TELEC);
Security	64bit and 128bit WEP Encryption; WPA Encryption
Antenna	Detachable Antenna 1.8dBi
Firewall	IP Filtering NAT (Network Address Translation) with VPN Pass through MAC Filtering
Supported WAN type	3G,Static IP, Dynamic IP, PPPoE,PPTP,L2TP
Connection Scheme	Connect-on-Demand, Auto-Disconnect, Auto-Reconnect
NAT function	Class C ;One-to-Many; Max 253 Users; Virtual Server; DMZ Host
VPN	PPTP, L2TP and IPSec Pass Through
Config.& Management	Web-Based Browser Configuration, SNMP DHCP Server and Client
Working Environment	Temperature: 0~40°C, Humidity 10%~90% non-condensing
OS supported	Windows 95/98/ME/NT/2000/XP/Vista; Linux
Power	Switching 5V 3.0A

3G/3.5G Modem Compatibility List

USB Interface

Brand	Model	3G System	Location Tested
BandLuxe	C-120	HSDPA	Taiwan
Huawei	E172	HSDPA	Germany
Huawei	E220	HSDPA	Taiwan
Huawei	E270	HSDPA/HSDPA	Singapore
LightSpeed	HSDPA-180C	HSDPA	Taiwan
LightSpeed	EDGE-180M	EDGE	Taiwan
Maxon	USB3-8521	HSDPA	Australia
Novatel	ES720	EVDO	USA
Novatel	U727	EVDO	USA
Novatel	MC950D	HSDPA	Taiwan
Option	ICON 225	HSDPA	Taiwan
Sony Ericsson	MD300	HSDPA	Taiwan
Sierra	AC881U	HSDPA	Taiwan
Solomon	S3GM-660	HSDPA	Taiwan
SpeedUp	SU-6200	CDMA2000 1x	Taiwan
SpeedUp	SU-8200	HSDPA	Taiwan
Verizon	ES720	EVDO	USA
Vodafone	E172	HSDPA	Germany
Vodafone	EasyBox	HSDPA	Taiwan
ZTE	MF620	HSDPA	Taiwan

Mobile Phones

Brand	Model	3G System	Location Tested
Nokia	E50	GPRS	Germany
Nokia	E90	HSDPA	Germany

PCMCIA/CardBus Interface

Brand	Model	3G System	Location Tested
C-Motech	CDC-650	EVDO	Israel
Eston	501P	CDMA2000	Taiwan
Eston	611P	EDGE	Taiwan
Huawei	E600	UMTS	Australia
Huawei	E620	HSDPA	Australia
Huawei	E800A	HSDPA	Australia
ITON530C	Globe Trotter	CDMA 1X	Taiwan
IPWireless	IPWireless_V1	UMTS	Australia
IPWireless	IPWireless_V3	UMTS	Australia
Kyocera	iBurst PC card	iBurst	Taiwan
Kyocera	KPC650	EVDO	Taiwan
Kyocera	1.9G AS	iBurst	Australia
LightSpeed	EDGE-100M	EDGE	Taiwan
LightSpeed	EDGE-100N	EDGE	Taiwan
LightSpeed	GPRS-100S	GPRS	Taiwan
MERLIN	U530	UMTS	Taiwan
Novatel	U530	UMTS	Australia
Novatel	U740	HSDPA	Australia
Option	GX0202	HSDPA	Australia
Option	Globe Trotter	UMTS	Taiwan
Option	Globe Trotter 3G+ EMEA	HSDPA	Germany
Option	Globe Trotter GT 3G Quad	HSDPA	Germany
Option	GT MAX	HSDPA	Taiwan
Option	GT Fusion+	HSDPA	Taiwan
Pantech	PX-500	EVDO	USA
Qualcom	GEO201	HSDPA	Germany
Sierra	AC595	EVDO	Australia
Sierra	AC775	EDGE	Thailand
Sierra	AC875	UMTS	Australia
Sierra	AC880	HSUPA	Australia
Sierra	AC881	HSUPA	Australia
Sony Ericsson	GC83	EDGE	Taiwan
Vodafone	GEO201	HSDPA	Germany
Vodafone	GT 3G+	HSDPA	Germany

Vodafone	GT 3G Quad	UMTS	Taiwan
Willcom	AX520N	PHS	Japan
Verizon	PC5740	EVDO	USA
Yiso	C893	EVDO	USA
ZTE	MF 332	HSDPA	Australia
Growell	C803	CDMA 1X EVDO	Taiwan
Growell	GW-1033C	CDMA2000 1X	Taiwan

Note: For the latest compatibility list, please see www.level1.com.