



LevelOne

WAP-0004

11g Wireless AP/Client/AP Router

USER MANUAL

Contents

1. Overview	4
1.1 Product Feature	4
1.2 System Requirements	4
1.3 How to switch within 3 modes	4
2. Getting Start with Access Point	6
2.1 Know the 11g Wireless Network Access Point	6
2.2 Connect to the 11g Wireless Network Access Point	6
2.3 Quick Setup with Wizard	7
2.3.1 Access the Setting Menu	7
2.3.2 Setup with Wizard	9
3. Configuration Access Point through WEB Browser	12
3.1 Status	12
3.2 Basic Setting	14
3.3 IP Setting	16
3.4 Advanced Setting	17
3.5 Security	18
3.6 Tools	19
4. Getting Start with Wireless Ethernet Adapter	21
4.1 Know the Wireless Ethernet Adapter	21
4.2 Connect to the Wireless Ethernet Adapter	21
4.2.1 Access the Setting Menu	22
4.2.2 Setup with Wizard	24
5. Configuration Wireless Ethernet Adapter through WEB Browser	27
5.1 Status	27
5.2 Basic Setting	29
5.3 IP Setting	31
5.4 Advanced Setting	32
5.5 Security	33
5.6 Tools	34
6. Getting Start with Wireless Router	35
6.1 Know the 802.11g Wireless Router	35
6.2 Connect to the 802.11g Wireless Router	35
6.2.1 Access the Setting Menu	35
6.2.2 Quick Setup with Wizard	37

7. Configuration Wireless Router through WEB Browser.....	45
7.1 LAN Setting	45
7.1.1 LAN & DHCP Server	45
7.1.2 WAN.....	46
7.1.3 Password	47
7.1.4 Time	48
7.2 Wireless	49
7.2.1 Basic	49
7.2.2 WEP.....	49
7.2.3 Advanced	52
7.3 Status.....	53
7.3.1 Device Information	53
7.3.2 Log.....	54
7.3.3 Log Setting.....	55
7.3.4 Statistic.....	56
7.3.5 Wireless	57
7.4 Routing	58
7.4.1 Static	58
7.4.2 Dynamic.....	59
7.4.3 Routing Table	60
7.5 Access	60
7.5.1 MAC Filters	61
7.5.2 Protocol Filter.....	62
7.5.3 IP Filter.....	62
7.5.4 Virtual Server	63
7.5.5 Special AP.....	65
7.5.6 DMZ	66
7.5.7 Firewall Rule	67
7.6 Management.....	69
7.6.1 Remote Management	69
7.7 Tools	71
7.7.1 Restart	71
7.7.2 Settings.....	72
7.7.3 Firmware	73
7.7.4 Ping Test	74

Digital Data Communications hereby declares that the device WAP-0004 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The EC Declaration of Conformity can be downloaded at: <http://www.level1.com/support.php>

1. Overview

Congratulations on your purchase of this outstanding 3-in1 LevelOne WAP-0004 Pocket Access Point.

This manual is about how to use the 3-in-1 WAP-0004, which including Access Point, Access Point Client and Wireless Router function.

1.1 Product Feature

- **3-in-1 function build-in** with easily accessible hot-key switch, including Access Point, Access Point Client and Wireless Router. It's also the **smallest** networking device in the market.
- **Low power consumption** <less than 460 mA>, and **support USB power adapter** which provides the best mobility.
- Compliance with **IEEE 802.11g** and **802.11b** standards
- Compliance with **WiFi** standard
- Achieving data rate up to **54Mbps** for 802.11g and **11Mbps** for 802.11b with wide range coverage
- Strong network security with **WEP** encryption, and **PWA-PSK** function.
- Quick and easy setup with **Web-based management utility**.

1.2 System Requirements

- Windows 98SE, Millennium Edition (ME), 2000 and XP operating systems
- Microsoft Internet Explorer 5.5 or higher
- At least one RJ-45 Ethernet network adapter installed.

1.3 How to switch within 3 modes

- 3 modes are AP, Client and wireless RT.
- Switch to the mode user wants with the hot key, then re-plug the power.
- Few seconds later, the device will reboot automatically to the mode user wants.
- For **AP**, please use **192.168.1.1** as the default IP to configure the settings.
- For **Client**, please use **192.168.1.50** as the default IP to configure the settings.
- For **wireless RT**, please use **192.168.1.1** as the default IP to configure the

settings, note that the settings must through the wireless connection, instead of RJ45 cable.

1.4 Package content

- . WAP-0004
- Power Adapter
- USB power apply cable
- CD ROM with user`s manual
- Quick Installation Guide

If any of the item is missing, please contact with your dealer.

2. Getting Start with Access Point

2.1 Know the 11g Wireless Network Access Point

Ports:

- Power Receptor
- Reset Button
- RJ-45 Ethernet Port

Cross-over cable is required to connect to computer directly

LEDs:

- Power LED: ON when the unit is powered up
- LAN LED: ON indicates LAN connection; BLINK indicates LAN activity
- WLAN LED: ON indicates WLAN is working; BLINK indicates wireless activity.

2.2 Connect to the 11g Wireless Network Access Point

Build the Infrastructure Mode




In order to setup an Infrastructure of a wireless network such as the example shown above, user will need the following:

1. A broadband Internet connection.

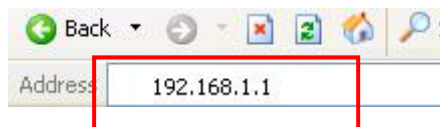
2. ADSL or Cable modem provided by ISP as part of the broadband connection installation.
3. A Router that connects to the ADSL/Cable modem for Internet connection sharing.
4. An Access Point to connect with the Router to form a wireless infrastructure network.
5. Wireless clients equipped with wireless networking devices such as wireless PC Card for wireless connection.

2.3 Quick Setup with Wizard

 Before installation, please set the IP address of your broadband router as 192.168.1.XXX. XXX can be from 2 to 254. And set the TCP/IP of your operating computer to “obtain IP address automatically”.

2.3.1 Access the Setting Menu

User could start to access the configuration menu anytime by opening a web browser window and typing the IP address of this access point. The default IP is **192.168.1.1**.



The below window will popup. Please enter the user name and password. Both of the default is “admin”.



Now, the main menu screen is popup.



The image shows the status screen of an 802.11g Wireless LAN Access Point. The header features the product name and a navigation menu. The main content area displays the current status of the device, including firmware version, LAN settings, and wireless settings. A green sidebar on the left contains the word 'Status' with a circular icon.

802.11g Wireless LAN Access Point

| Wizard | **Status** | Basic Setting | IP Setting | Advanced Setting | Security | Tools |

Status

Firmware Version V1.00

LAN MAC:00-4B-14-7F-6A-C8

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 86


Receive: 198

Wireless

SSID: POCKET_AP



2.3.2 Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get Access Point configuration ready to run in 4 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.




Welcome to the **54Mbps** Access Point Setup Wizard. The Wizard will direct you through these four quick steps. Start by clicking on **Next**.

- Step 1. Set your new password
- Step 2. Set the SSID and Channel
- Step 3. Set Encryption
- Step 4. Restart

Step 1: Set Password

User can change the password and then click “**Next**” to continue.






Set Password

You may want to change the Administrator password of this Access Point to prevent authorized modification to the configuration settings. Enter your new password in the following text fields. Click Next to continue with setup or Exit to quit setup wizard.

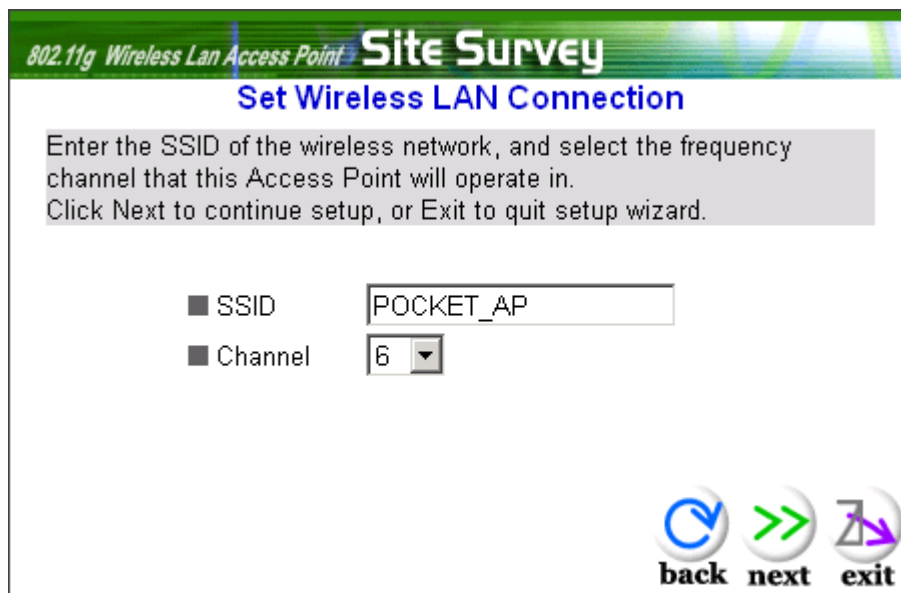
■ Password

■ Verify Password

Step2: Set WLAN Connection

Please type the name of SSID and select the channel. Then, click “**Next**” to continue.






802.11g Wireless Lan Access Point Site Survey

Set Wireless LAN Connection

Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in.
Click Next to continue setup, or Exit to quit setup wizard.

■ SSID

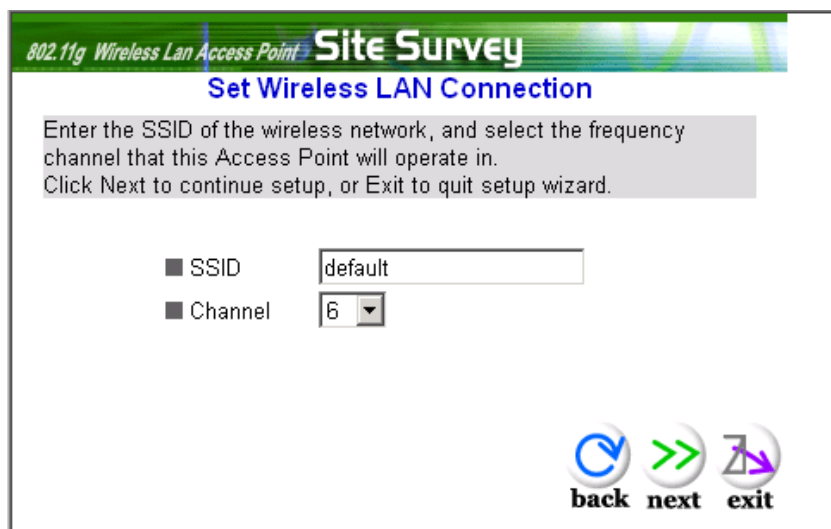
■ Channel

back next exit

Step 3: Set Wireless LAN Connection

If user doesn't want to use “default” as the SSID, user can change SSID here. User can also choose different channel to avoid noise coming from other wireless networking devices. Please click “**Next**” to continue.






802.11g Wireless Lan Access Point Site Survey

Set Wireless LAN Connection

Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in.
Click Next to continue setup, or Exit to quit setup wizard.

■ SSID

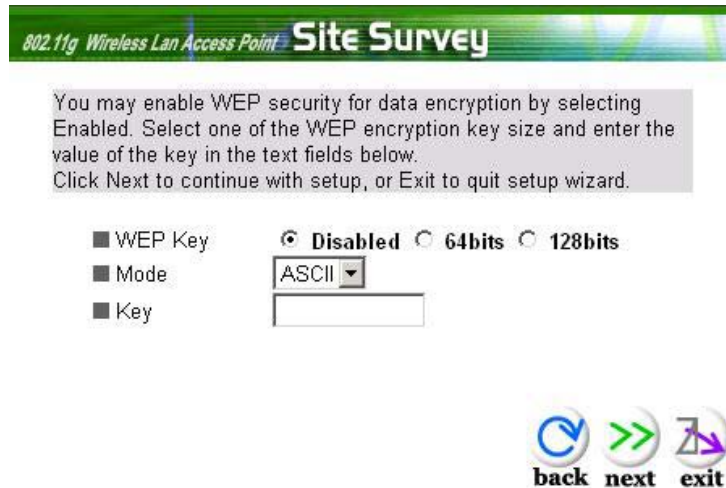
■ Channel

back next exit

Step 4: Set WEP Encryption

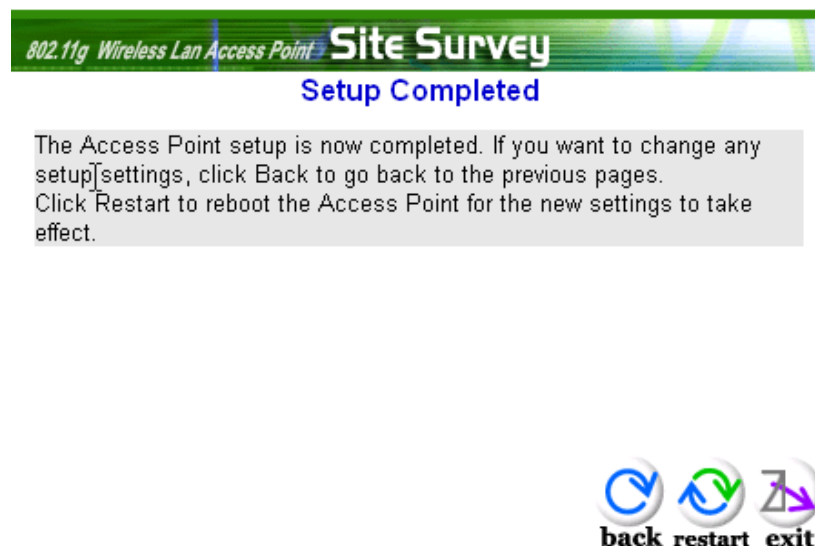
If user wants to enable WEP, please click “**Enabled**”. Then, select the key size of WEP encryption and enter the key value in the key text box. Please click “**Next**” to continue.



The screenshot shows the '802.11g Wireless Lan Access Point Site Survey' setup wizard. The title bar is green with white text. Below the title bar, there is a grey instruction box: 'You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below. Click Next to continue with setup, or Exit to quit setup wizard.' Below the instruction box, there are three labels: 'WEP Key', 'Mode', and 'Key'. The 'WEP Key' label is followed by three radio buttons: 'Disabled' (selected), '64bits', and '128bits'. The 'Mode' label is followed by a dropdown menu showing 'ASCII'. The 'Key' label is followed by a text input field. At the bottom, there are three buttons: 'back' (with a blue circular arrow icon), 'next' (with a green double arrow icon), and 'exit' (with a purple arrow pointing out of a box icon).

Step 5: Restart

The Setup wizard is now completed. The new settings will be effective after the Access Point restarted. Please click “**Restart**” to reboot the Access Point. If user does not want to make any changes, please click “**exit**” to quit without any changes. User also can go back to modify the setting by clicking “**Back**”.

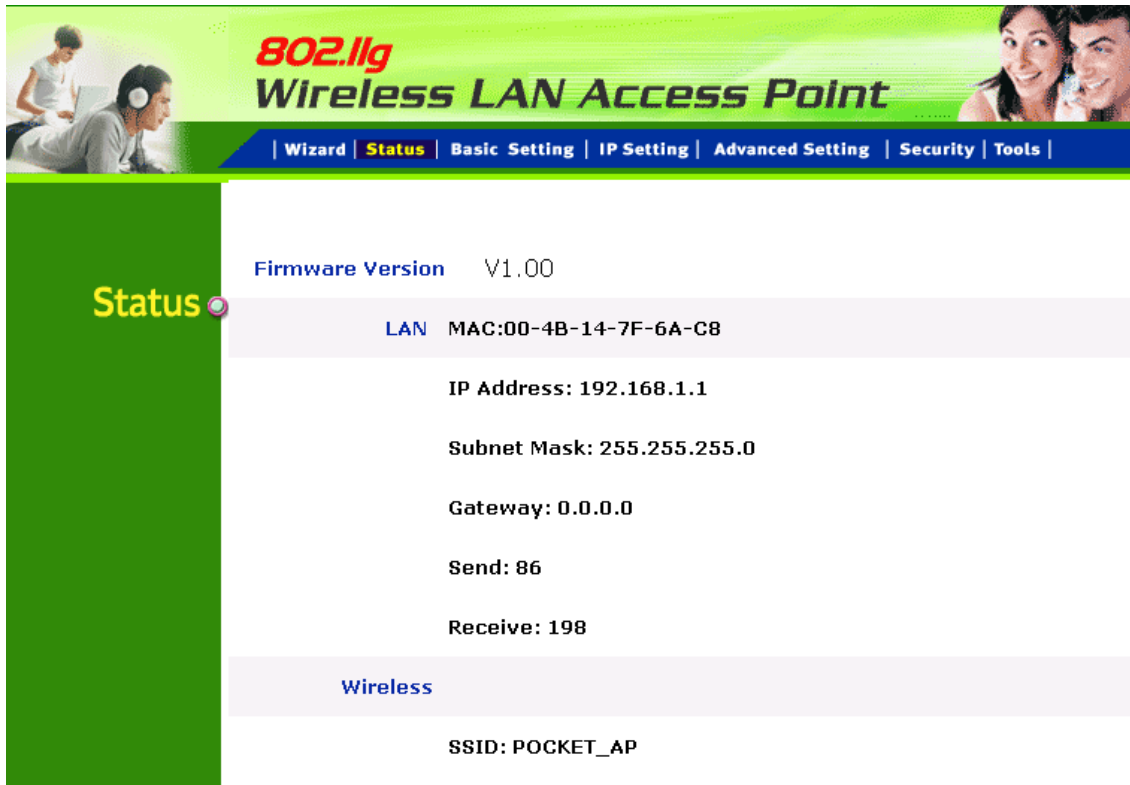


The screenshot shows the '802.11g Wireless Lan Access Point Site Survey' setup wizard. The title bar is green with white text. Below the title bar, the text 'Setup Completed' is displayed in blue. Below this, there is a grey instruction box: 'The Access Point setup is now completed. If you want to change any setup[settings], click Back to go back to the previous pages. Click Restart to reboot the Access Point for the new settings to take effect.' At the bottom, there are three buttons: 'back' (with a blue circular arrow icon), 'restart' (with a green circular arrow icon), and 'exit' (with a purple arrow pointing out of a box icon).

3. Configuration Access Point through WEB Browser

3.1 Status

This page as below shows the following information.



The screenshot displays the web interface of an 802.11g Wireless LAN Access Point. The header features the product name and a navigation menu with options: Wizard, Status (highlighted), Basic Setting, IP Setting, Advanced Setting, Security, and Tools. A green sidebar on the left contains the word 'Status' with a circular icon. The main content area shows the following information:

Firmware Version		V1.00
LAN	MAC:00-4B-14-7F-6A-C8	
	IP Address: 192.168.1.1	
	Subnet Mask: 255.255.255.0	
	Gateway: 0.0.0.0	
	Send: 86	
	Receive: 198	
Wireless		
	SSID: POCKET_AP	

Firmware Version: Shows the current firmware version.

LAN: Shows the Mac address, IP address (default: 192.168.1.1), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current ESSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

View Log: Once clicked, the page will change to login page. The login page records every event and the time that it happens.



[View Log](#)

[First Page](#)[Last Page](#)[Previous Page](#)[Next Page](#)[Clear Log](#)[Refresh](#)

Time	Message
Jul/27/2004 11:14:20	System started
Jul/27/2004 11:14:20	SSID = default CHANNEL = 06

User may clear the entries recorded in the log by clicking the “**Clear Log**” button, and refresh the screen to show the latest log entries by clicking the “**Refresh**” button.

3.2 Basic Setting

This is the page allow user to change the access point settings.

802.11g Wireless LAN Access Point

| Wizard | Status | **Basic Setting** | IP Setting | Advanced Setting | Security | Tools |

Basic Setting

AP Name:

SSID:

Channel: (Domain:ETSI)

Authentication: ☒ Open System ☐ Shared Key ☐ WPA-PSK

WEP Key: ☒ Disable ☐ 64bits ☐ 128bits

Mode:

☒ 1.

☐ 2.

☐ 3.

AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Channel: The channel that AP will operate in. User can select the channel range from 1 to 11 for North America (FCC) domain, 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Authentication Type: The authentication type default is set to open system. There are three options: open system; shared key; and WPA-PSK. User may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

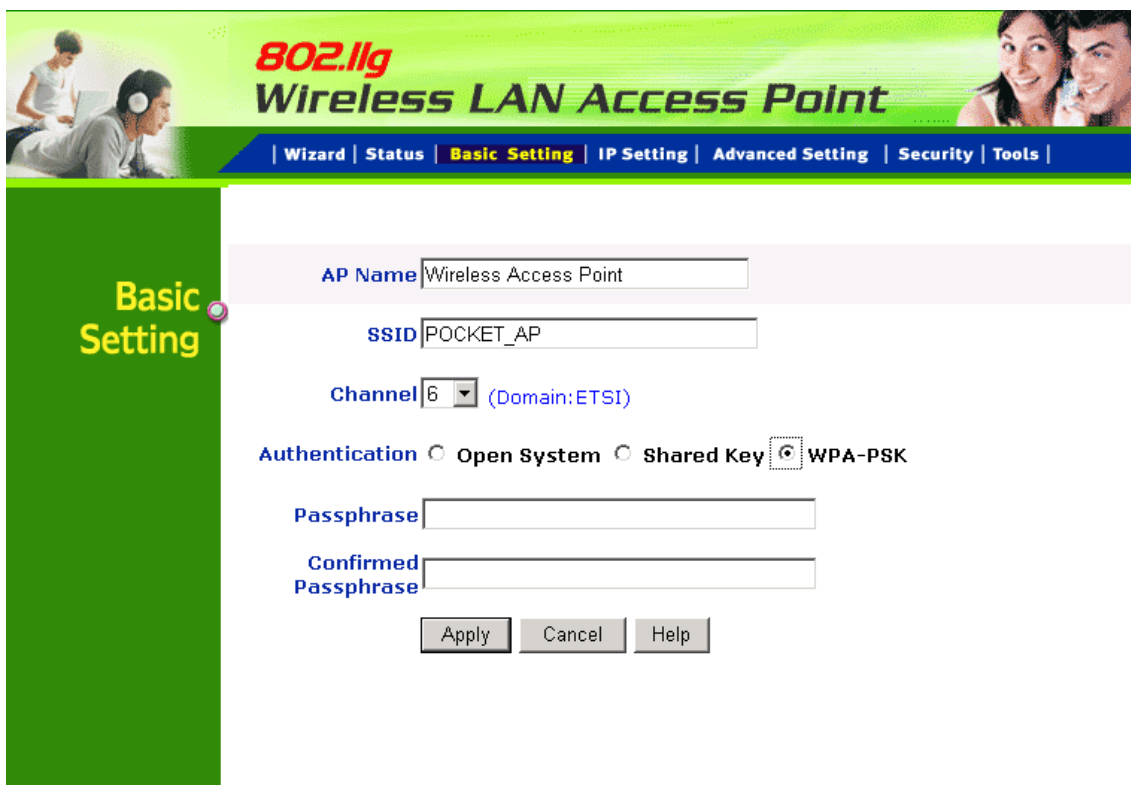
WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is

selected, the key value must be entered in ASCII or HEX format.

Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.

Apply: For the changes made to any of the items above to be effective, click “**Apply**”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

If **WPA-PSK** is enabled, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



The screenshot shows the configuration interface for an 802.11g Wireless LAN Access Point. The top banner features the text "802.11g Wireless LAN Access Point" and a navigation menu with links: Wizard, Status, Basic Setting (highlighted), IP Setting, Advanced Setting, Security, and Tools. On the left, a green sidebar contains the text "Basic Setting" with a circular icon. The main content area is a light gray form with the following fields and options:

- AP Name:** A text input field containing "Wireless Access Point".
- SSID:** A text input field containing "POCKET_AP".
- Channel:** A dropdown menu showing "6" with the text "(Domain:ETSI)" to its right.
- Authentication:** A group of radio buttons with labels: "Open System", "Shared Key", and "WPA-PSK". The "WPA-PSK" option is selected.
- Passphrase:** A text input field.
- Confirmed Passphrase:** A text input field.
- Buttons:** Three buttons labeled "Apply", "Cancel", and "Help" are located at the bottom of the form.

Note: Once **WPA-PSK** function enables, it will take some time to make the setting active.

3.3 IP Setting

This page allows user to configure the IP and DHCP settings of the Access Point.

The screenshot shows the configuration interface for an 802.11g Wireless LAN Access Point. The top banner features the product name and a navigation menu with links: Wizard, Status, Basic Setting, IP Setting (highlighted), Advanced Setting, Security, and Tools. On the left, a green sidebar contains the text 'IP Setting' with a circular icon. The main content area is divided into sections for LAN IP and DHCP Server settings.

LAN IP ☐ Obtain IP Automatically

☒ Fixed IP

Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

Gateway 0 . 0 . 0 . 0

DHCP Server ☐ On

☒ Off

IP Range From 192 . 168 . 1 . 100 to 192 . 168 . 1 . 199

DNS Server 0 . 0 . 0 . 0

Buttons: Apply, Cancel, Help

The default IP address of this access point is 192.168.1.1 with the subnet mask of 255.255.255.0. User can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

User can also set the Access Point to obtain the IP from a DHCP server, **but it is not recommended**. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server: It is not recommended to enable the DHCP Server if user has a DHCP server running in LAN network because it probably will cause possible the conflict of IP assignment. Enable the DHCP server function by selecting the option “On”, and enter the IP range. **IP range** : When user set the IP range that Client can get the IP in the range.

Click “**Apply**” for the changes to be effective.

DNS server: If User’s local Ethernet support DNS function, user can fix the DNS address in the space.

3.4 Advanced Setting

This page contains configurations for advanced users, which the change reflects the wireless performance and operating modes.

802.11g Wireless LAN Access Point

| Wizard | Status | Basic Setting | IP Setting | **Advanced Setting** | Security | Tools |

Advanced Setting

Beacon Interval (msec, range: 1~1000, default:100)

RTS Threshold (range: 256~2432, default:2432)

Fragmentation Threshold (range: 256~2346, default:2346, even number only)

DTIM Interval (range: 1~255, default:3)

SSID broadcast ☒ Enable ☐ Disable

Mode Setting ☐ G Mode ☒ Mix Mode

TX Rates (Mbps)

Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2346 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients

hear the beacons and awaken to receive the broadcast and multicast messages.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For secure purpose, user may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point.

Mode setting : 1) G mode- Only support 11g client to connect!

2) Mix mode- Support 11b&11g client to connect!

TX Rates: User also can fix the transmission at specific data rate, if choose “Auto” data rate, the Wireless Ethernet Adapter will change the data rate to have the best receive or transmit quality

3.5 Security

This page is where user configures the security features supported by this Access Point.

The screenshot shows the configuration interface for an 802.11g Wireless LAN Access Point. The top banner features the text "802.11g Wireless LAN Access Point" and a navigation menu with links: Wizard, Status, Basic Setting, IP Setting, Advanced Setting, Security (highlighted), and Tools. On the left, a green sidebar contains the word "Security" with a lock icon. The main content area is divided into two sections. The first section, titled "Password", contains fields for "Administrator id:" (with "admin" entered), "AP Password New:" (masked with dots), and "Confirm:" (masked with dots). Below these fields are "Apply", "Cancel", and "Help" buttons. The second section, titled "MAC Filter", has two radio buttons: "Enabled" and "Disabled" (which is selected). Below the radio buttons, there are two options: "Only deny PCs with MAC listed below to access device" (selected) and "Only allow PCs with MAC listed below to access device". A dropdown menu shows "1~10". Below this, there are seven rows of MAC address input fields, labeled "MAC 1" through "MAC 7". Each row consists of six individual input boxes separated by hyphens.

Password: Allow user to change the new login password. Here are the necessary steps:

1. Enter the new password in the “**AP Password New:**” field.
2. Enter the new password again in the “**Confirm**” field.
3. Click “**Apply**”

MAC Filter: MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the “**Enabled**” radio box, select one of two choices:

- Only deny PCs with MAC listed below to access device
- Only allow PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. User can browse through the MAC address saved by selecting the drop-down box.

For any changes made in the security page, click “**Apply**” for the changes to be effective.

3.6 Tools

Four functions are provided in this page, Backup, Restore Settings, Restore default settings and Firmware Upgrade.



Backup Settings: Click on “**Backup**” button, which will open a FileSave Dialog

box, where user gets to save all the current settings and configurations to a file.

Restore Settings: Click on the “**Browse**” button to open a FileOpen Dialog box, where user gets to select the file, which saves previous settings and configurations. Upon selecting the saved file, click “**Restore**” and complete the restore process when the access point re-operates after it restarts.

Restore to default settings: Click on “**Default**” button to restore the access point back to its manufacture default settings.

Firmware Upgrade: Click on the “**Browse**” button to open a FileOpen Dialog box, where gets to select the firmware file, which download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates after it restarts.

4. Getting Start with Wireless Ethernet Adapter

4.1 Know the Wireless Ethernet Adapter

Ports:

- Power Receptor
- Reset Button
- RJ-45 Ethernet Port

Cross-over cable is required to connect to computer directly

LEDs:

- Power LED: ON when the unit is powered up
- LAN LED: ON indicates LAN connection; BLINK indicates LAN activity
- WLAN LED: ON indicates WLAN is working; BLINK indicates wireless activity.

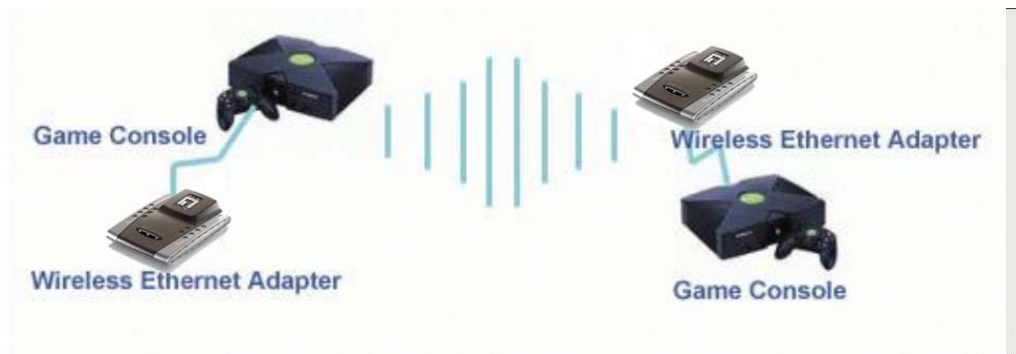
4.2 Connect to the Wireless Ethernet Adapter

This wireless Ethernet adapter transforms the Ethernet-enabled devices to have the wireless function. The wireless Ethernet adapter enables wireless communication over network. There are two examples shown as the below.


Infrastructure Mode:



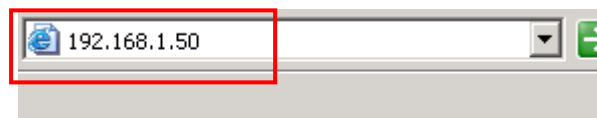
Ad-Hoc Mode:



4.2.1 Access the Setting Menu

 Before installation, please set the IP address of your broadband router as 192.168.1.XXX. XXX can be from 1 to 254, but not including 50. And set the TCP/IP of your operating computer to “obtain IP address automatically”.

User could start to access the configuration menu anytime by opening a web browser window by typing the IP address of this access point. The default IP is **192.168.1.50**.



The below window will popup. Please enter the user name and password. Both of the default is “admin”.



Now, the main menu screen is popup.



The image shows a web-based status screen for an 802.11g Wireless LAN Ethernet Adapter. The interface has a green header with the product name and a navigation bar. A green sidebar on the left contains the word 'Status' in yellow. The main content area displays network configuration details for both LAN and Wireless interfaces.

802.11g Wireless LAN Ethernet Adapter

| Wizard | **Status** | Basic Setting | IP Setting | Advanced Setting | Security | Tools |

Status

Firmware Version V1.00

LAN MAC:00-4B-14-7F-6A-C8

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 66

Receive: 1104


Wireless

SSID: Sales

Encryption Function : Disabled



4.2.2 Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get Access Point configuration ready to run in 4 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.




Welcome to the **54Mbps** Access Point Setup Wizard. The Wizard will direct you through these four quick steps. Start by clicking on **Next**.

- Step 1. Set your new password
- Step 2. Set the SSID and Channel
- Step 3. Set Encryption
- Step 4. Restart

Step 1: Set Password

User can change the password and then click “**Next**” to continue.






Set Password

You may want to change the Administrator password of this Access Point to prevent authorized modification to the configuration settings. Enter your new password in the following text fields. Click Next to continue with setup or Exit to quit setup wizard.

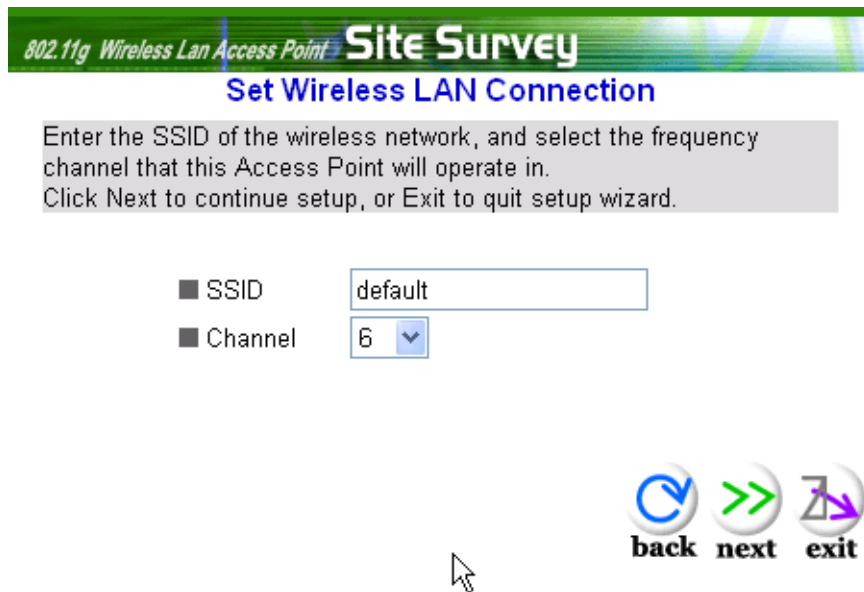
■ Password

■ Verify Password

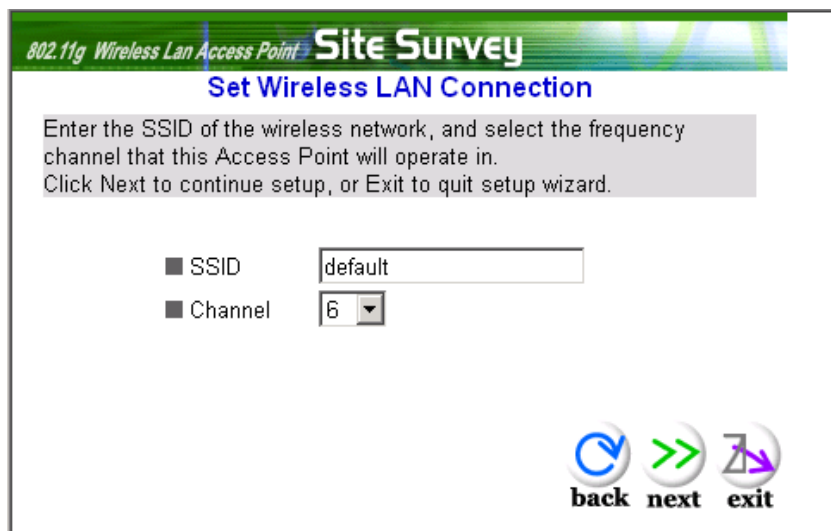
Step2: Set WLAN Connection

Please type the name of SSID and select the channel. Click “**Next**” to continue.



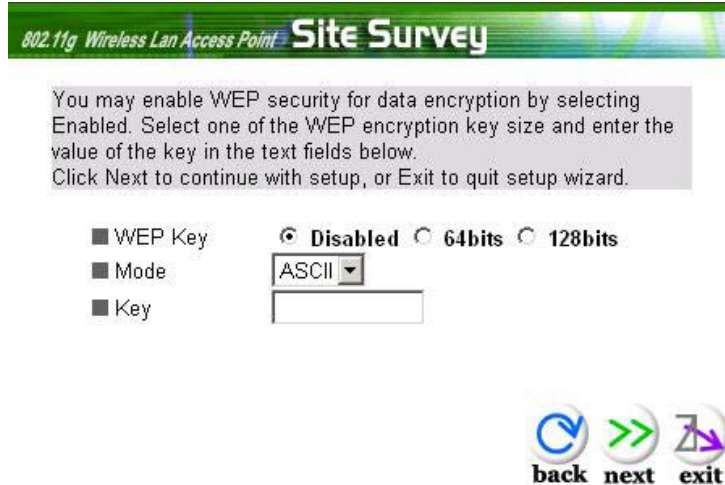
Step 3: Set Wireless LAN Connection

IF user doesn't want to use “default” as the SSID, user can change SSID here. Also user can choose different channel to avoid noise coming from other wireless networking devices. Please click “**Next**” to continue.



Step 4: Set WEP Encryption

If user wants to enable WEP, please click **“Enabled”**. Then, select the key size of WEP encryption and enter the key value in the key text box. Click **“Next”** to continue.






802.11g Wireless Lan Access Point Site Survey

You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below. Click Next to continue with setup, or Exit to quit setup wizard.

☒ WEP Key ☒ Disabled ☐ 64bits ☐ 128bits

☐ Mode ASCII

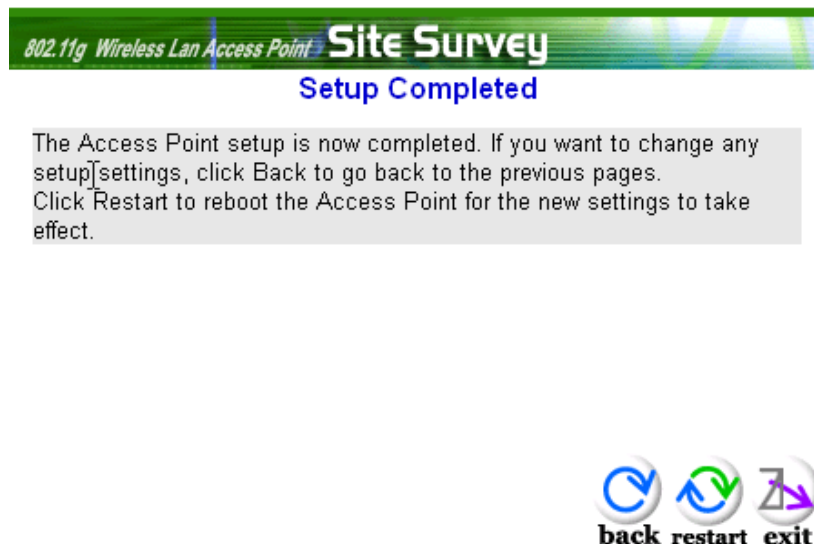
☐ Key

back next exit

Step 5: Restart




The Setup wizard is now completed. The new settings will be effective after the Access Point restarted. Please click **“Restart”** to reboot the Access Point. If user does not want to make any changes, please click **“exit”** to quit without any changes. User also can go back to modify the setting by clicking **“Back”**.



802.11g Wireless Lan Access Point Site Survey

Setup Completed

The Access Point setup is now completed. If you want to change any setup settings, click Back to go back to the previous pages. Click Restart to reboot the Access Point for the new settings to take effect.

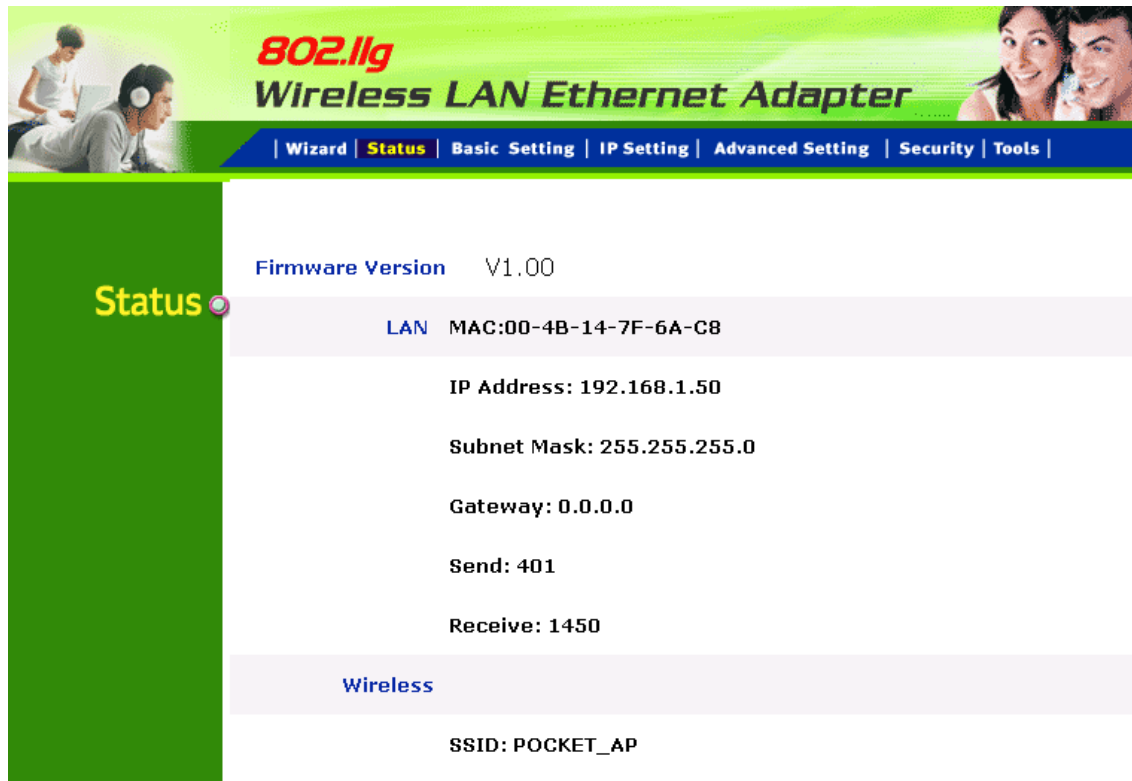
  

back restart exit

5. Configuration Wireless Ethernet Adapter through WEB Browser

5.1 Status

This page as below shows the following information.



Firmware Version: Shows the current firmware version.

LAN: Shows the Mac address, IP address (default: 192.168.1.50), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current ESSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

View Log: Upon clicked, the page will change to log page. The log page records every event and the time that it happens.



[View Log](#)

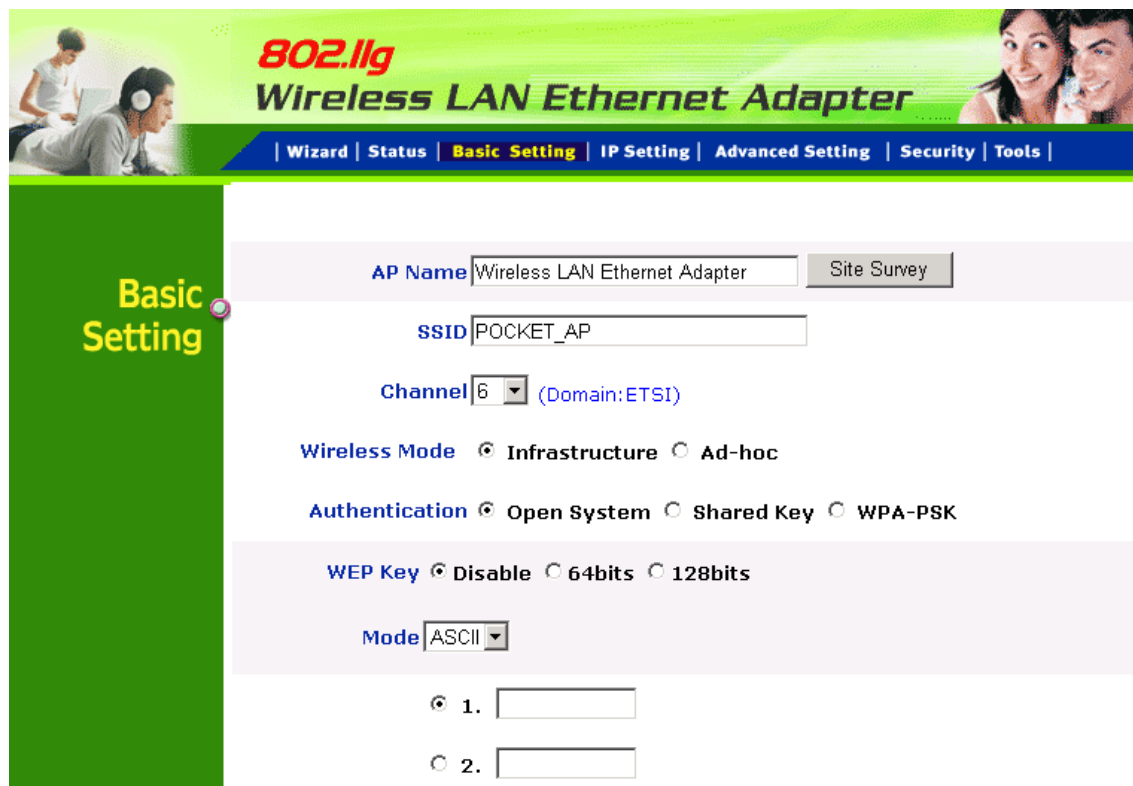
[First Page](#)[Last Page](#)[Previous Page](#)[Next Page](#)[Clear Log](#)[Refresh](#)

Time	Message
Jul/28/2004 11:25:26	System started
Jul/28/2004 11:25:26	SSID = POCKET_AP CHANNEL = 06

User may clear the entries recorded in the log by clicking the “**Clear Log**” button, and refresh the screen to show the latest log entries by clicking “**Refresh**” button.

5.2 Basic Setting

This is the page allow to change the settings of access point.



802.11g Wireless LAN Ethernet Adapter

| Wizard | Status | **Basic Setting** | IP Setting | Advanced Setting | Security | Tools |

Basic Setting

AP Name: Wireless LAN Ethernet Adapter

SSID: POCKET_AP

Channel: 6 (Domain:ETSI)

Wireless Mode: ☒ Infrastructure ☐ Ad-hoc

Authentication: ☒ Open System ☐ Shared Key ☐ WPA-PSK

WEP Key: ☒ Disable ☐ 64bits ☐ 128bits

Mode: ASCII

☒ 1.

☐ 2.

AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Channel: The channel that AP will operate in. User can select the channel range of 1 to 11 for North America (FCC) domain, 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

Wireless Mode: There are two modes for this option, one is infrastructure, and the other is Ad-hoc.

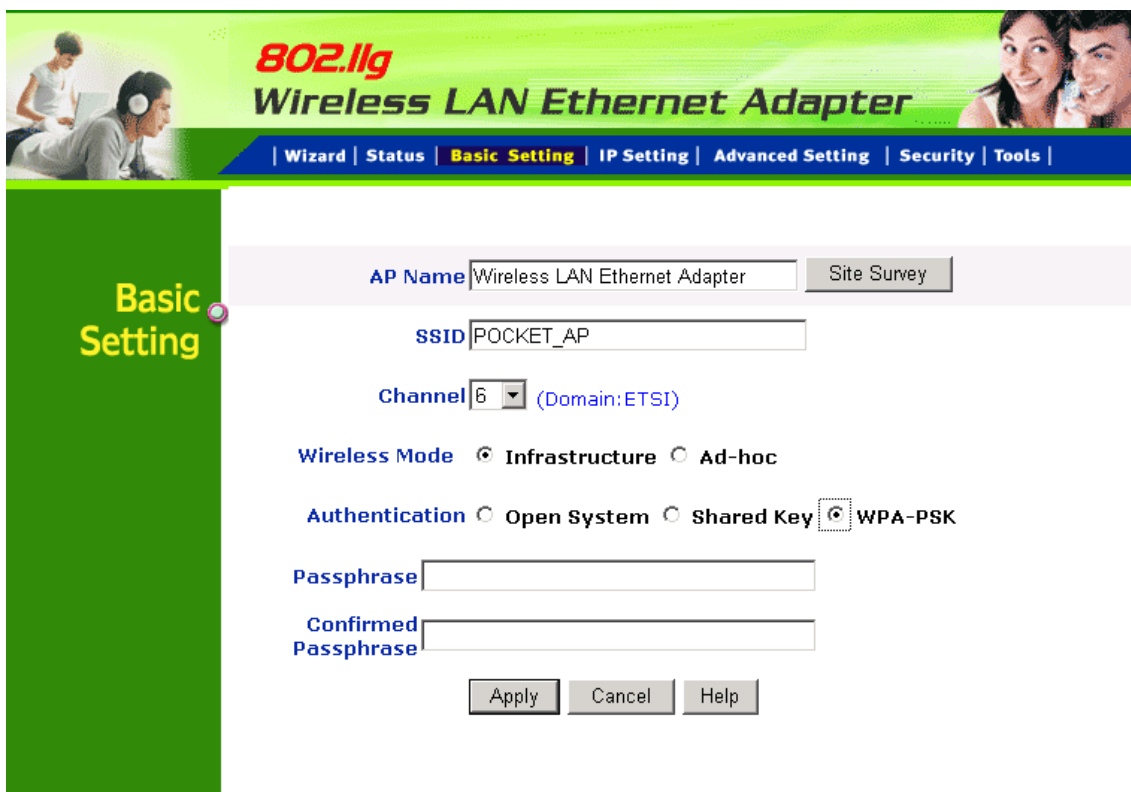
Authentication Type: The authentication type default is set to open system. There are three options: open system; shared key; and WPA-PSK. User may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: To disable WEP security, click on the “**Disable**” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.

Apply: For the changes made to any of the items above to be effective, click “**Apply**”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

If **WPA-PSK** is enabled, users need to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



The screenshot shows the configuration interface for a wireless LAN adapter. The top banner features the text "802.11g Wireless LAN Ethernet Adapter" and a navigation bar with links: Wizard, Status, Basic Setting (highlighted), IP Setting, Advanced Setting, Security, and Tools. On the left, a green sidebar contains the text "Basic Setting". The main content area includes the following fields and options:

- AP Name:** Wireless LAN Ethernet Adapter (with a "Site Survey" button next to it)
- SSID:** POCKET_AP
- Channel:** 6 (with a dropdown arrow and "(Domain:ETSI)" text)
- Wireless Mode:** Infrastructure (selected with a radio button), Ad-hoc
- Authentication:** Open System, Shared Key, WPA-PSK (selected with a radio button)
- Passphrase:** (empty text field)
- Confirmed Passphrase:** (empty text field)
- Buttons:** Apply, Cancel, Help

Note: Once **WPA-PSK** function enables, it will take some time to make the setting active.

5.3 IP Setting

This page allows users to configure the IP and DHCP settings of the Access Point.

802.11g Wireless LAN Ethernet Adapter

| Wizard | Status | Basic Setting | **IP Setting** | Advanced Setting | Security | Tools |

IP Setting

LAN IP ☒ Obtain IP Automatically

☒ Fixed IP

Address . . .

Subnet Mask . . .

Gateway . . .

The default IP address of this Wireless Ethernet Adapter is 192.168.1.50 with the subnet mask of 255.255.255.0. User can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

User can also set the Wireless Ethernet Adapter to obtain the IP from a DHCP server, but it is not recommended. Select the option “**Obtain IP Automatically**” and click “**Apply**” button for the changes to be effective.



It is not recommended that setting the Wireless Ethernet Adapter to “Obtain IP Automatically”. Unless you are fully aware of your network environment, and can trace the IP address of your Ethernet Adapter from your broadband router.

5.4 Advanced Setting

This page contains configurations for advanced users, which the change reflects the wireless performance and operating modes.

802.11g Wireless LAN Ethernet Adapter

| Wizard | Status | Basic Setting | IP Setting | **Advanced Setting** | Security | Tools |

Advanced Setting

Beacon Interval (msec, range: 1~1000, default: 100)

RTS Threshold (range: 256~2432, default: 2432)

Fragmentation Threshold (range: 256~2346, default: 2346, even number only)

DTIM Interval (range: 1~255, default: 3)

Preamble Type ☐ Short Preamble ☒ Long Preamble

TX Rates (Mbps)

Apply Cancel Help

Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2346 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients hear the beacons and awaken to receive the broadcast and multicast messages.

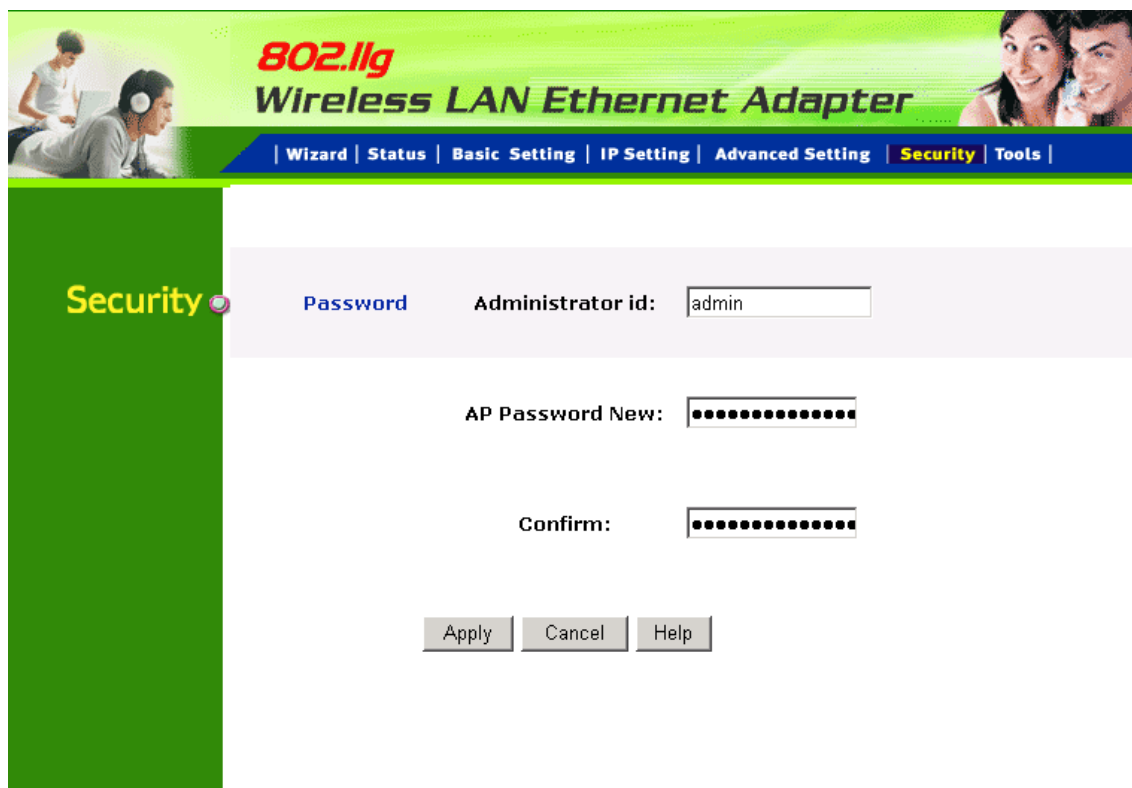
Preamble: Select **Long** or **Short** Preamble type. Preamble is a sequence of bits transmitted at 1Mbps that allows the PHY circuitry to reach steady-state demodulation and synchronization of bit clock and frame start. Two different

preambles and headers are defined: the mandatory supported Long Preamble and header, which interoperates with the 1 Mbit/s and 2 Mbit/s DSSS specification (as described in IEEE Std 802.11), and an optional Short Preamble and header (as described in IEEE Std 802.11b). At the receiver, the Preamble and header are processed to aid in demodulation and delivery of the PSDU. The Short Preamble and header may be used to minimize overhead and, thus, maximize the network data throughput. However, the Short Preamble is supported only from the IEEE 802.11b (High- Rate) standard and not from the original IEEE 802.11. That means that stations using Short-Preamble cannot communicate with stations implementing the original version of the protocol

TX Rates: User also can fix the transmission at specific data rate, if choose “Auto” data rate, the Wireless Ethernet Adapter will change the data rate to have the best receive or transmit quality.

5.5 Security

This page is where configures the security features supported by Access Point Client.



802.11g
Wireless LAN Ethernet Adapter

| Wizard | Status | Basic Setting | IP Setting | Advanced Setting | **Security** | Tools |

Security

Password

Administrator id:

AP Password New:

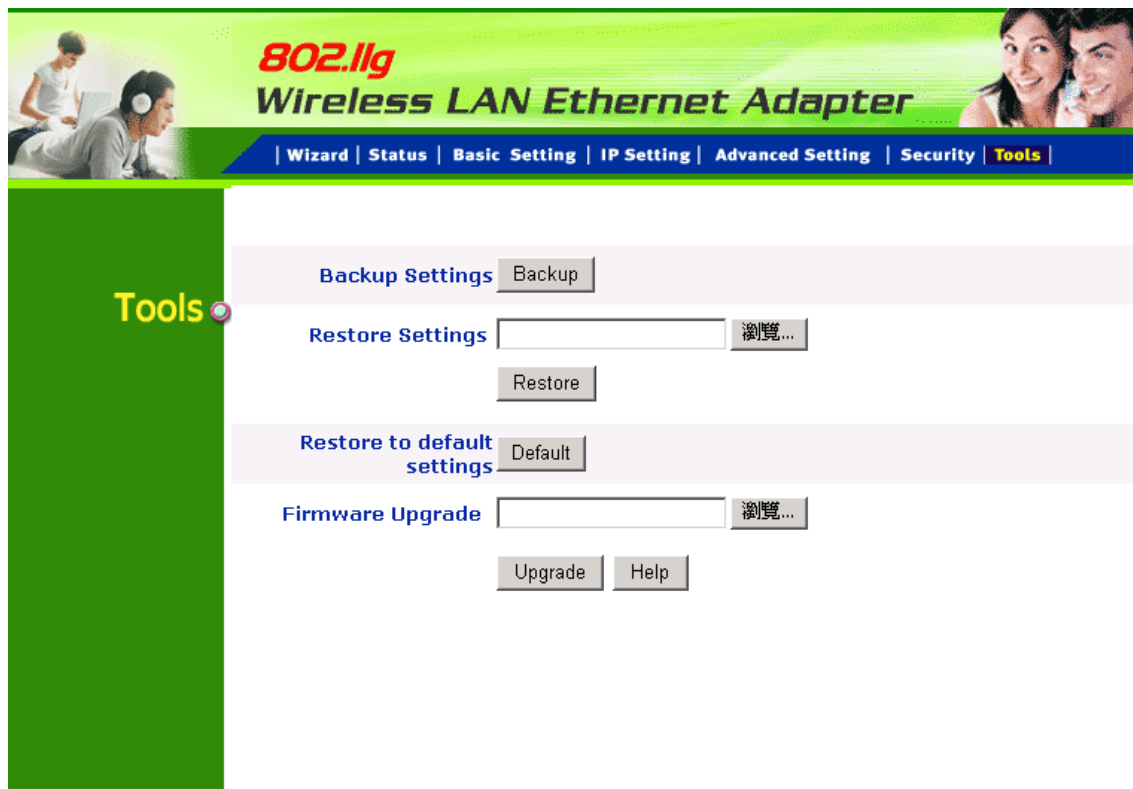
Confirm:

Password: Allow to change the new login password. Here are the necessary steps:

1. Enter the new password in the “**AP Password New:**” field.
2. Enter the new password again in the “**Confirm**” field.
3. Click “**Apply**”

5.6 Tools

Four functions are provided in this page, Backup, Restore Settings, Restore default settings and Firmware Upgrade.



Backup Settings: Click on “**Backup**” button, which will open a FileSave Dialog box, where gets to save all the current settings and configurations to a file.

Restore Settings: Click on the “**Browse**” button to open a FileOpen Dialog box, where gets to select the file, which saves previous settings and configurations. Upon selecting the saved file, click “**Restore**” and complete the restore process when the access point re-operates after it restarts.

Restore to default settings: Click on “**Default**” button to restore the access point back to its manufacture default settings.

Firmware Upgrade: Click on the “**Browse**” button to open a FileOpen Dialog

box, where get to select the firmware file, which download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates after it restarts.

6. Getting Start with Wireless Router

6.1 Know the 802.11g Wireless Router

Ports:

- Power Receptor
- Reset Button
- RJ-45 Ethernet Port
Cross-over cable is required to connect to computer directly
- There is no visual LAN port for Pocket AP.

LEDs:

- Power LED: ON when the unit is powered up
- LAN LED: ON indicates LAN connection; BLINK indicates LAN activity
- WLAN LED: ON indicates WLAN is working; BLINK indicates wireless activity.

6.2 Connect to the 802.11g Wireless Router

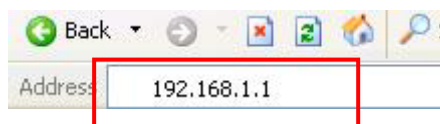


Before installation, please set the TCP/IP of your operating computer to “obtain IP address automatically”.

6.2.1 Access the Setting Menu

User could start to access the configuration menu anytime by opening a web browser window by typing the IP address of this wireless router. The default IP is 192.168.1.1.

Note: to configure the settings must through the wireless connection, instead of RJ45 cable.

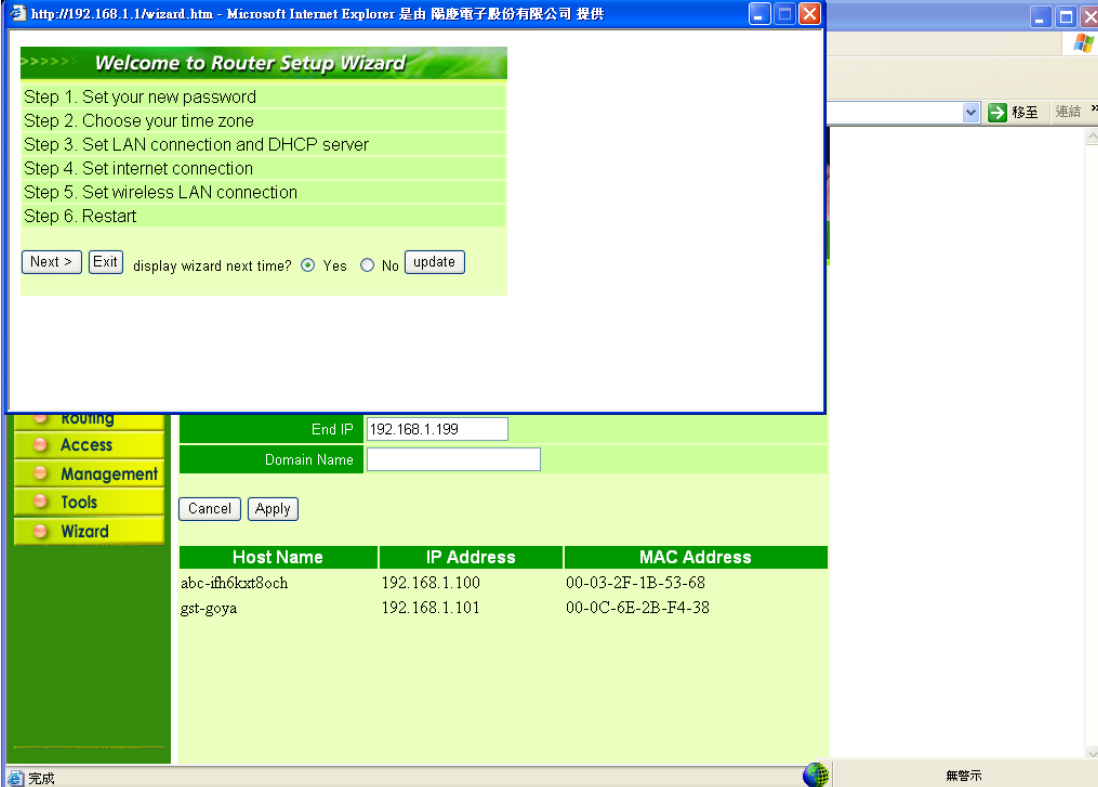


The below window will popup. Please enter the user name and password. Both of the default is “admin”.



A login window titled "Connect to 192.168.1.1" with a blue header and a yellow body. It features a "Wireless LAN Router" section with a "User name:" field containing "admin" and a "Password:" field with masked characters. A "Remember my password" checkbox is below the password field. "OK" and "Cancel" buttons are at the bottom.

Now, the main menu screen is popup.



A screenshot of a web browser showing the "Welcome to Router Setup Wizard" page. The page lists six steps: 1. Set your new password, 2. Choose your time zone, 3. Set LAN connection and DHCP server, 4. Set internet connection, 5. Set wireless LAN connection, and 6. Restart. Below the steps are "Next >", "Exit", and "display wizard next time?" options with "Yes" and "No" radio buttons and an "update" button. A sidebar on the left contains a menu with "Routing", "Access", "Management", "Tools", and "Wizard". The main content area shows "End IP" as 192.168.1.199 and a "Domain Name" field. Below this is a table with columns "Host Name", "IP Address", and "MAC Address".

Host Name	IP Address	MAC Address
abc-ifn6kxt8och	192.168.1.100	00-03-2F-1B-53-68
gst-goya	192.168.1.101	00-0C-6E-2B-F4-38

6.2.2 Quick Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get wireless router configuration ready to run in 6 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.



The screenshot shows the 'Welcome to Router Setup Wizard' window. It has a green header bar with the title. Below the header, there is a list of six steps: Step 1. Set your new password, Step 2. Choose your time zone, Step 3. Set LAN connection and DHCP server, Step 4. Set internet connection, Step 5. Set wireless LAN connection, and Step 6. Restart. At the bottom, there are two buttons: 'Next >' and 'Exit'. To the right of these buttons is a label 'display wizard next time?' followed by two radio buttons: 'Yes' (which is selected) and 'No'. To the right of the radio buttons is an 'update' button.

>>>>> **Welcome to Router Setup Wizard**

Step 1. Set your new password
Step 2. Choose your time zone
Step 3. Set LAN connection and DHCP server
Step 4. Set internet connection
Step 5. Set wireless LAN connection
Step 6. Restart

display wizard next time? ☒ Yes ☐ No

Step 1: Set new Password

User can change the password and then click “**Next**” to continue.



The screenshot shows the 'Set Password' window. It has a green header bar with the title. Below the header, there is a title 'Set Password' in blue. There are two text input fields: 'Password' and 'Verify Password'. Both fields are filled with black dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Exit'.

>>>>> **Welcome to Router Setup Wizard**

Set Password

Password

Verify Password

Step2: Choose time zone

Select properly time zone from the drop down list. Please click “**Next**” to continue.



>>>>> **Welcome to Router Setup Wizard**

Choose Time Zone

(GMT-08:00) Pacific Time (US & Canada) ▼

< Back Next > Exit

Step 3: Set LAN connection and DHCP server

Set IP address and mask. The default IP is 192.168.1.1. If user likes to enable DHCP, please click “**Enabled**”. DHCP enabled is able to automatically assign IP addresses. Please assign the range of IP addresses in the fields of “**Range start**” and “**Range end**”. Please click “**Next**” to continue.



>>>>> **Welcome to Router Setup Wizard**

Set LAN & DHCP Server

LAN IP Address 192.168.1.1

LAN Subnet Mask 255.255.255.0

DHCP Server ☒ Enable ☐ Disable

Range Start 192.168.1.100

Range End 192.168.1.199

< Back Next > Exit

Step 4: Set Internet connection

Select how the router will set up the Internet connection: Obtained IP automatically; Fixed IP address; PPPoE to obtain IP automatically; PPPoE with a fixed IP address; PPTP.

Obtain IP automatically (DHCP client):

If user wants to enable DHCP server, choose "**Obtain IP automatically (DHCP client)**" to have the router assign IP addresses automatically.



Fixed IP Address:



If Fixed IP address is assigned, the below screen will pop up. Please set the WAN address and DNS server.

>>>>>> **Welcome to Router Setup Wizard**

Set Fixed IP Address

WAN IP Address	<input type="text" value="0.0.0.0"/>
WAN Subnet Mask	<input type="text" value="0.0.0.0"/>
WAN Gateway Address	<input type="text" value="0.0.0.0"/>
DNS Server Address 1	<input type="text" value="0.0.0.0"/>
DNS Server Address 2	<input type="text" value="0.0.0.0"/>
DNS Server Address 3	<input type="text" value="0.0.0.0"/>

PPPoE to obtain IP automatically:

>>>>>> **Welcome to Router Setup Wizard**

Select Internet Connection Type

☐ Obtain IP automatically (DHCP client)

☐ Fixed IP address

☒ PPPoE to obtain IP automatically

☐ PPPoE with a fixed IP address

☐ PPTP

>>>>> **Welcome to Router Setup Wizard**

Set PPPoE to obtain IP automatically

User Name	<input type="text"/>
Password	<input type="password"/>
Verify Password	<input type="password"/>

PPPoE with a fixed IP address:

>>>>> **Welcome to Router Setup Wizard**

Select Internet Connection Type

☐ Obtain IP automatically (DHCP client)

☐ Fixed IP address

☐ PPPoE to obtain IP automatically

☒ PPPoE with a fixed IP address

☐ PPTP

>>>>> **Welcome to Router Setup Wizard**

Set PPPoe with a fixed IP Address

User Name

Password

Verify Password

IP Address

PPTP:

>>>>>> **Welcome to Router Setup Wizard**

Select Internet Connection Type

☐ Obtain IP automatically (DHCP client)

☐ Fixed IP address

☐ PPPoE to obtain IP automatically

☐ PPPoE with a fixed IP address

☒ PPTP

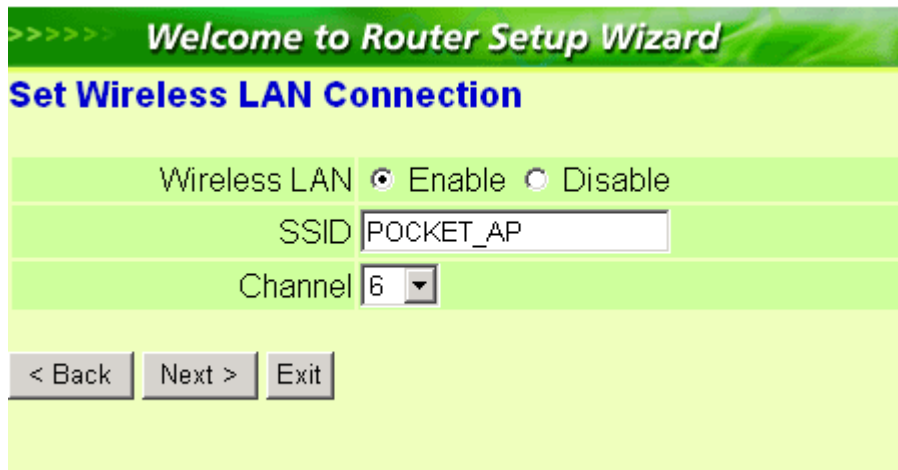
>>>>>> **Welcome to Router Setup Wizard**

Set PPTP Client

My IP	0.0.0.0
Subnet Mask	0.0.0.0
GateWay	0.0.0.0
Server IP	0.0.0.0
PPTP Account	
PPTP Password
Retype Password

Step 5: Set Wireless LAN connection

Click “**enable**” to enable wireless LAN. If user enables the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.



The screenshot shows a web-based setup wizard with a green header bar containing the text '>>>>> Welcome to Router Setup Wizard'. Below the header, the title 'Set Wireless LAN Connection' is displayed in blue. The main content area has a light green background and contains three rows of settings: 'Wireless LAN' with radio buttons for 'Enable' (selected) and 'Disable'; 'SSID' with a text box containing 'POCKET_AP'; and 'Channel' with a dropdown menu showing '6'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Exit'.

Step 6: Restart

The Setup wizard is now completed. The new settings will be effective after the Wireless router restarted. Please click “**Restart**” to reboot the router. If user does not want to make any changes, please click “**exit**” to quit without any changes. User also can go back to modify the setting by clicking “**Back**”.



The screenshot shows the final screen of the setup wizard. The green header bar contains the text '>>>>> Welcome to Router Setup Wizard'. Below the header, the title 'Setup Completed' is displayed in blue. The main content area has a light green background and contains a message: 'Click "Restart" button to save the settings and restart Wireless Router.' At the bottom, there are three buttons: '< Back', 'Restart', and 'Exit'.

7. Configuration Wireless Router through WEB Browser

7.1 LAN Setting

The screen leads to configure the LAN & DHCP Server, set WAN parameters, create Administrator and User passwords, and set the local time, time zone, and dynamic DNS.

7.1.1 LAN & DHCP Server

This page enables to set LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.

The screenshot shows the configuration interface for a wireless router. The title bar reads "802.11g Wireless Broadband Router". Below the title bar, there are navigation tabs: "LAN&DHCP server", "WAN", "Password", and "Time". A "HELP" button is also present. On the left side, there is a vertical menu with buttons: "Main", "Wireless", "Status", "Routing", "Access", "Management", "Tools", and "Wizard". The main content area contains the following fields:

Host Name	Wireless LAN Router
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Start IP	192.168.1.100
End IP	192.168.1.199
Domain Name	

Below the fields are "Cancel" and "Apply" buttons. At the bottom, there is a table with the following headers:

Host Name	IP Address	MAC Address
-----------	------------	-------------

Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "AP-Router."

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default

subnet mask is 255.255.255.0.

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Domain Name: Type the local domain name of the network in the text box. This item is optional.

7.1.2 WAN

This screen leads to set up the router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.

802.11g Wireless Broadband Router

► LAN&DHCP server ► **WAN** ► Password ► Time **HELP**

Main
Wireless
Status
Routing
Access
Management
Tools
Wizard

Connection Type: DHCP Client or Fixed IP ▼

☒ Obtain IP Automatically
☐ Specify IP

WAN IP

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0

DNS 1: 0.0.0.0
DNS 2: 0.0.0.0
DNS 3: 0.0.0.0

MAC Address: 00 - 0D - 88 - C0 - F9 - 54 **Clone MAC Address**

Cancel Apply

Connection Type: Select the connection type, either DHCP client, Fixed IP or

PPPoE from the drop-down list.

WAN IP: Select whether to specify an IP address manually, or DHCP to obtain an IP address automatically. When “**Specify IP**” is selected, type the IP address, subnet mask, and default gateway in the text boxes. ISP will provide this information.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. ISP will provide this information.

MAC Address: If required by ISP, type the MAC address of the router WAN interface in this field.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. ISP will provide this information.

7.1.3 Password

This screen leads to set administrative and user passwords. These passwords are used to gain access to the router interface.

802.11g
Wireless Broadband Router

► LAN&DHCP server ► WAN ► Password ► Time

HELP

Main
Wireless
Status
Routing
Access
Management
Tools
Wizard

Administrator(The login name is "admin")

New Password:

Confirm Password:

User(The login name is "user")

New Password:

Confirm Password:

Cancel Apply

Administrator: Type the password the Administrator will use to log in to the system. The password must be typed again for confirmation.

7.1.4 Time

This screen leads to set the time and date for the router's real-time clock, select properly time zone, and enable or disable daylight saving.

The screenshot shows the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the router's name and a navigation bar with links: LAN&DHCP server, WAN, Password, and Time. A sidebar on the left contains a menu with icons and labels: Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area is titled 'Time' and contains the following settings:

- Local Time:** Apr/01/2002 00:40:18
- Time Zone:** (GMT-08:00) Pacific Time (US & Canada) (selected from a dropdown)
- Default NTP server:** (empty text field)
- Set the time:** Year 2002, Month Apr, Day 01, Hour 00, Minute 40, Second 18. A 'Set Time' button is present.
- Daylight Saving:** Enabled (radio button), Disabled (radio button, selected). Start Jan 01, End Jan 01.

At the bottom of the configuration area are 'Cancel' and 'Apply' buttons.

Local Time: Displays the local time and date.

Time Zone: Select properly time zone from the drop-down list.

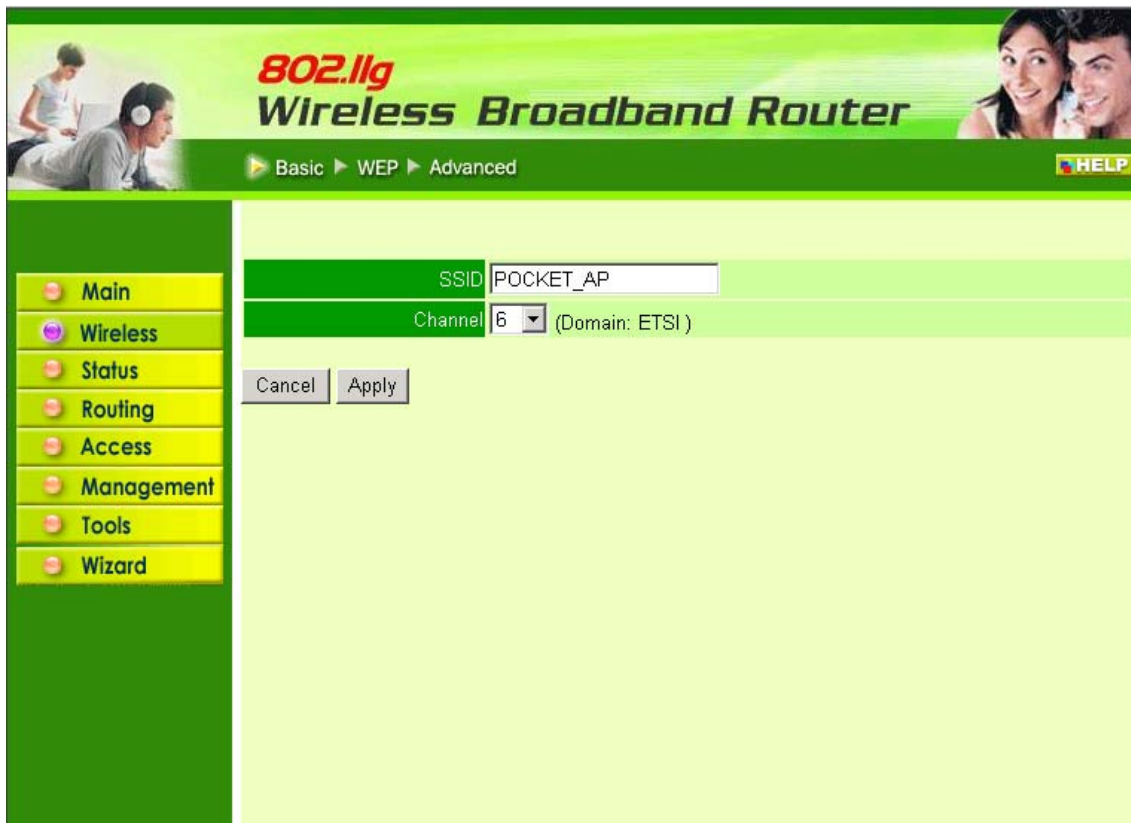
Daylight Saving: Enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

7.2 Wireless

This section leads to set wireless communications parameters for the router's wireless LAN feature.

7.2.1 Basic

This page allow to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.



The screenshot shows the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the text "802.11g Wireless Broadband Router" and a "HELP" button. Below the banner, a navigation bar includes "Basic", "WEP", and "Advanced" tabs, with "Basic" being the active tab. On the left, a vertical menu lists various configuration options: Main, Wireless (highlighted), Status, Routing, Access, Management, Tools, and Wizard. The main content area displays the "Wireless" settings. It includes a text box for "SSID" containing "POCKET_AP" and a dropdown menu for "Channel" set to "6" (Domain: ETSI). Below these fields are "Cancel" and "Apply" buttons.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

7.2.2 WEP

This screen leads to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications.

Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key. This router also supports WPA-PSK.

802.11g
Wireless Broadband Router

Basic WEP Advanced

HELP

Main
Wireless
Status
Routing
Access
Management
Tools
Wizard

Authentication Type ☒ Open System ☐ Shared Key ☐ WPA-PSK

WEP ☐ Enabled ☒ Disabled

Mode HEX

WEP Key 64-bit

Key1 ☒ 0000000000

Key 2 ☐ 0000000000

Key 3 ☐ 0000000000

Key 4 ☐ 0000000000

Cancel Apply Clear

Authentication Type: The authentication type default is set to open system. There are three options: Open System; Shared Key and WPA-PSK..

WEP: Enable or Disabled. This is to make WEP enabled or disabled.

Mode: Select the key mode in ASCII or HEX

WEP Key: Select the level of encryption from the drop-down list. The router supports, 64- and 128-bit encryption.

Key 1 ~ Key 4: Create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select which key user wants to use by clicking the radio button next to the key. Click “**Clear**” to erase key values. Click “**Apply**” button for the changes to be effective.

If **WPA-PSK** is selected, please set the PSK key in the pass phrase field. The length should be 8 characters at least.



The screenshot displays the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the text "802.11g Wireless Broadband Router" and a "HELP" button. Below the banner, a navigation bar includes "Basic", "WEP", and "Advanced" tabs. A left-hand menu lists various configuration options: Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area is titled "Authentication Type" and shows three radio button options: "Open System", "Shared Key", and "WPA-PSK". The "WPA-PSK" option is selected. Below these options are two text input fields labeled "Passphrase" and "Confirmed Passphrase". At the bottom of the configuration area are three buttons: "Cancel", "Apply", and "Clear".

Note: Once **WPA-PSK** function enables, it will take some time to make the setting active.

7.2.3 Advanced

This screen leads to configure advanced wireless functions.

The screenshot shows the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the text "802.11g Wireless Broadband Router" and navigation links for "Basic", "WEP", and "Advanced" (which is selected). A "HELP" button is also present. On the left, a sidebar contains icons and labels for "Main", "Wireless", "Status", "Routing", "Access", "Management", "Tools", and "Wizard". The main configuration area contains the following settings:

Beacon Interval	100	(default: 100 msec, range: 1~1000)
RTS Threshold	2432	(default: 2432, range: 256~2432)
Fragmentation Threshold	2346	(default: 2346, range: 256~2346, even number only)
DTIM Interval	3	(default: 3, range: 1~255)
TX Rates (Mbps)	Auto	
SSID Broadcast	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	

At the bottom of the configuration area are "Cancel" and "Apply" buttons.

Beacon Interval: Type the beacon interval in the text box. User can specify a value from 1 to 1000. The default beacon interval is 100.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2432 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 256 and 2432 until packet transfer rates are minimized. (**NOTE:** *set this fragmentation threshold value may diminish system performance.*)

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. User can specify a value between 1 and 65535. The default value is 3.

TX Rates (Mbps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

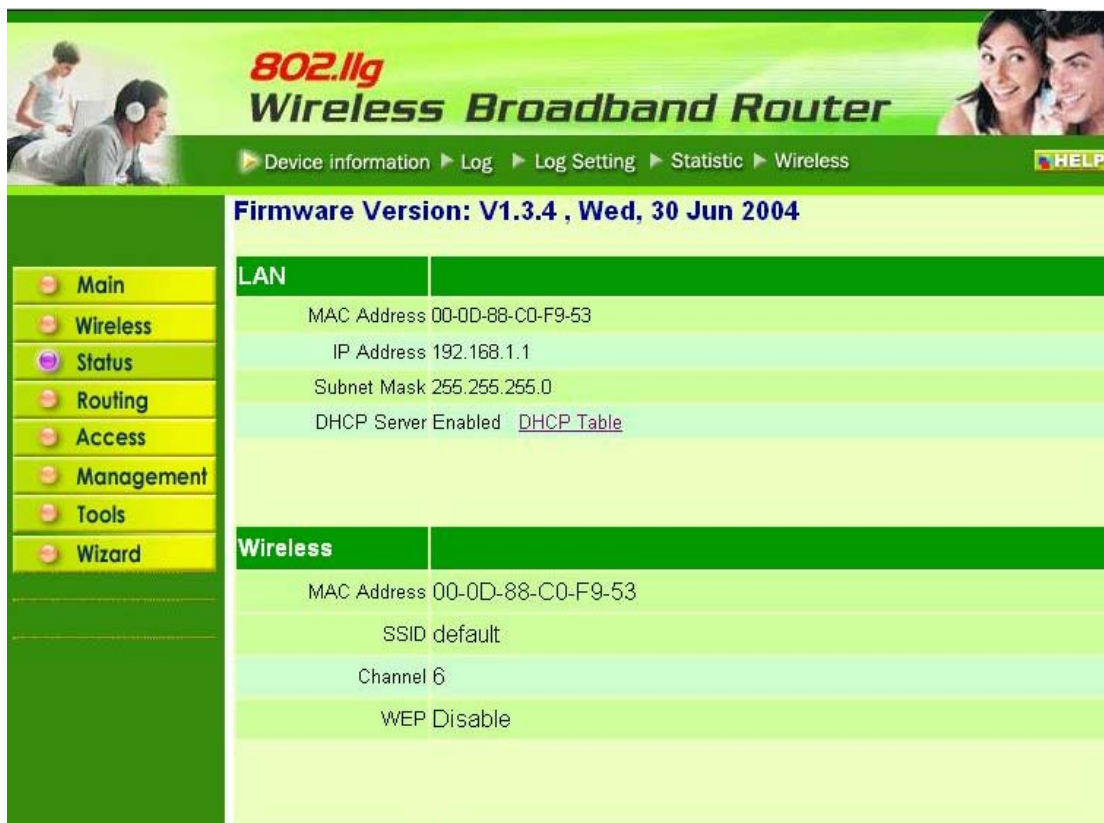
SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For secure purpose, user may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point

7.3 Status

This selection leads to view the status of the router LAN and Wireless connections, and view logs and statistics pertaining to connections and packet transfers.

7.3.1 Device Information

This screen leads to view the router LAN and Wireless configuration.



Firmware Version: Displays the latest build of the router firmware interface.

After updating the firmware in Tools - Firmware, check this to ensure that firmware was successfully updated.

LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click "**DHCP Table**" to view a list of client stations currently connected to the router LAN interface.

Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether WEP is enabled or not.

7.3.2 Log

This screen leads to view a running log of router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click **“First Page”** to view the first page of the log

Click **“Last Page”** to view the final page of the log

Click **“Previous Page”** to view the page just before the current page

Click **“Next Page”** to view the page just after the current page

Click **“Clear Log”** to delete the contents of the log and begin a new log

Click **“Refresh”** to renew log statistics



The screenshot shows the web interface of an 802.11g Wireless Broadband Router. The header includes the router model and navigation links: Device information, Log, Log Setting, Statistic, and Wireless. A left sidebar contains menu items: Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area displays log controls (First Page, Last Page, Previous Page, Next Page, Clear Log, Refresh) and a table of log entries.

Time	Message	Source	Destination	Note
Apr/01/2002 00:49:06	DHCP Discover			
Apr/01/2002 00:49:02	DHCP Discover			
Apr/01/2002 00:49:01	DHCP Discover no response			
Apr/01/2002 00:49:00	DHCP Discover			
Apr/01/2002 00:48:27	DHCP Discover			
Apr/01/2002 00:48:11	DHCP Discover			
Apr/01/2002 00:48:05	DHCP lease IP 192.168.1.100 to work			00-0D-88-A2-16-BD
Apr/01/2002	DHCP Discover			

Time: Displays the time and date that the log entry was created.

Message: Displays summary information about the log entry.

Source: Displays the source of the communication.

Destination: Displays the destination of the communication.

Note: Displays the IP address of the communication

7.3.3 Log Setting

This screen leads to set router logging parameters.

The screenshot shows the 'Log Setting' page of an 802.11g Wireless Broadband Router. The interface is green-themed. At the top, there's a banner with the router model and a navigation bar with links: Device information, Log, Log Setting (active), Statistic, and Wireless. A 'HELP' button is also present. On the left, a sidebar lists menu items: Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area contains the following fields and options:

- SMTP Server:** A text input field.
- Send to:** A text input field for the email address, followed by an 'Email Log Now' button.
- Syslog Server:** A text input field containing '0.0.0.0'.
- Log Type:** A section with four checkboxes:
 - ☒ System Activity
 - ☒ Attacks
 - ☐ Dropped Packets
 - ☒ Notice
- Buttons:** 'Cancel' and 'Apply' buttons at the bottom.

SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.

Send to: Type an email address for the log to be sent to. Click “**Email Log Now**” to immediately send the current log.

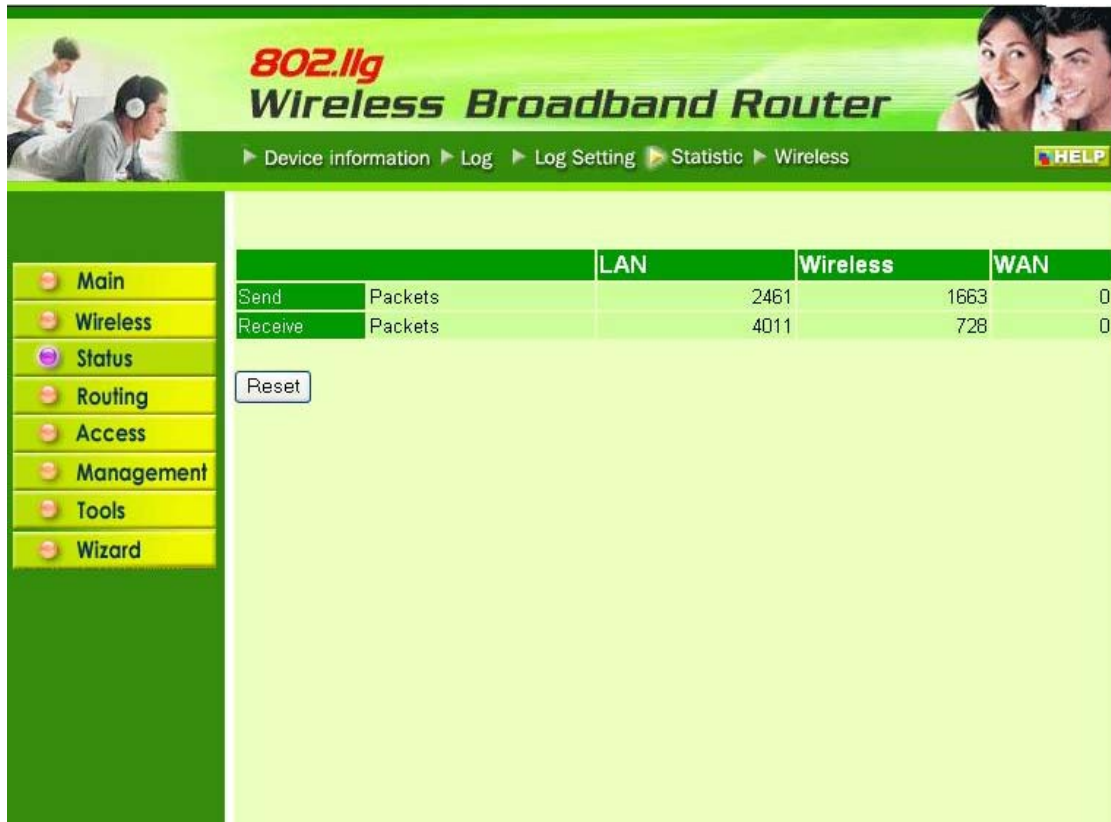
Syslog Server: Type the IP address of the Syslog Server if user wants the router to listen and receive incoming Syslog messages.

Log Type: Select what items will be included in the log:

- **System Activity:** Displays information related to router operation.
- **Debug Information:** Displays information related to errors and system malfunction.
- **Attacks:** Displays information about any malicious activity on the network.
- **Dropped Packets:** Displays information about packets that have not been transferred successfully.
- **Notice:** Displays important notices by the system administrator.

7.3.4 Statistic

This screen displays a table that shows the rate of packet transmission via the router LAN and WAN ports (in bytes per second).



802.11g Wireless Broadband Router

► Device information ► Log ► Log Setting ► **Statistic** ► Wireless **HELP**

		LAN	Wireless	WAN
Send	Packets	2461	1663	0
Receive	Packets	4011	728	0

Click “**Reset**” to erase all statistics and begin logging statistics again.

7.3.5 Wireless

This screen leads to view information about wireless devices that are connected to the wireless router.



Connected Time: How long the wireless device has been connected to the LAN via the router?

MAC Address: Displays the devices wireless LAN interface MAC address.

7.4 Routing

This selection leads to set how the router forwards data: Static and Dynamic. Routing Table enables user to view the information created by the router that displays the network interconnection topology.

7.4.1 Static

It enables user to set parameters by which the router forwards data to its destination if network has a static IP address.

The screenshot shows the configuration interface for a router. The header includes the brand name '802.11g Wireless Broadband Router' and navigation tabs for 'Static', 'Dynamic', and 'Routing Table'. A sidebar on the left contains a menu with options: Main, Wireless, Status, Routing (highlighted), Access, Management, Tools, and Wizard. The main content area has input fields for 'Network Address', 'Network Mask', 'Gateway Address', 'Interface' (a dropdown menu currently showing 'LAN'), and 'Metric'. Below these fields are buttons for 'Add', 'Update', 'Delete', and 'New'. At the bottom, there is a table with the following headers: 'Network Address', 'Mask', 'Gateway', 'Interface', and 'Metric'.

Network Address	Mask	Gateway	Interface	Metric
-----------------	------	---------	-----------	--------

Network Address: Type the static IP address which network uses to access the Internet. ISP or network administrator provides this information.

Network Mask: Type the network (subnet) mask for network. If user does not type a value here, the network mask defaults to 255.255.255.255. ISP or network administrator provides this information.

Gateway Address: Type the gateway address for network. ISP or network administrator provides this information.

Interface: Select which interface, WAN or LAN, used to connect to the Internet.

Metric: Select which metric to apply to this configuration.

Add: Click to add the configuration to the static IP address table at the bottom of

the page.

Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click “**Update**” to confirm the changes.

Delete: Select one of the entries in the static IP address table at the bottom of the page and click “**Delete**” to remove the entry.

New: Click “**New**” to clear the text boxes and add required information to create a new entry.

7.4.2 Dynamic

This screen leads to set NAT parameters.

The screenshot shows the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the text "802.11g Wireless Broadband Router" and a "HELP" button. Below the banner, there are three tabs: "Static", "Dynamic" (which is selected), and "Routing Table". On the left side, there is a vertical menu with buttons for "Main", "Wireless", "Status", "Routing" (which is highlighted), "Access", "Management", "Tools", and "Wizard". The main content area displays three rows of settings, each with a label and two radio buttons: "NAT" with "Enabled" and "Disabled" options; "Transmit" with "Disabled", "RIP 1", and "RIP 2" options; and "Receive" with "Disabled", "RIP 1", and "RIP 2" options. At the bottom of the settings area, there are "Cancel" and "Apply" buttons.

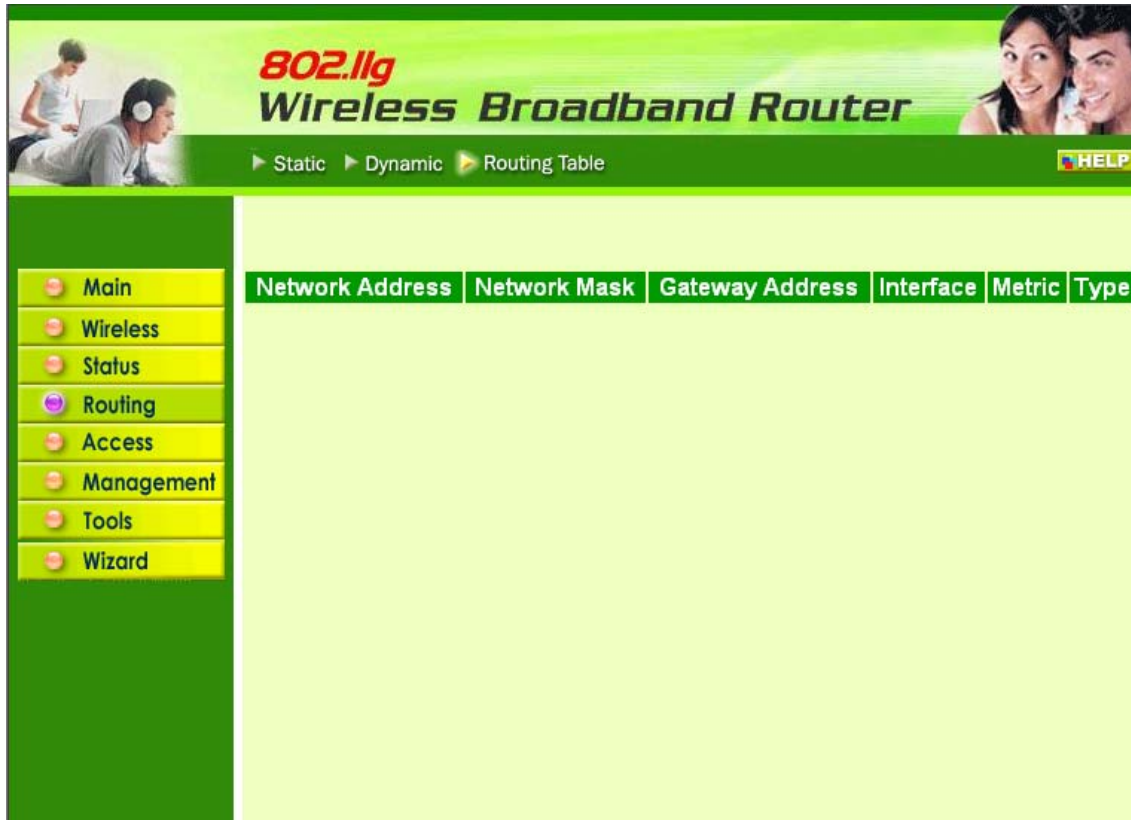
NAT: Click the radio buttons to enable or disable NAT.

Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2

7.4.3 Routing Table

This screen leads to view the routing table for the router. The routing table is a database created by the router that displays the network interconnection topology.



Network Address: Displays the network IP address of the connected node.

Network Mask: Displays the network (subnet) mask of the connected node.

Gateway Address: Displays the gateway address of the connected node.

Interface: Displays whether the node is connected via a WAN or LAN.

Metric: Displays the metric of the connected node.

Type: Displays whether the node has a static or dynamic IP address

7.5 Access

This page leads to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

7.5.1 MAC Filters

Allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to “**Disabled**” to disable the MAC filter.

802.11g Wireless Broadband Router

Mac Filter ▶ Protocol Filter ▶ IP filter ▶ Virtual Server ▶ Special AP ▶ DMZ ▶ Firewall Rule **HELP**

MAC Filter

☒ Disabled MAC Filters

☐ Only **allow** computers with MAC address listed below to access the network

☐ Only **deny** computers with MAC address listed below to access the network

Apply

MAC Table

Name

MAC Address - - - - -

Add Update Delete Clear

Name	MAC Address	Connection
------	-------------	------------

Disable: Once the function of MAC filter is disabled, those listed in the MAC Table are allowed Internet access.

Enable: All users are allowed Internet access except those users in the MAC Table are deny Internet access.

MAC Table: Use this section to create a user profile which Internet access is denied or allowed. The user profiles are listed in the table at the bottom of the page. (**Note:** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which user edited.)

Name: Type the name of the user to be permitted/denied access.

MAC Address: Type the MAC address of the user's network interface.

Add: Click to add the user to the list at the bottom of the page.

Update: Click to update information for the user, if user has changed any of the fields.

Delete: Select a user from the table at the bottom of the list and click “**Delete**” to

remove the user profile.

New: Click “New” to erase all fields and enter new information.

7.5.2 Protocol Filter

This screen leads to allow and deny access based upon a communications protocol list which has been created. The protocol filter profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user edited:

The screenshot shows the configuration interface for a 802.11g Wireless Broadband Router. The top navigation bar includes links for Mac Filter, Protocol Filter (selected), IP filter, Virtual Server, Special AP, DMZ, Firewall Rule, and a HELP button. A left sidebar contains a menu with options: Main, Wireless, Status, Routing, Access (highlighted), Management, Tools, and Wizard. The main content area is titled 'Protocol Filter' and contains the following elements:

- Radio buttons for 'Disable List' and 'Enable List'. The 'Enable List' option is selected, with the text 'Deny to access internet from LAN.' below it.
- An 'Apply' button.
- A section titled 'Edit protocol Filter in List' containing:
 - Enable status: 'Enable' (selected) and 'Disabled' radio buttons.
 - Name: A text input field.
 - Protocol: A dropdown menu currently set to 'TCP'.
 - Port Range: Two text input fields separated by a hyphen, with a note '(Type Range for ICMP)'.
- Buttons for 'Add', 'Update', 'Delete', and 'New'.
- A table listing existing protocol filters:

	Name	Protocol	Range
<input type="checkbox"/>	Filter FTP	TCP	20-21
<input type="checkbox"/>	Filter HTTP	TCP	80
<input type="checkbox"/>	Filter HTTPS	TCP	443
<input type="checkbox"/>	Filter SMTP	TCP	25

7.5.3 IP Filter

This screen leads to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access. The IP filter profiles are listed in the table at the bottom of the page. (**Note:** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which user edited.)

802.11g Wireless Broadband Router

Mac Filter Protocol Filter **IP filter** Virtual Server Special AP DMZ Firewall Rule **HELP**

Main Wireless Status Routing **Access** Management Tools Wizard

Enable ☐ Enable ☐ Disabled

Range Start

Range End

Add Update Delete Clear

Start	End

Enable: Click to enable or disable the IP address filter.

Range Start: Type the minimum address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

Range End: Type the minimum address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.

Add: Click to add the IP range to the table at the bottom of the screen.

Update: Click to update information for the range if user has selected a list item and have made changes.

Delete: Select a list item and click “**Delete**” to remove the item from the list.

New: Click “**New**” to erase all fields and enter new information.

7.5.4 Virtual Server

This screen leads to create a virtual server via the router. If the router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user edited.

802.11g
Wireless Broadband Router

Mac Filter Protocol Filter IP filter **Virtual Server** Special AP DMZ Firewall Rule **HELP**

Enable ☐ Enable ☐ Disabled

Name

Protocol

Private Port

Public Port

LAN Server

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTP	TCP 80/80	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	IPSec	UDP 500/500	0.0.0.0

Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select the protocol (TCP or UDP) used for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

Add: Click to add the virtual server to the table at the bottom of the screen.

Update: Click to update information for the virtual server if user has selected a list item and have made changes.

Delete: Select a list item and click “**Delete**” to remove the item from the list.

New: Click “**New**” to erase all fields and enter new information.

7.5.5 Special AP

This screen leads to specify special applications, such as games, that require multiple connections that are inhibited by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user edited.

	Name	Trigger Port Range	Incoming Port
<input type="checkbox"/>	Battle.net	6112	6112
<input type="checkbox"/>	Dialpad	7175	51200-51201,51210
<input type="checkbox"/>	ICU II	2019	2000-2038,2050-2051,2069,2085,3010-3030
<input type="checkbox"/>	MSN Gaming Zone	47624	2300-2400,28800-29000
<input type="checkbox"/>	PC-to-Phone	12053	12120,12122,24150-24220
<input type="checkbox"/>	Quick Time 4	554	6970-6999

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router WAN connection. Click Disabled on a profile to prevent users from accessing the application on the WAN.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used to access the application.
- **Port Range:** Type the port range that can be used to access the application in the text

boxes.

Incoming: Defines which incoming communications users are permitted to connect with.

- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.
- **Port:** Type the port number that can be used for the incoming communication.

Add: Click to add the special application profile to the table at the bottom of the screen.

Update: Click to update information for the special application if user has selected a list item and have made changes.

Delete: Select a list item and click “**Delete**” to remove the item from the list.

New: Click “**New**” to erase all fields and enter new information.

7.5.6 DMZ

This screen leads to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.

Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.

The screenshot shows the configuration interface for an 802.11g Wireless Broadband Router. The top banner features the router's name and a navigation bar with links: Mac Filter, Protocol Filter, IP filter, Virtual Server, Special AP, DMZ (highlighted), Firewall Rule, and a HELP button. On the left is a vertical menu with buttons for Main, Wireless, Status, Routing, Access (highlighted), Management, Tools, and Wizard. The main content area is titled 'DMZ' and contains an 'Enable' section with radio buttons for 'Enabled' (selected) and 'Disabled'. Below this is a text field for 'DMZ Host IP' with the value '0.0.0.0'. An 'Apply' button is located at the bottom right of the form. A small red 'X' icon is visible in the bottom left corner of the interface.

Enable: Click to enable or disable the DMZ.

DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Apply: Click to save the settings.

7.5.7 Firewall Rule

This screen leads to set up the firewall. The router provides basic firewall functions, by filtering all the packets that enter the router using a set of rules. The rules are in an order sequence list--the lower the rule number, the higher the priority the rule has.

Action	Timeout	Name	Source	Destination	Protocol
<input checked="" type="checkbox"/> Allow	300	Allow to Ping WAN port	WAN,*	LAN,192.168.1.1	ICMP,8
<input checked="" type="checkbox"/> Deny	300	Default	*,*	LAN,*,	IP (0),*
<input checked="" type="checkbox"/> Allow	300	Default	LAN,*,	*,*	IP (0),*

Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Inactive Timeout: Type the number of seconds of network inactivity that elapses before the router refuses the incoming packet.

Source: Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.

- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if user has selected a list item and have made changes.

Delete: Select a list item and click “**Delete**” to remove the item from the list.

New: Click “**New**” to erase all fields and enter new information.

Priority Up: Select a rule from the list and click “**Priority Up**” to increase the priority of the rule.

Priority Down: Select a rule from the list and click “**Priority Down**” to decrease the priority of the rule.

Update Priority: After increasing or decreasing the priority of a rule, click “**Update Priority**” to save the changes.

7.6 Management

Management leads to set up Remote Management feature.

7.6.1 Remote Management

This screen leads to set up remote management. Using remote management, the router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.

The screenshot shows the 'Remote Management' configuration page for an 802.11g Wireless Broadband Router. The page has a green header with the router's name and a 'Remote Management' title. A sidebar on the left contains navigation links: Main, Wireless, Status, Routing, Access, Management (selected), Tools, and Wizard. The main content area is divided into two sections: 'HTTP' and 'Allow to Ping WAN Port'. The 'HTTP' section has a 'port' field set to 8080 and a 'Remote IP Range' field with 'From' and 'To' sub-fields. The 'Allow to Ping WAN Port' section has a 'Remote IP Range' field with 'From' and 'To' sub-fields. Below these are two rows of radio buttons: 'UPNP Enable' (Enabled/Disabled) and 'Gaming mode' (Enabled/Disabled). At the bottom are 'Cancel' and 'Apply' buttons.

Section	Field	Value / Options
HTTP	port	8080
	Remote IP Range	From * [] To []
Allow to Ping WAN Port	Remote IP Range	From * [] To []
	UPNP Enable	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	Gaming mode	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Buttons: Cancel, Apply

HTTP: Set up HTTP access for remote management.

Allow to Ping WAN Port: Type a range of router IP addresses that can be pinged from remote locations

UPNP: UPNP is short for Universal Plug and Play that is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The Router is an UPnP enabled router and will only work with other UPnP devices/software. If user does not want to use the UPnP functionality, it can be disabled by selecting "**Disabled**".

GAMING MODE: If user is experiencing difficulties when playing online games or even certain applications that use voice data, user may need to enable

Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode is disabled.

7.7 Tools

This page leads to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure router settings, upgrade the firmware, and ping remote IP addresses.

7.7.1 Restart

Click “**Restar**”^t to restart the system in the event the system is not performing correctly.



7.7.2 Settings

This screen leads to save settings as a profile and load profiles for different circumstances. User can also load the factory default settings, and run a setup wizard to configure the router and router interface.

The screenshot shows the web interface of an 802.11g Wireless Broadband Router. The header features the brand name '802.11g Wireless Broadband Router' and navigation links: 'Restart', 'Settings', 'Firmware', and 'Ping test'. A 'HELP' button is also present. On the left, a sidebar menu lists various settings categories: Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area is titled 'VPN Pass-Through' and includes a description: 'Allows VPN connections to pass through.' Below this, there are two rows of radio buttons for 'PPTP' and 'IPSec', each with 'Enabled' and 'Disabled' options. An 'Apply' button is located below these options. The next section is 'Save Settings', which contains a 'Save' button. Following this is the 'Load Settings' section, which includes a text input field, a 'Browse...' button, and a 'Load' button. The final section is 'Restore Factory Default Settings', which contains a 'Restore' button.

VPN Pass-Through: Choose enable or disable on the PPTP or IPSec.

Save Settings: Click to save the current configuration as a profile that user can load when necessary.

Load Settings: Click “**Browse**” and go to the location of a stored profile. Click “**Load**” to load the profile's settings.

Restore Factory Default Settings: Click to restore the default settings. All configuration changes user has made will be lost.

7.7.3 Firmware

This screen leads to keep the router firmware up to date.



Please follow the below instructions:

1. Download the latest firmware from the manufacturer's Web site, and save it to disk.
2. Click "**Browse**" and go to the location of the downloaded firmware file. Select the file and click "**Upgrade**" to update the firmware to the latest release

7.7.4 Ping Test

The ping test is to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click “**Ping**” to start testing.



The screenshot displays the web interface of an 802.11g Wireless Broadband Router. The header features the product name "802.11g Wireless Broadband Router" in a stylized font, accompanied by images of a person using a laptop and a smiling couple. Below the header, a navigation bar includes links for "Restart", "Settings", "Firmware", and "Ping test", along with a "HELP" button. On the left side, a vertical menu lists various configuration options: "Main", "Wireless", "Status", "Routing", "Access", "Management", "Tools", and "Wizard". The main content area is titled "Host Name or IP address:" and contains a text input field and a "Ping" button.

Glossary

Access Point: An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc: An independent wireless LAN network formed by a group of computers, each with a network adapter.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type: Indication of an authentication algorithm which can be supported by the Access Point:

1. Open System: Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.

2. Shared Key: Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone: The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth: The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Beacon: A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit: A binary digit, which is either 0 or 1 for value, is the smallest unit for data.

Bridge: An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

Browser: An application program that enables one to read the content and interact in the World Wide Web or Intranet.

BSS: BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that associated with it.

Channel: The bandwidth which wireless Radio operates is divided into several segments, which we call them "Channels". AP and the client stations that it

associated work in one of the channels.

CSMA/CA: In local area networking, this is the CSMA technique that combines slotted time -division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP: Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS: Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address: An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption: A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS: ESS stands for "Extended Service Set". More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID: The unique identifier that identifies the ESS. In infrastructure association, the stations use the same ESSID as AP's to get connected.

Ethernet: A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation: When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold: The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway: a device that interconnects networks with different, incompatible communication protocols.

HEX: Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE: The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure: An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

ISM Band: The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address: Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting: Sending data to a group of nodes instead of a single destination.

Node: A network junction or connection point, typically a computer or workstation.

Packet: A unit of data routed between an origin and a destination in a network.

PLCP: Physical layer convergence protocol

PPDU: PLCP protocol data unit

Preamble Type: During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU: PLCP service data unit

Roaming: A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS: Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold: Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask: The method used for splitting IP networks into a series of sub-groups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP/IP: Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e. intranet or internet. When set up with direct access to the Internet, computer is provided with a copy of the TCP/IP program just as every other computer that user may send messages to or get information from also has a copy of TCP/IP.

Throughput: The amount of data transferred successfully from one point to another in a given period of time.

WEP: Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.