P600 Wireless 11g Outdoor AP Bridge

User Manual

Version 1.0

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise without the prior writing of the publisher.

DEC. 2004

Contents

1. Introduction

Thank you for purchasing your P600 Wireless 802.11g Outdoor AP Bridge.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- P600 Wireless 802.11g Outdoor AP Bridge
- CD - User Guide
- PoE Host / Cord
- Waterproof RJ-45 connector
- Mount Kit package

Note: if anything is missing, please contact your vendor

2. Safety Notification

Your Wireless AP should be placed in a safe and secure location. To ensure proper operation, please keep the unit away from water and other damaging elements. Please read the user manual thoroughly before you install the device. The device should only be repaired by authorized and qualified personnel.

- Please do not try to open or repair the device yourself.
- Do not place the device in a damp or humid location, i.e. a bathroom.
- The device should be placed in a sheltered and non-slip location within a temperature range of +5 to +40 Celsius degree.
- Please do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

3. AP Default Settings

The default settings are shown following.

| User	admin
Password	admin
AP IP Address	192.168.1.250
AP Subnet Mask	255.255.255.0
RF ESSID	ap11g
11g RF Channel	6
Mode	11b+g
Encryption	Disabled

4. Web Management Settings

TURN ON POWER SUPPLY
Quick power cycle can caused system corruption. When power on, be careful not to shut down in about 5 seconds, because data is writing to the flash.

START UP & LOGIN
In order to configure the outdoor Wireless 11g AP, you must use your web browser and manually input http://**192.168.1.250** into the Address box and press Enter. The Main Page will appear.
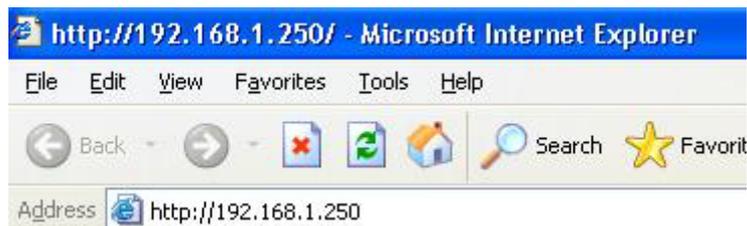
To start configure the outdoor Wireless 11g AP, you must login as "**admin"** in the **User Name** box. And input password "**admin**" on the password section.

Once you have logged-in as administrator, it is a good idea to change the administrator password to ensure a secure protection to the outdoor Wireless 11g AP. The Security Settings section described later in this manual describes how to change the password.

Once you have input the correct password and logged-in, the screen will change to the Setup page screen.

4.1. Primary Setup

<table>
<tr><td>

MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER
To change the configuration, use Internet Explorer (IE) or Netscape Communicator to connect the WEB management **192.168.1.250.**

</td></tr>
</table>

Primary Setup

This screen contains all of the AP's basic setup functions.


.

Most users will be able to configure the AP and get it working properly using the settings on this screen.

LAN IP Address and Subnet Mask: This is the AP's IP Address and Subnet Mask as seen on the internal LAN. The default value is 192.168.1.250 for IP Address and 255.255.255.0 for Subnet Mask.
Wireless: This section provide the Wireless Network settings for your WLAN
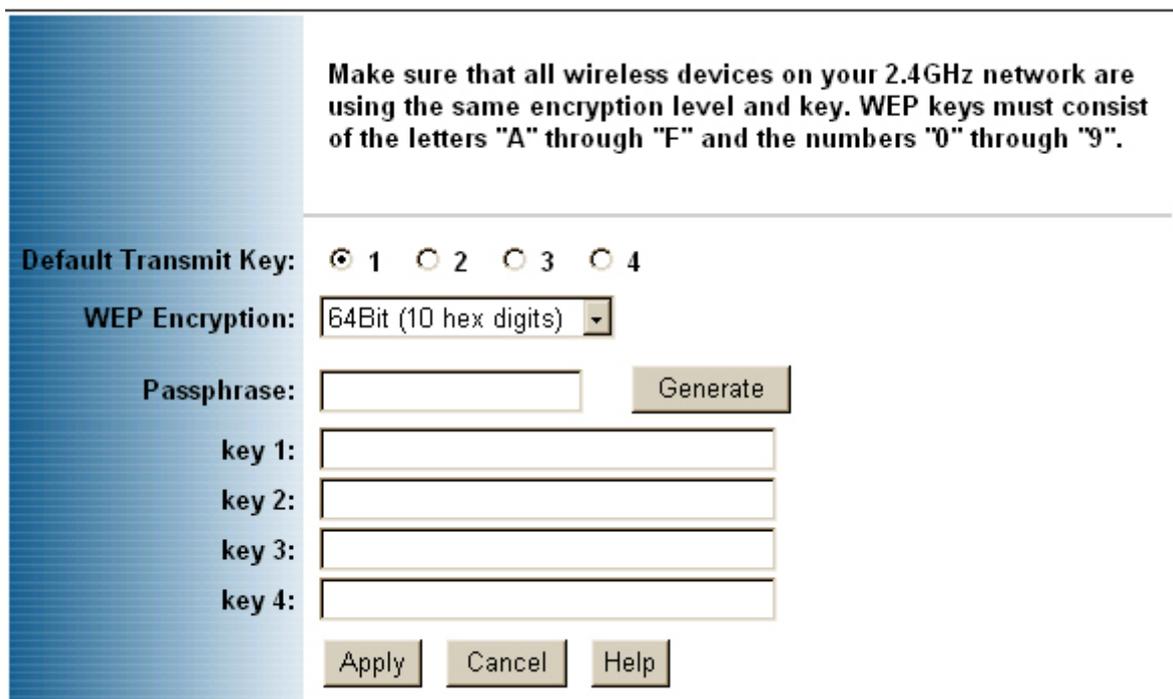
Wireless Settings
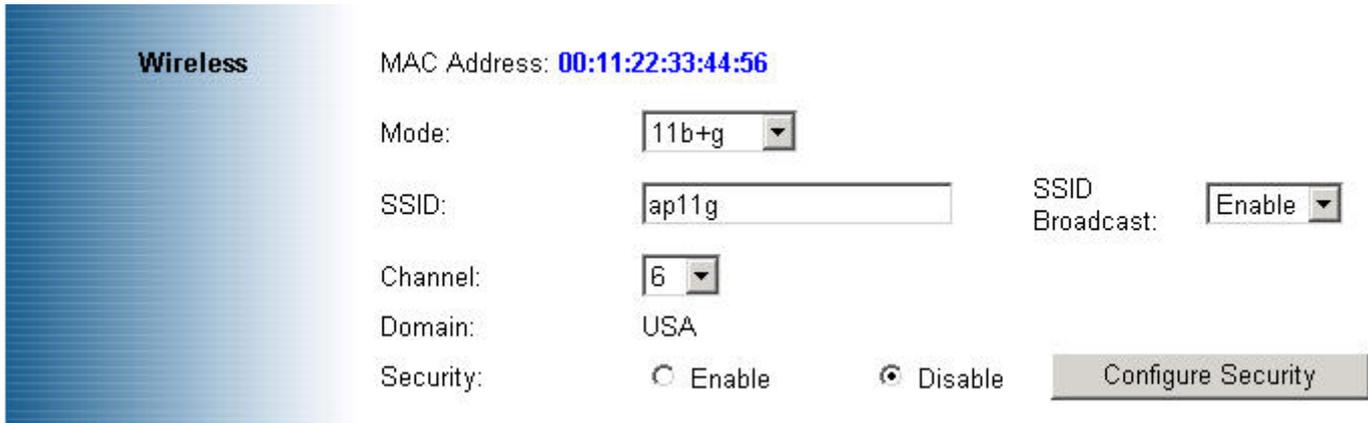
SSID: The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the APs that will be communicating with mobile wireless stations.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.

Security: There are 3 types of security to be selected. To secure your Wireless Networks, it's strongly recommended to enable this feature.

-WEP

Make sure that all wireless devices on your network are using the same encryption level and key. WEP keys must consist of the letters "A" through "F" and the numbers "0" through "9."
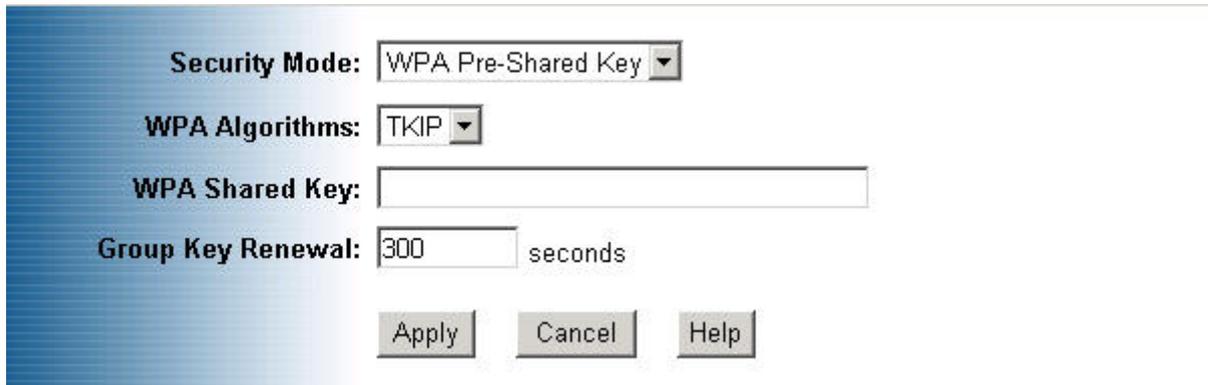
Important Notice

In order to make right use of WPA, please ensure that your current Wireless Adapter's driver, and Wireless Utility can support it, WPA needs 802.1x authentication (when RADIUS mode is chosen), though the Operating System must also support 802.1x protocol. For Microsoft's OS family, only Windows XP has incorporated this by default. The rest of the OS must installed 3er party's client software such as Funk ODySSey.

-WPA-Preshared key

There are two encryption options for WPA Pre-Shared Key, TKIP and AES. TKIP stands for Temporal Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes a symmetric 128-Bit block data encryption.

To use WPA Pre-Shared Key, enter a password in the WPA Shared Key field between 8 and 63 characters long. You may also enter a Group Key Renewal Interval time between 0 and 99,999 seconds.
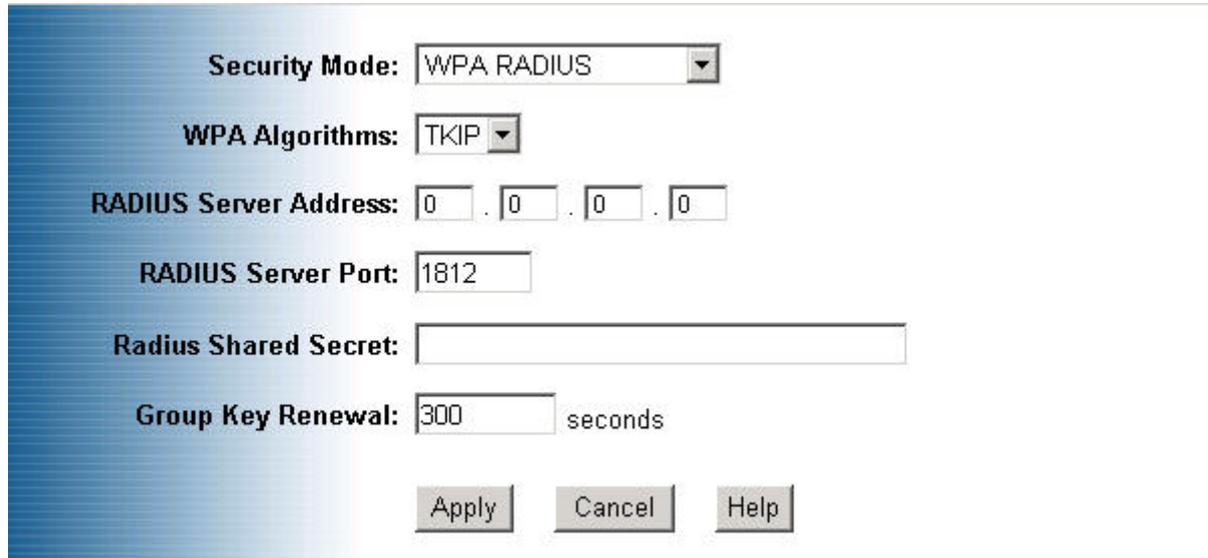
WPA Algorithms	Please choose your algorithms method. You can select between TKIP or AES.
WPA Shared Key	Please input the Pre-Shared Key. The key should be 8 characters or 63 characters in alphanumeric.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

-WPA RADIUS

WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

WPA Algorithms	Please choose your algorithms method. You can select between TKIP or AES.
Radius Server Address	Please input your RADIUS Server IP address.
RADIUS Server Port	Please input the Authentication port of your RADIUS server. The default port being used is 1812
RADIUS Shared Key	The RADIUS server will accept the authentication if both **Shared Key** matched.
Group Key Renewal	Please input the period of renewal time. The default selection is 300 seconds.

* Click **Apply** to save your settings.

4.2. System

AP Password: Changing the password for the AP is as easy as typing the password into the **Enter New Password** field. Then, type it again into the Re-enter to confirm.

* Click the **Apply** button to save the setting.

Use the default password when you first open the configuration pages, after you have configured these settings, you should set a new password for the AP (using the Password screen). This will increase security, protecting the AP from unauthorized changes.

Restore Factory Defaults: Click the **Yes** button to reset all configuration settings to factory default values. Note: Any settings you have saved will be lost when the default settings are restored. Click the **No** button to disable the Restore Factory Defaults feature.

Click the **Apply** button to save the setting.

Backup/Restore Setting: Click Backup to store the Access Point's configuration on your local PC. Click Restore to restore Access Point's configuration from your local PC

* Check all the settings and click **Apply** to save them.

4.3. Operating Mode

Access Point: This mode provides access for wireless stations to wired LANs and from wired LANs to wireless stations.

AP Repeater: This mode allows the AP to keep the AP function role and at the same time performing a communication with other 802.11g AP to establish and extend your Wireless Network cover. Please enter the Remote Access Point's MAC address to enable this feature.
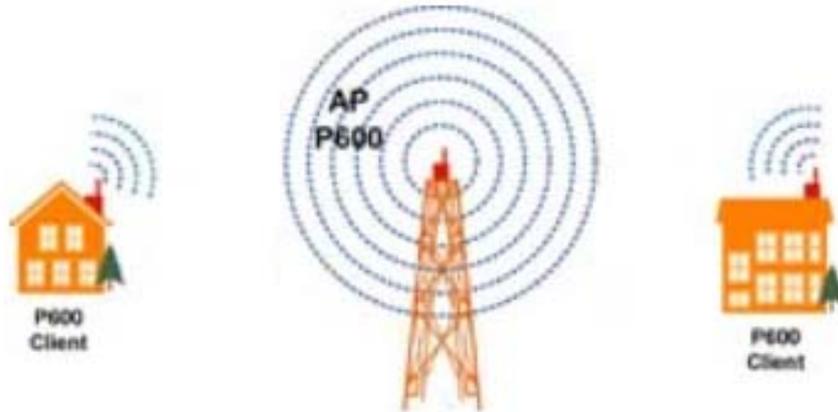
Wireless Bridge: This mode allows the connection of one or more remote LANs with a central LAN.
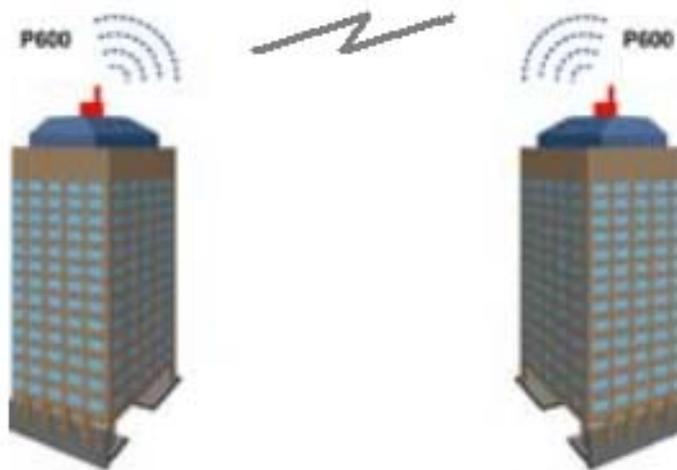
* Click **Apply** to save your settings.

4.4. Status

This screen displays the IEEE 802.11g AP's current status and settings. This information is read-only. This page will auto re-flash every 5 seconds to keep most update information.

LAN section will be displaying all information related on AP, such as the IP address and the current configuration type.

Wireless section will be displaying information related on the Wireless interface, such as SSID, Channel, Encryption and statistics of network traffic.

*Click the **Refresh** button to refresh the AP's status and settings.

4.5 Traffic Log

Traffic Log: The AP can keep logs of all incoming or outgoing traffic for your network traffic. This feature is disabled by default. To keep activity logs, select **Enable**.

To keep a permanent record of activity logs as a file on your PC's hard drive, Log viewer software must be used. In the Send Log to field, enter the fixed IP address of the PC running the Log viewer software. The AP will send updated logs to that PC.

To see a temporary log of the AP's most recent traffic, click the **View Log** button..

Click the **Apply** button to save the setting.

4.6 Access Control

Access Control: This function will allow administrator to have access control by enter MAC address of client stations. When **Enable** this function, two new options will show up.

Depend on the filtering propose, it can be selected to **Deny** or **Allow**.
Fill the client stations MAC list to complete the configuration. The table could store up to **40** different MAC addresses. Please follow the format that it required when an address is input.

* Click **Apply** to save your settings.

4.7 Advanced Wireless

Authentication Type:
  Auto: Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.
  Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.
  Shared Key: Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **AUTO** to have the AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is **AUTO**.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the AP to synchronize the wireless network. The default value is **100**.

RTS Threshold: This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

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.

* Click **Apply** to save your settings.

4.8. SNMP INFO

SNMP INFO: The SNMP screen allows you to customize the Simple Network Management Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

SNMPv2c		To enable the SNMP support feature, select **Enable**. Otherwise, select **Disable**.
Identification	Contact	In the contact field, enter contact information for the AP.
	Unit Name and description	In the Unit Name and description field, enter the name of the AP or AP description.
	Physical Location	In the Physical Location field, specify the area or location where the AP resides.
SNMP Community	public	You may change the SNMP Community's name from its default, **public**. Then configure the community's access as either **Read-Only** or **Read-Write**.
	private	You may change the SNMP Community's name from its default, **public**. Then configure the community's access as either **Read-Only** or **Read-Write**.

Click **Apply** to save your settings.

4.9. Upgrade Firmware
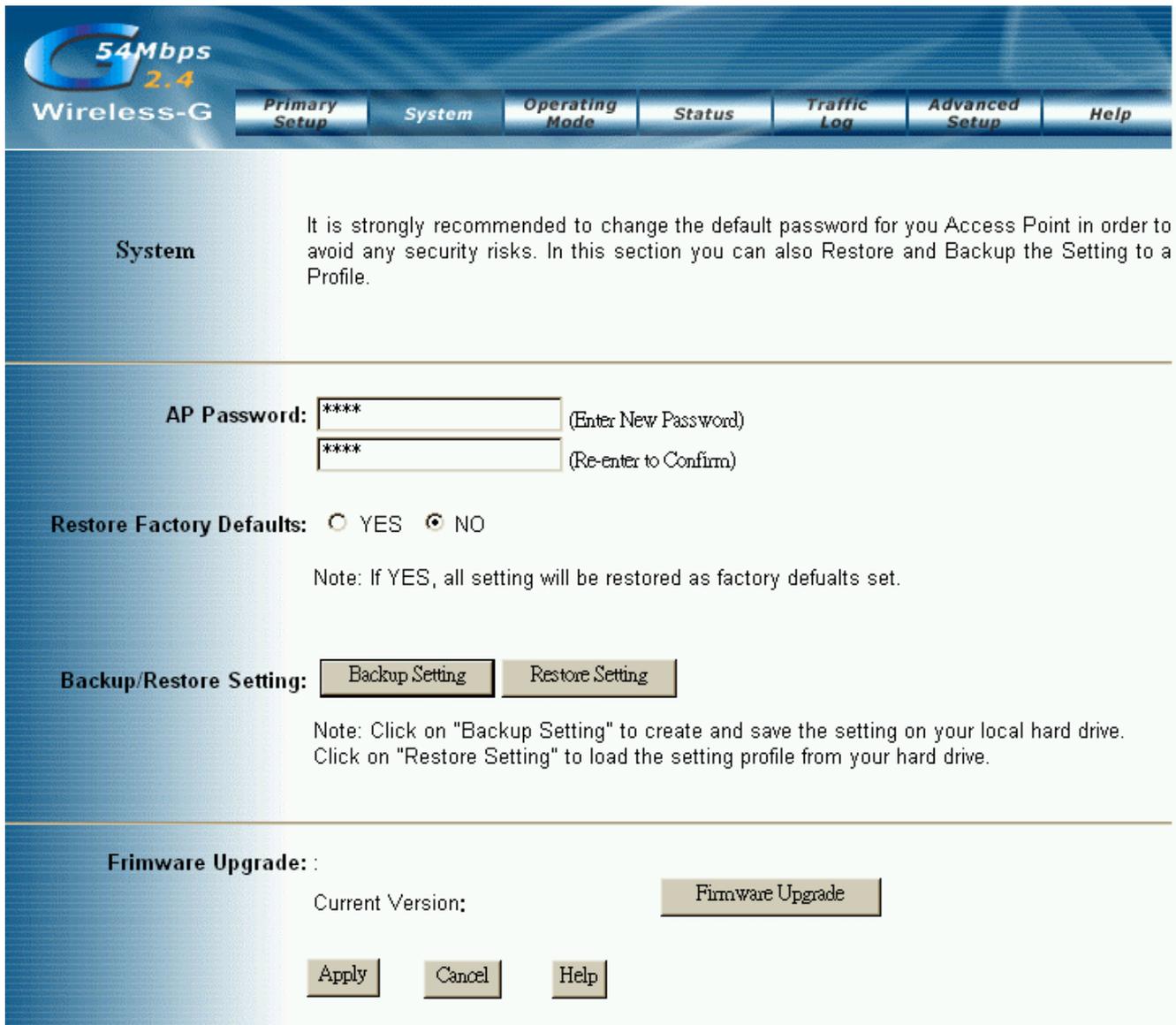
To perform the firmware upgrade action, please go to the System section.

Firmware Upgrade: Click the **Firmware Upgrade** button to load new firmware onto the AP. If the AP is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

Note: When you upgrade the AP's firmware, you may lose its configuration settings, so make sure you write down the AP's settings before you upgrade its firmware.

To upgrade the AP's firmware:

1. Download the firmware upgrade file from the internet.

2. Extract the firmware upgrade file.

3. Click the Firmware Upgrade button.

4. On the Firmware Upgrade screen, click the **Browse** button to find the firmware upgrade file.

5. Double-click the firmware upgrade file.

6. Click the Upgrade button, and follow the on-screen instructions.

Note: Do not power off the AP or press the Reset button while the firmware is being upgraded.

5. Troubleshooting

Basic Functions

My Wireless AP will not turn on. No LED's light up.

Cause:
- The power is not connected.

Resolution:
- Connect the PoE adapter to your AP and plug it into the power outlet.

Note: Only use the PoE adapter provided with your AP. Using any other adapter may damage your AP.

LAN Connection Problems I can't access my AP.

Cause:
- The unit is not powered on.
- There is not a network connection.
- The computer you are using does not have a compatible IP Address.

Resolution:
- Make sure your AP is powered on.
- Make sure that your computer has a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the AP. For example, if the AP is set to 192.168.1.250, change the IP address of your computer to 192.168.1.15 or another unique IP Address that corresponds to the 192.168.1.X subnet.
Use the Reset button located on the rear of the AP to revert to the default
settings.

I can't connect to other computers on my LAN.

Cause:
- The IP Addresses of the computers are not set correctly.
- Network cables are not connected properly.
- Windows network settings are not set correctly.

Resolution:
- Make sure that each computer has a unique IP Address. And the IP must be in the same subnet as the AP.
- Make sure that the Link LED is on. If it is not, try a different network cable.
- Check each computer for correct network settings.

Wireless Troubleshooting
I can't access the Wireless AP from a wireless network card

Cause:
- Out of range.
- IP Address is not set correctly.

Resolution:
- Make sure that the Mode, SSID, Channel and encryption settings are set the same on each wireless adapter.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- Check your IP Address to make sure that it is compatible with the Wireless AP.

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

SparkLAN declares that P600N (FCC ID: RYK-04061131) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.