802.11g Wireless Ethernet Adapter

User's Manual

Version 1.0

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.

The WCM-100 (FCC ID: RYK-WCM100) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Copyright Statement

Mar. 2006

Contents

1. Introduction

Thank you for purchasing 802.11g Wireless Ethernet Adapter.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- 802.11g Wireless Ethernet Adapter
- Quick Installation Guide
- Combo Cable
- User Manual CD

Note: if anything is missing, please contact your vendor

2. Safety Notification

Your Wireless Ethernet Adapter 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 by 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. Hardware Installation

Front Panel

The front panel provides LED's for device status. Refer to the following table for the meaning of each feature.

LED	STATUS	Description
POWER	Off	No power
	Green On	1. Power on 2. Reset to default 3. Firmware upgrade (first 1 minute)
	Green Blink	1. System up 2. Power on 3. Firmware upgrade
LINK	Off	No Ethernet link detected
	Green On	10/100Mbps Fast Ethernet link detected.
	Green Blink	Indicates data traffic on the 10/100 Mbps LAN
ACT	Green Blink	Indicates the device is linking or active data through wireless links

Side Panel

The side panel features 1 LAN ports and Reset button. Refer to the following table for the meaning of each feature.

Power (DC 5v)	Used to connect to the power outlet. Only use the power adapter provided with the device. Use of an unauthorized power adapter may cause damage to your device and violate your warranty.
Reset	Press the Reset Button for approximate ten seconds, all configurations will set to factory default settings.
LAN	The RJ-45 Ethernet port used to connect your PC, hub, switch or Ethernet network.

AP Default Settings

The default settings are shown following.

User	
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

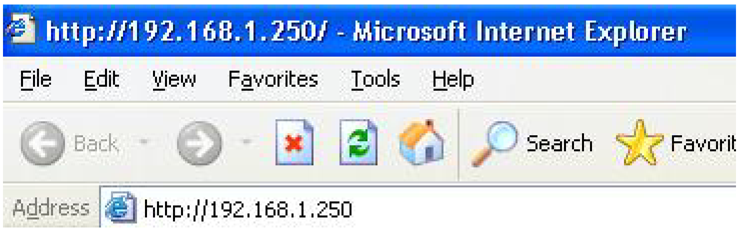
Quick power cycle can caused system corruption. When power on, be careful not to shut down in about 5 seconds, because data is writing to the flash.

START UP & LOGIN

Before Starting

The default IP address setting for the unit is a class C IP address (192.168.1.250/ 255.255.255.0). Please make sure that the current workstation is following the class C IP address range, from 192.168.1.1 to 192.168.1.254 if you would like to do any configuration by this workstation.

In order to configure the Wireless 11g AP, you must use your web browser and manually input http://**192.168.1.250** into the Address box and press Enter on explorer. The Main Page will appear.



http://192.168.1.250

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

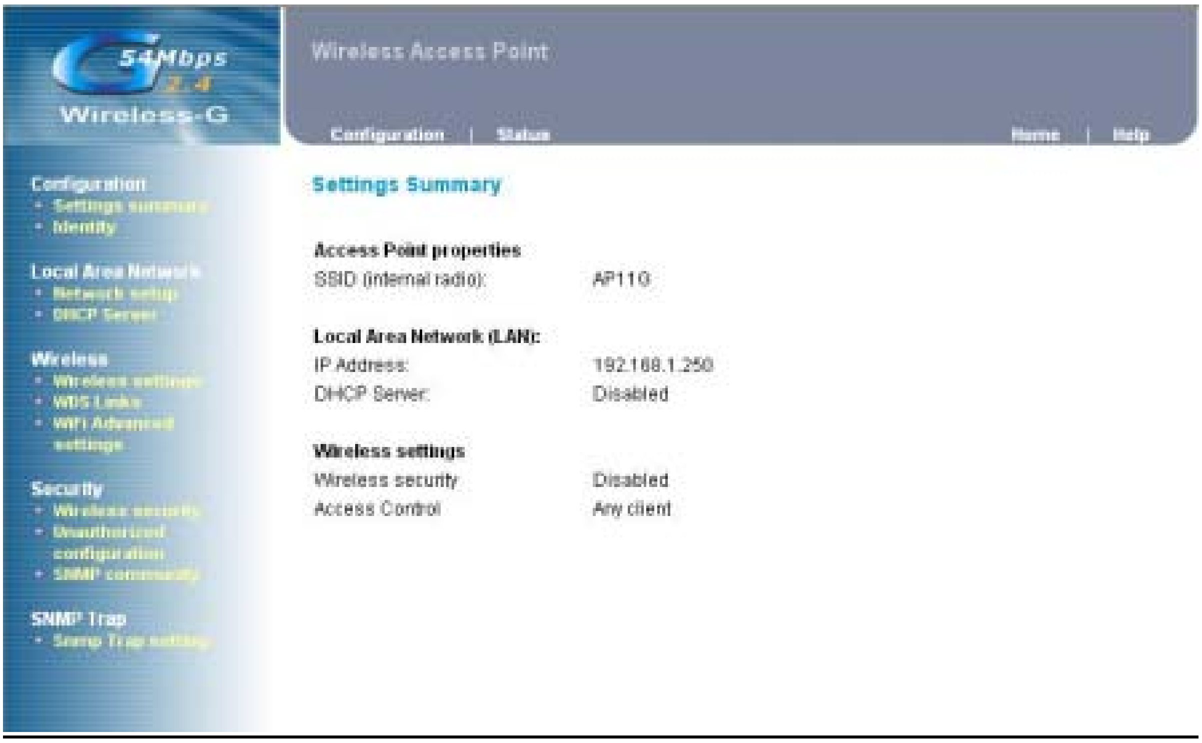
Once you have input the correct password and logged-in, the screen will change to the Setup page screen.

4.1 Configuration

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.**

Settings Summary

This section contains the AP's basic settings information.



Settings Summary

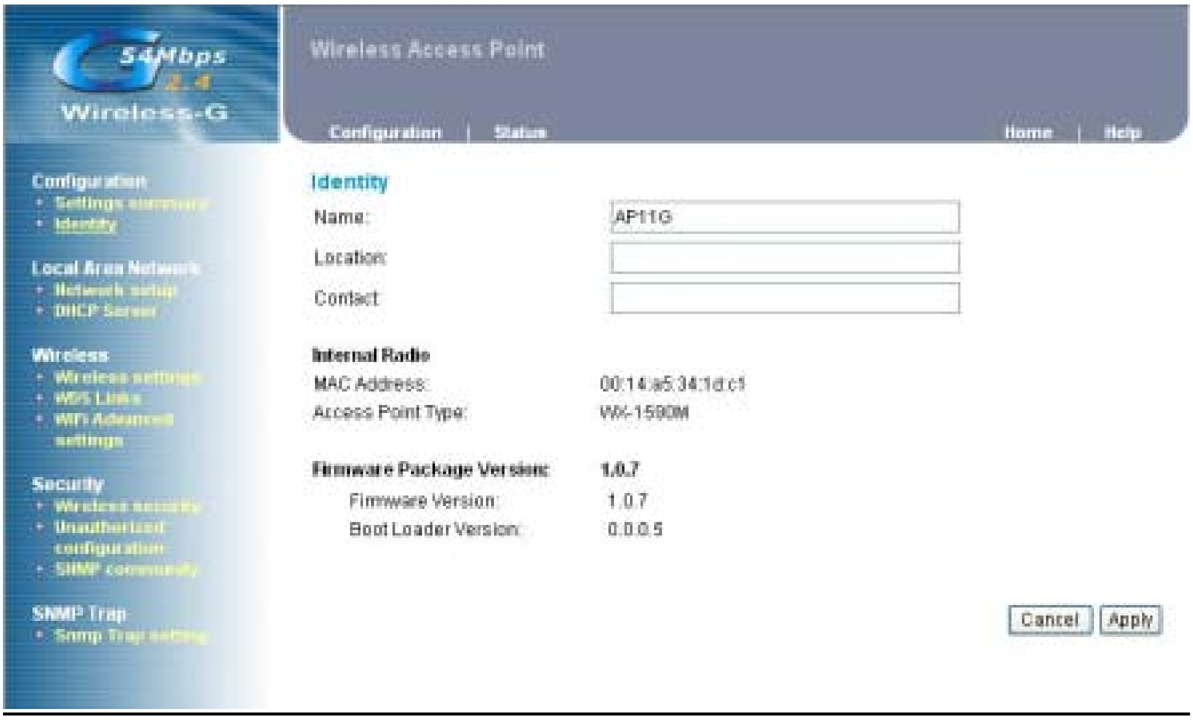
Access Point properties
SSID (internal radio): AP11G

Local Area Network (LAN):
IP Address: 192.168.1.250
DHCP Server: Disabled

Wireless settings
Wireless security Disabled
Access Control Any client

Identity

This section contains the AP's current firmware version. Also It can allow user to define the identity information for this unit if there are many same type units locate at one network.



Identity

Name: AP11G
Location:
Contact:

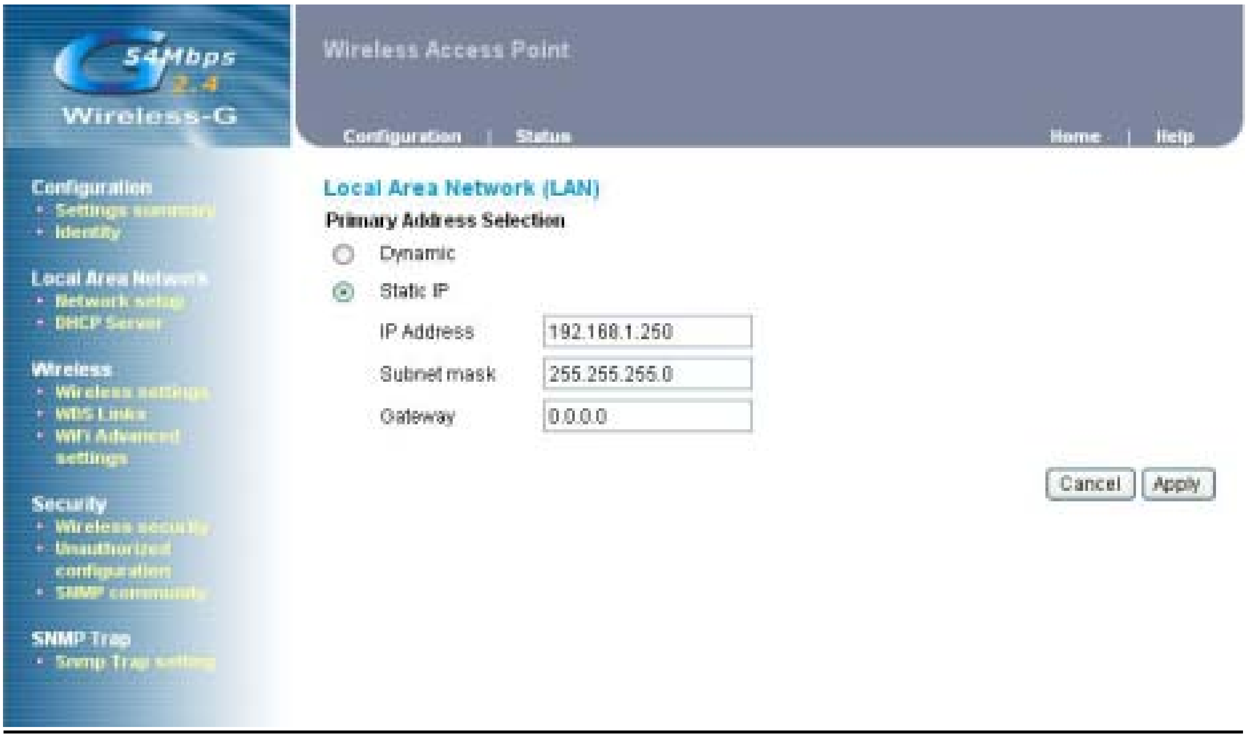
Internal Radio
MAC Address: 00:14:a5:34:1d:c1
Access Point Type: WX-1590M

Firmware Package Version: **1.0.7**
Firmware Version: 1.0.7
Boot Loader Version: 0.0.0.5

4.2 Local Area Network

Local Area Network(LAN)

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.



Local Area Network (LAN)

Primary Address Selection

○ Dynamic

● Static IP

IP Address 192.168.1.250

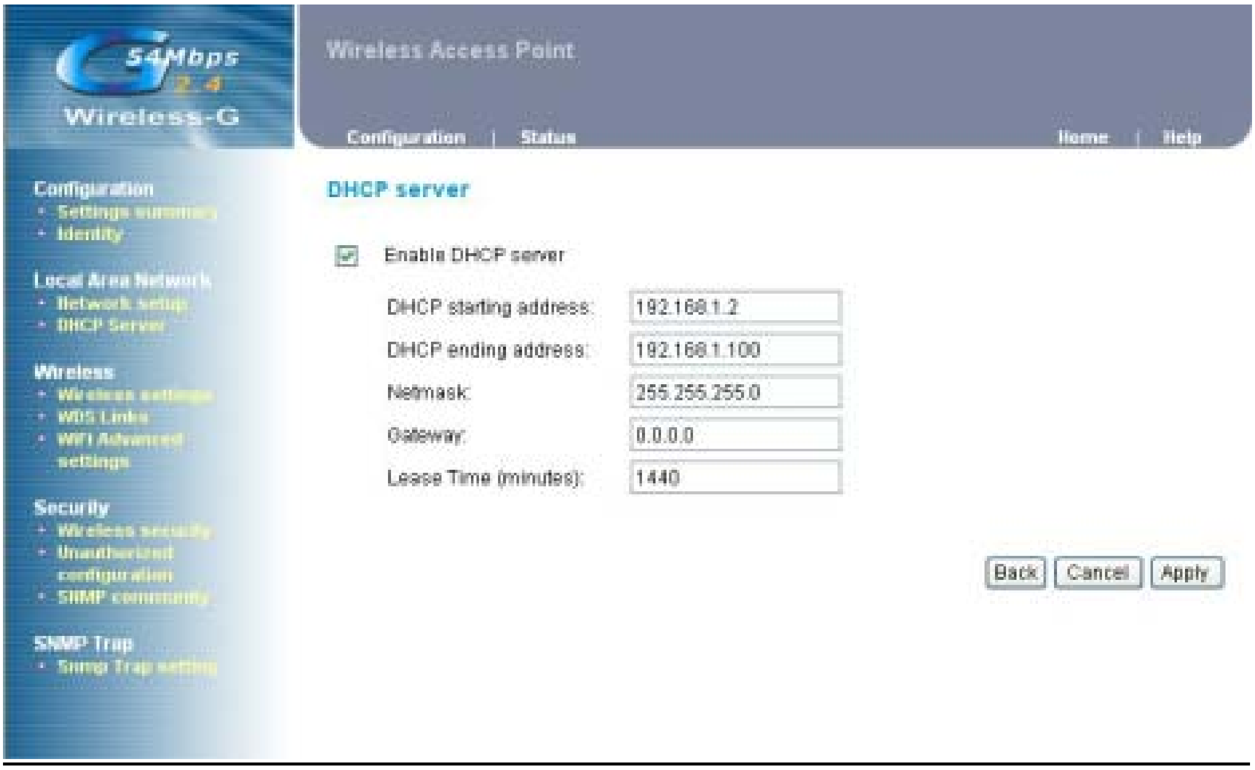
Subnet mask 255.255.255.0

Gateway 0.0.0.0

DHCP Server Settings

The DHCP Server section allows you to configure the settings for the AP's Dynamic Host Configuration Protocol (DHCP) server function. The AP can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the AP's DHCP server option, you must configure your entire network PCs to connect to a DHCP server, the AP.
If you disable the AP's DHCP server function, you must configure the IP Address, Subnet Mask, and DNS for each network computer (note that each IP Address must be unique).

Global Settings: Select the **Enable** option to enable the AP's DHCP server option.
If you already have a DHCP server on your network or you do not want a DHCP server, then select **Disable** from the options.
If you enable the DHCP server function, you have to enter a numerical value for the DHCP server starting and ending addresses. Then the DHCP server will follow this range to assign IP address for each DHCP clients.
If your DHCP clients must route to other network or with internet service, then the Gateway IP address will be necessary.



DHCP server

☑ Enable DHCP server

DHCP starting address:	192.168.1.2
DHCP ending address:	192.168.1.100
Netmask:	255.255.255.0
Gateway:	0.0.0.0
Lease Time (minutes):	1440

4.3 Wireless

SSID **:** only Access Points and clients that share this SSID are able to communicate with each other. Your networking client allows you to choose to which network you connect. The network names you see there are SSIDs.

Band **:** select the policy for internal radio. There are 3 types of band setting, the default mode is Mixed.

Radio 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.

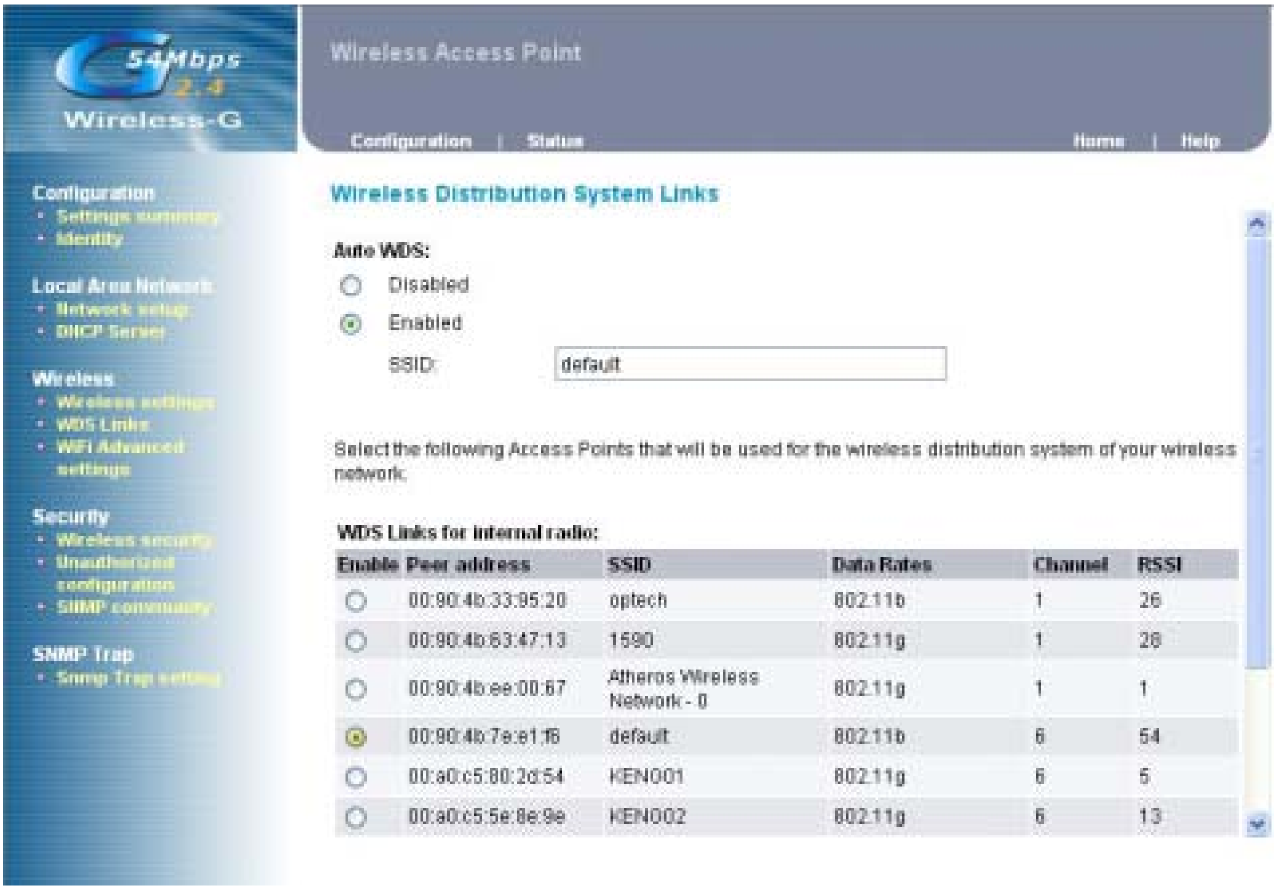
Broadcast SSID **:** this setting is related with SSID for whether it can be broadcasted by wireless or not.

Enable L2 Isolation: enable this setting will reject clients to communicate between themselves by this AP.

Preamble Type **:** select the head length of the packet. There are 2 types can be supported, long and short.

WDS Links

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 coverage. Please select the checkbox to enable AP on the WDS list to perform WDS application or enter the Remote Access Point's MAC address to enable this feature.



Wireless Distribution System Links

Auto WDS:

○ Disabled

● Enabled

SSID: default

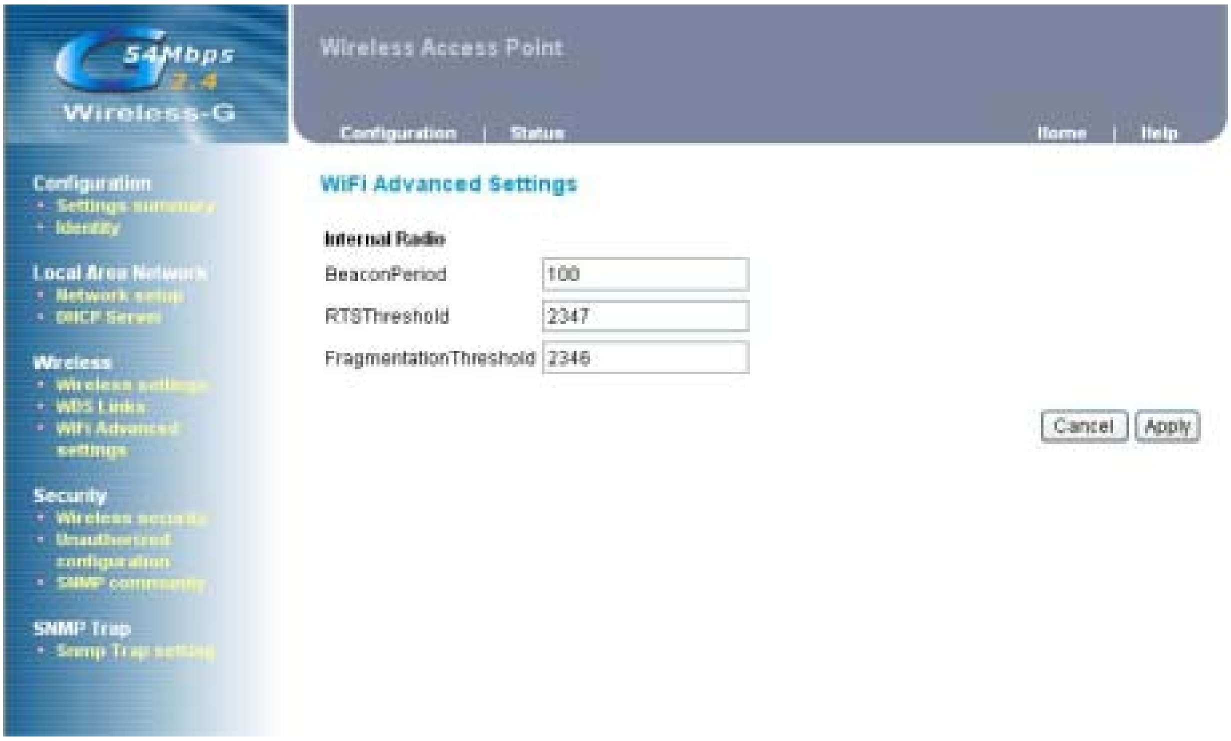
Select the following Access Points that will be used for the wireless distribution system of your wireless network.

WDS Links for internal radio:

Enable	Peer address	SSID	Data Rates	Channel	RSSI
○	00:90:4b:33:95:20	optech	802.11b	1	26
○	00:90:4b:63:47:13	1590	802.11g	1	28
○	00:90:4b:ee:00:67	Atheros Wireless Network - 0	802.11g	1	1
●	00:90:4b:7e:e1:f6	default	802.11b	6	54
○	00:a0:c5:80:2d:54	KEN001	802.11g	6	5
○	00:a0:c5:5e:8e:9e	KEN002	802.11g	6	13

WiFi Advanced Setting

In this page you can configure the WiFi advance settings: Beacon Period, RTS Threshold and the Fragmentation Threshold. The default value of Beacon Period is 100, RTS Threshold is 2347 and the Fragmentation Threshold is 2346.



WiFi Advanced Settings

Internal Radio

BeaconPeriod	100
RTSThreshold	2347
FragmentationThreshold	2346

4.4 Security

Wireless Security

The Wireless Security Setting separates 4 items setting. They are included ACL, RADIUS Server, WEP and WPA.

Access Control List : This function will allow administrator to have access control by enter MAC address of client stations.

RADIUS Servers : With this option you use a RADIUS server to handle access control.
RADIUS ("Remote Authentication Dial In User Service" is a standard for user authentication. The RADIUS server contains a database with users and their access rights. When a user wants to use the Access Point, the Access Point contacts the RADIUS server to see if this is permitted.

To add a RADIUS server:

1. Click Add to add a RADIUS server.
2. In the window that appears, enter the following data:
   - IP Address: the IP address of the RADIUS server.
   - UDP Port: the UDP port number of the RADIUS server.
   - Secret: the password for access to the RADIUS server.
3. Click OK. The server is now added to the list.

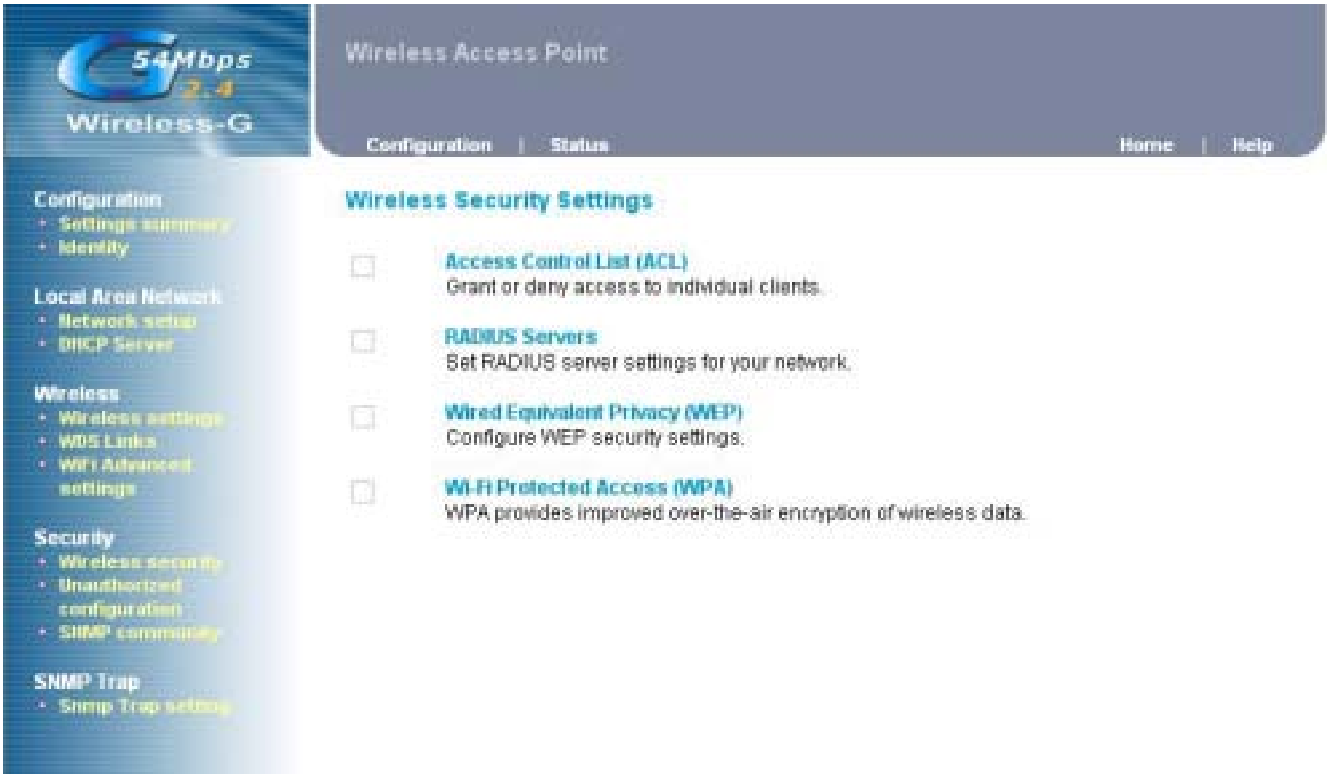
You can add more than one RADIUS server. The first server in the list will be used by default, the second will be used if the first is not available, etc.

To delete a RADIUS server from the list:

1. Click Delete.
2. Select the RADIUS server that you want to remove from the list.
3. Click OK. The list is updated.

Wired Equivalent Privacy (WEP) : select the check box will enable WEP function. WEP security supports 2 types encrypted format, one is Hexadecimal and the other is ASCII format.

Wi-Fi Protected Access (WPA) : The WPA security pre-shared key supports TKIP and AES algorithm. TKIP and AES utilize a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. 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. You also can using WPA RADIUS to enlaces the wireless security.



Wireless Security Settings

□ **Access Control List (ACL)**
Grant or deny access to individual clients.

□ **RADIUS Servers**
Set RADIUS server settings for your network.

□ **Wired Equivalent Privacy (WEP)**
Configure WEP security settings.

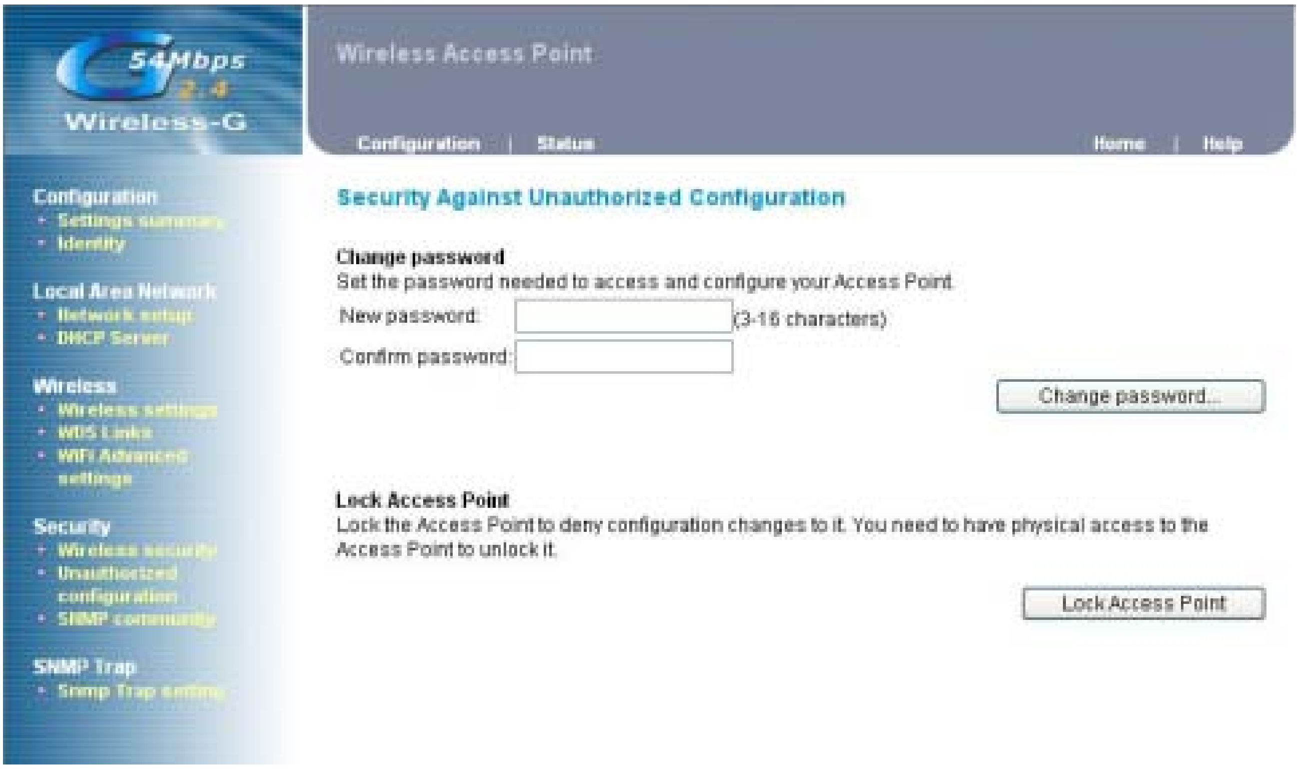
□ **Wi-Fi Protected Access (WPA)**
WPA provides improved over-the-air encryption of wireless data.

Unauthorized configuration

Changing the password for the AP is as easy as typing the password into the **New Password** field. Then, type it again into the Confirm password to confirm.

There is no 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.

Also you can lock this AP to deny any configuration changes. Once you lock this AP, only by hardware reset can unlock this device.



Security Against Unauthorized Configuration

Change password

Set the password needed to access and configure your Access Point.

New password: (3-16 characters)

Confirm password:

Lock Access Point

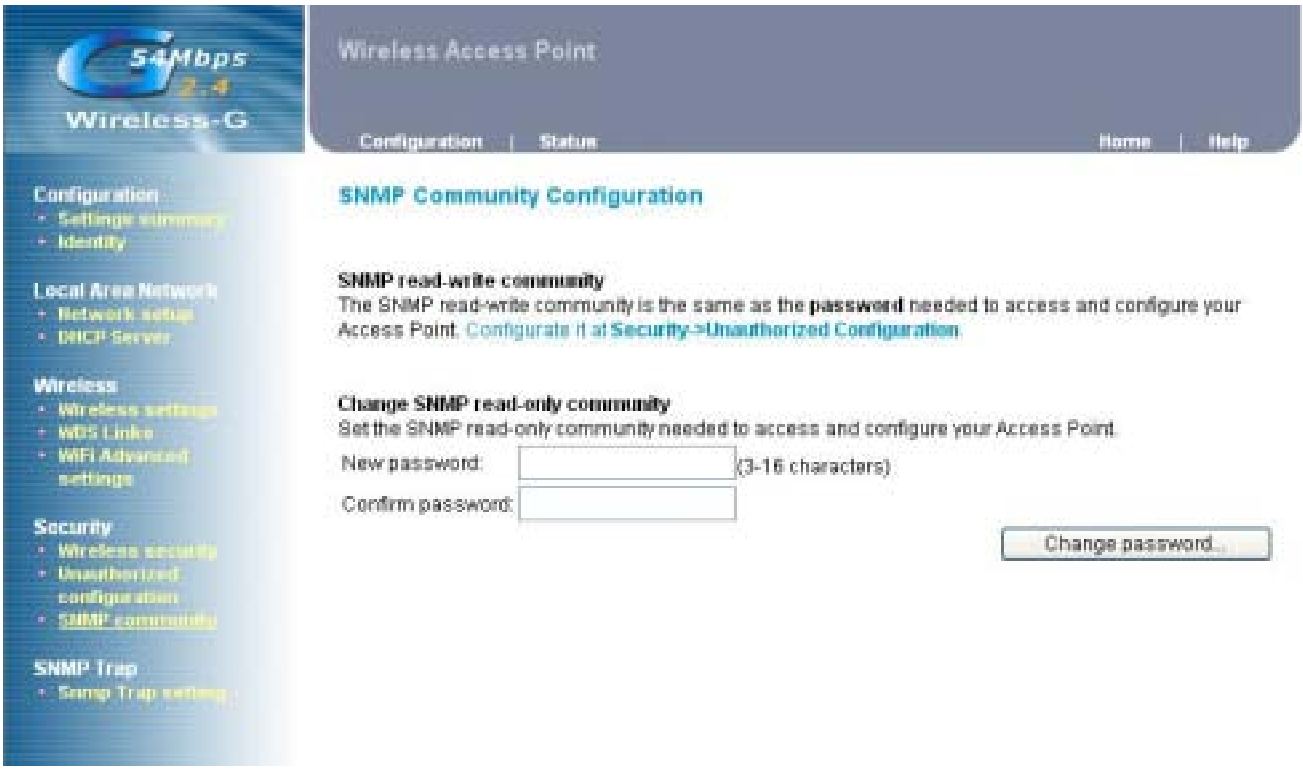
Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it.

SNMP Community Configuration

In this page you can configure the following settings:

SNMP read-write community
The SNMP read-write community is the same as the **password** needed to access and configure your Access Point.

Change SNMP read-only community
Set the SNMP read-only community needed to access and configure your Access Point.



SNMP Community Configuration

SNMP read-write community
The SNMP read-write community is the same as the **password** needed to access and configure your Access Point. Configurate it at **Security->Unauthorized Configuration**.

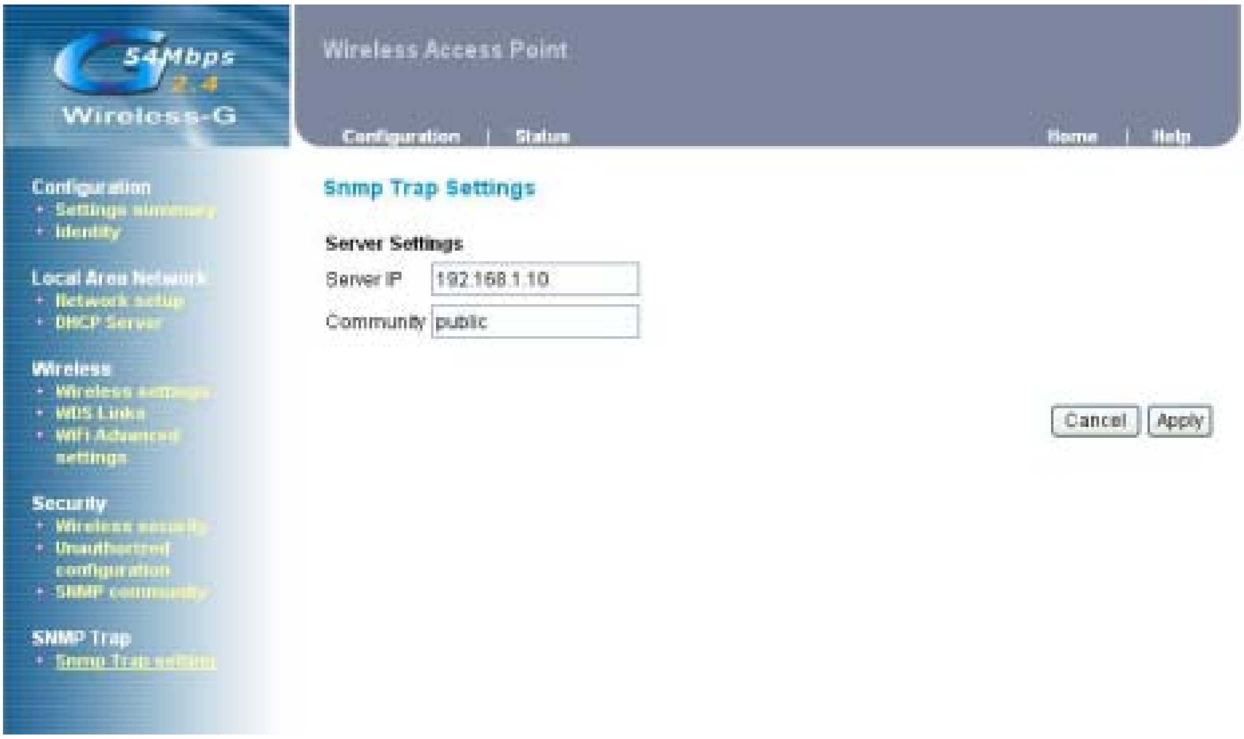
Change SNMP read-only community
Set the SNMP read-only community needed to access and configure your Access Point.

New password: (3-16 characters)

Confirm password:

4.5 SNMP Trap Settings

In this page you can configure the SNMP trap Settings



Snmp Trap Settings

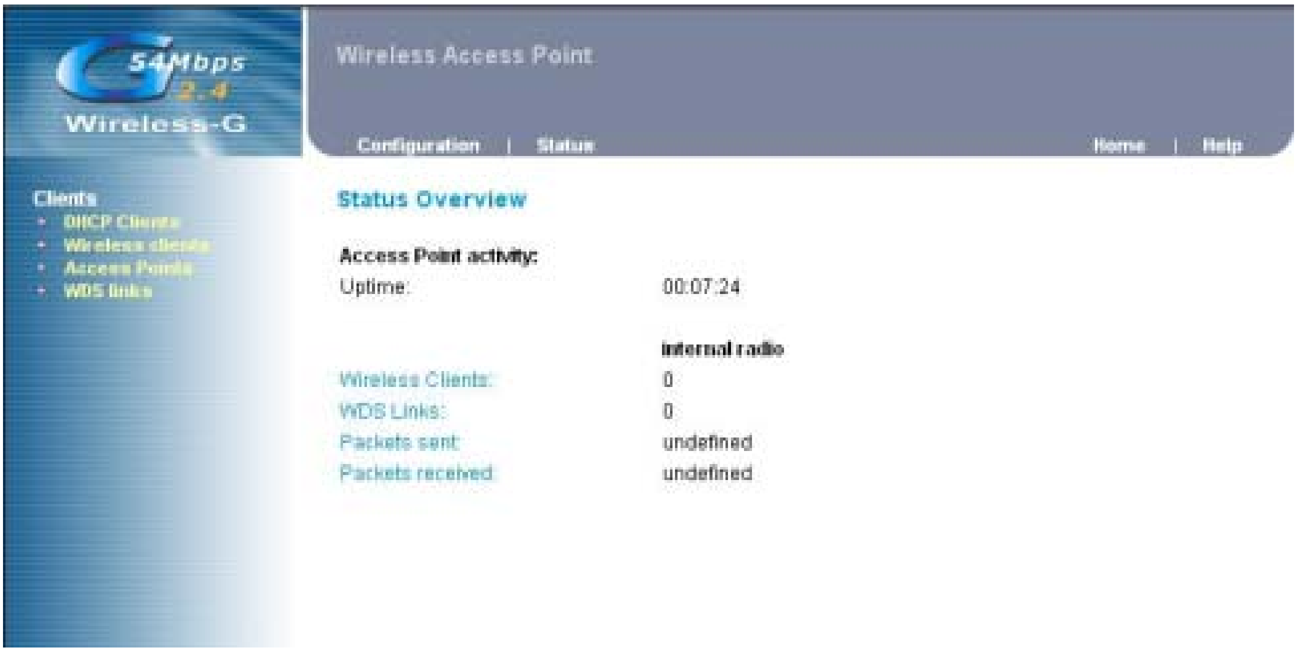
Server Settings

Server IP 192.168.1.10

Community public

4.6 Status Overview

In this section, we provide a series of statistics about this AP. User can check each status via this page. For example, if you would like to check how many clients already associated on this AP, you may click the link on left site “ Wireless clients “ for detail. For other detail information, please tip other links for reference.



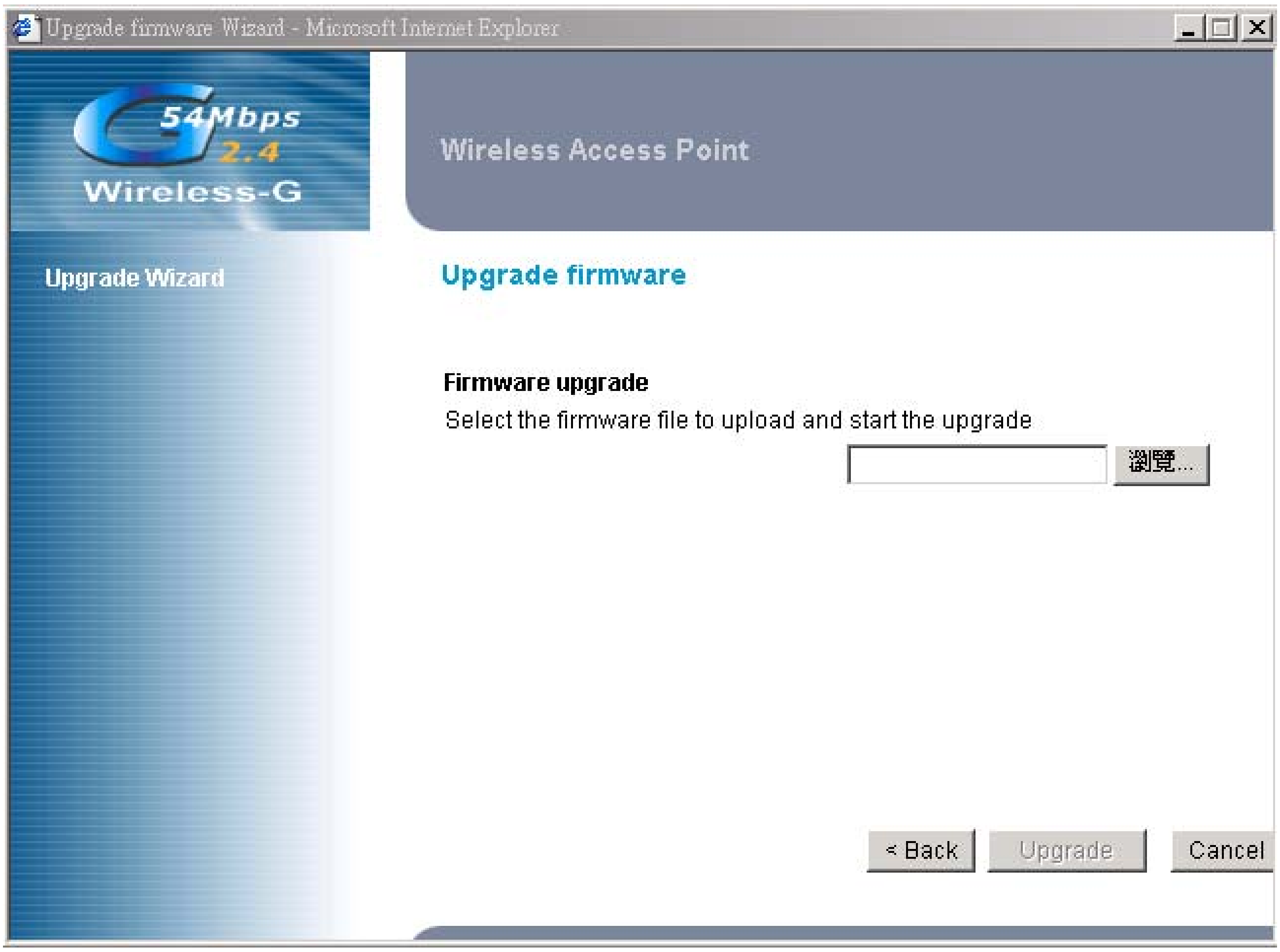
Status Overview

Access Point activity:

Uptime:	00:07:24
	internal radio
Wireless Clients:	0
WDS Links:	0
Packets sent:	undefined
Packets received:	undefined

4.7 Upgrade Firmware

Click the **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.

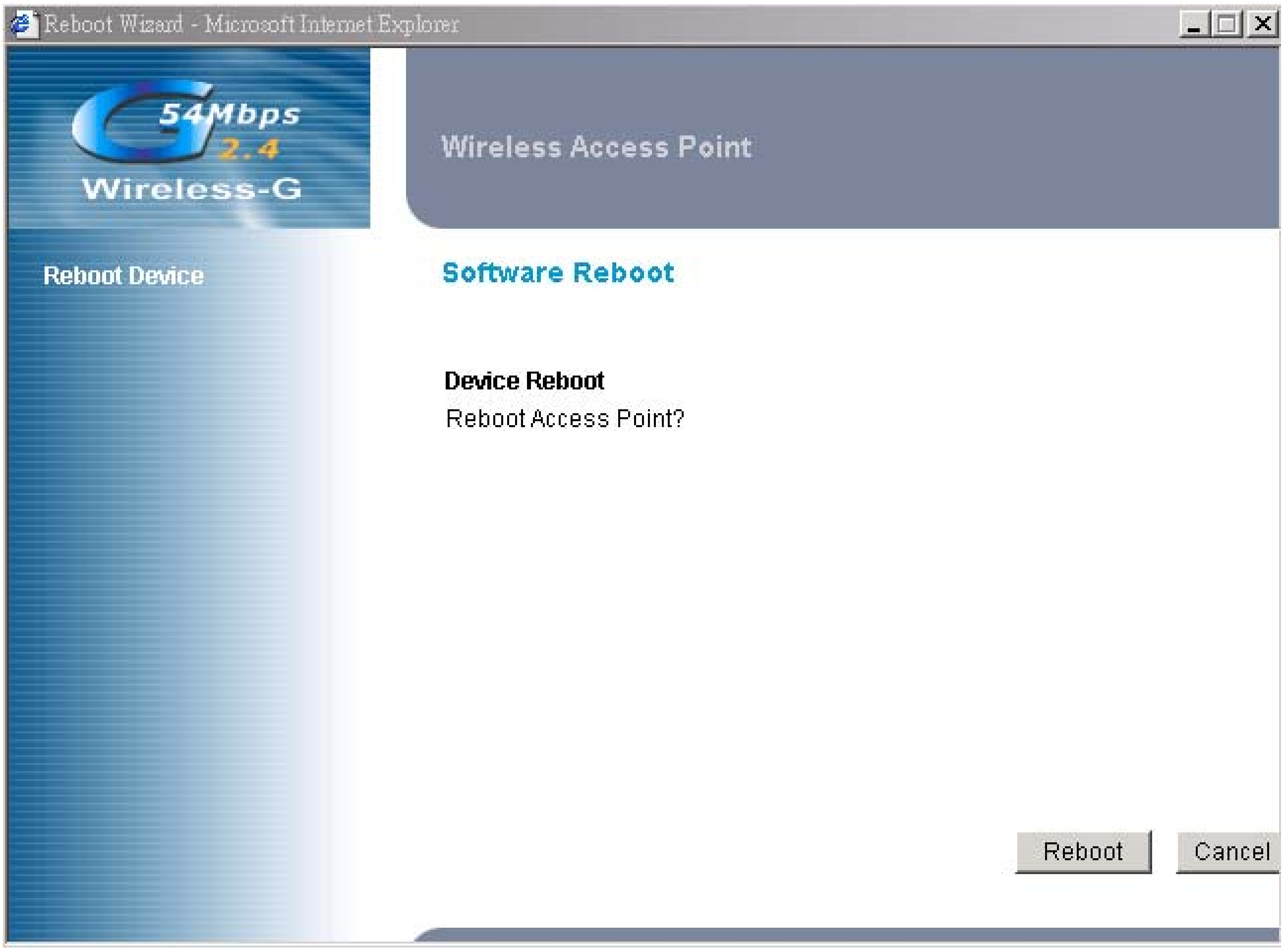


Firmware upgrade

Select the firmware file to upload and start the upgrade

4.8 Reboot Access Point

This function provides AP performing an initial action by web management. Same result could be done by power off/on this unit.

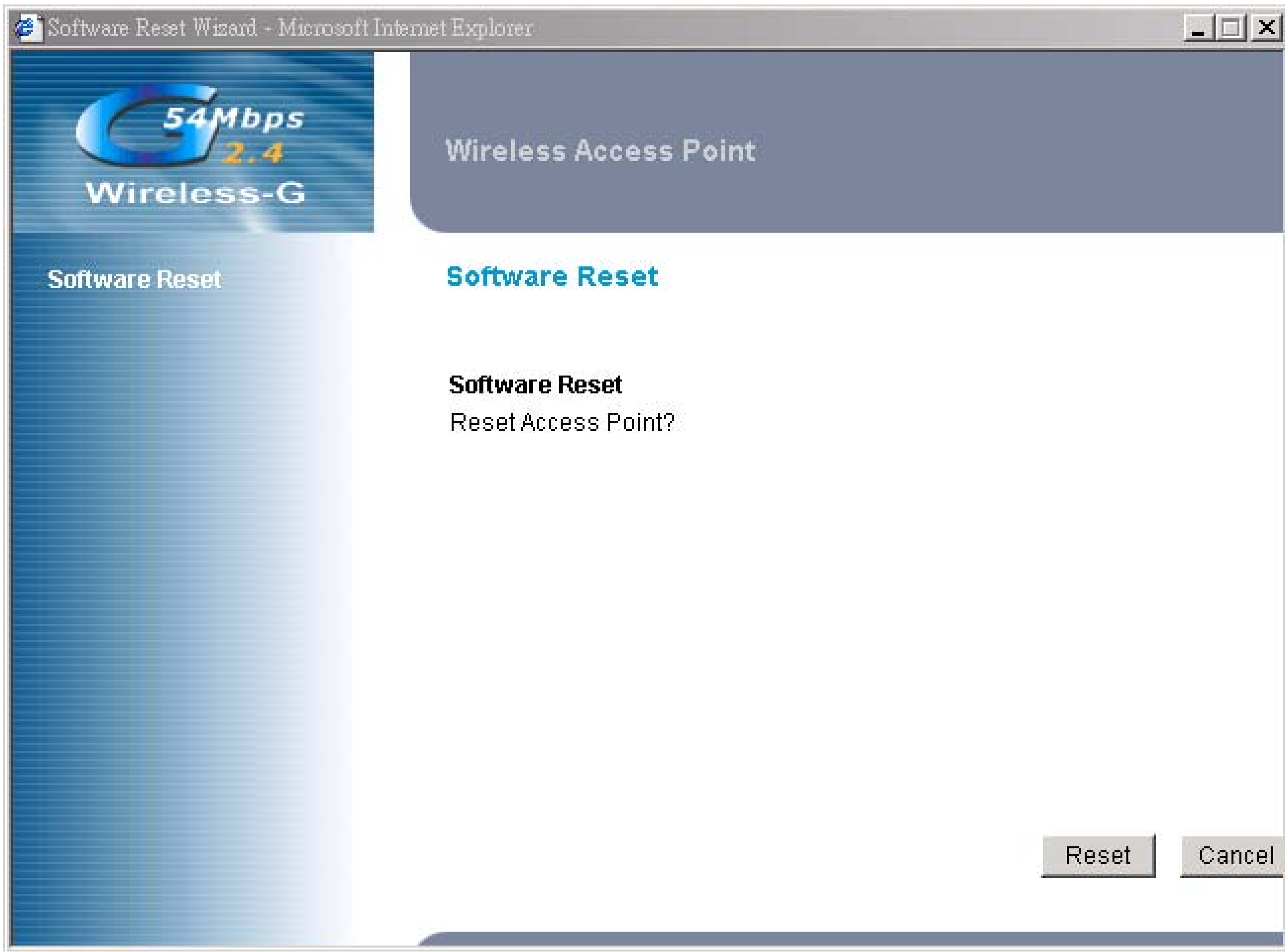


Device Reboot

Reboot Access Point?

4.9 Restore Factory Defaults

Click the **Reset** 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.

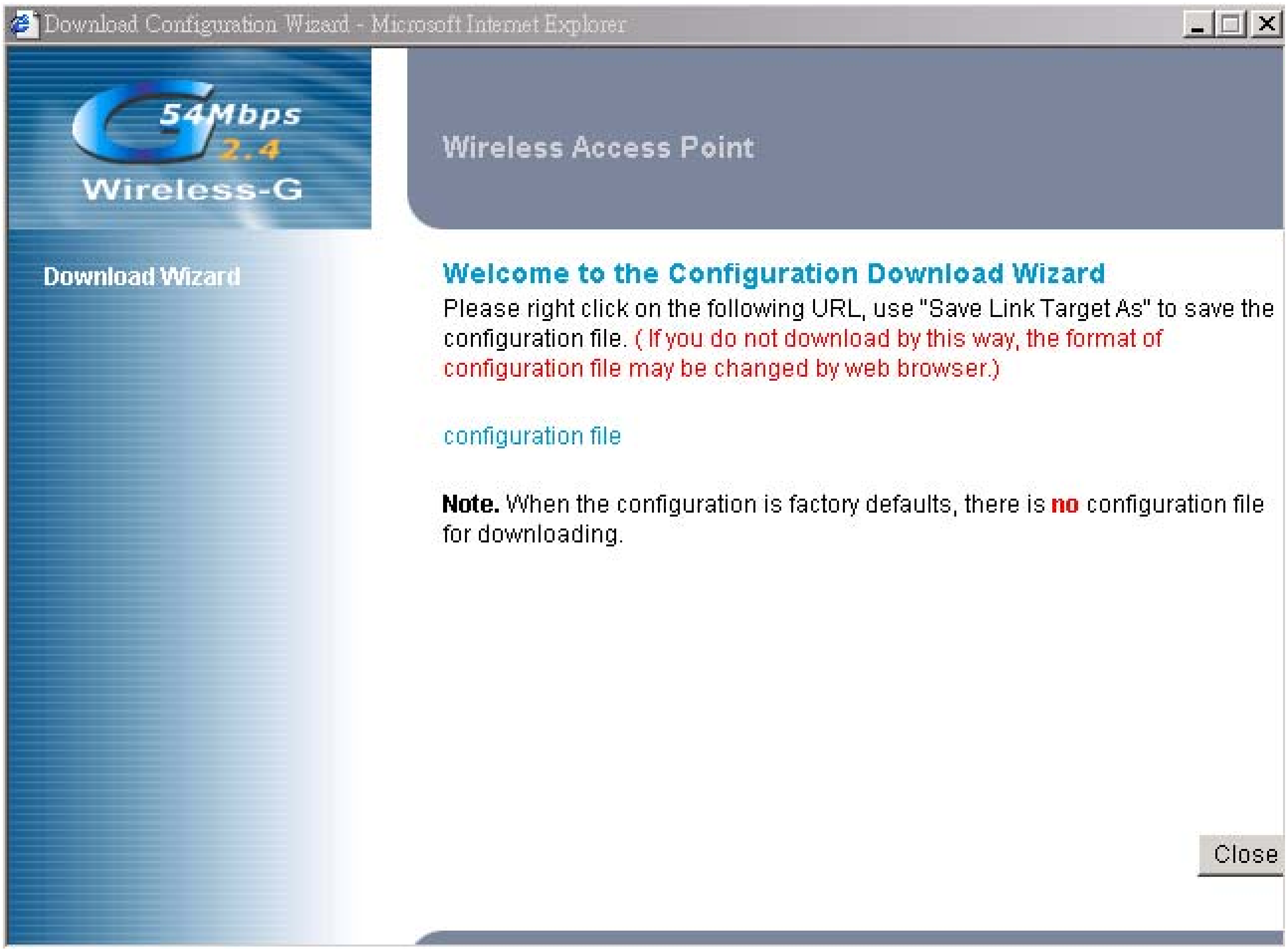


Software Reset

Software Reset
Reset Access Point?

4.10 Configuration Profile Download

This function provides AP configuration download, user can save current AP settings in one profile for later restored usage. Using this way can save more time for configure this device again if it has been reset factory default.



Welcome to the Configuration Download Wizard

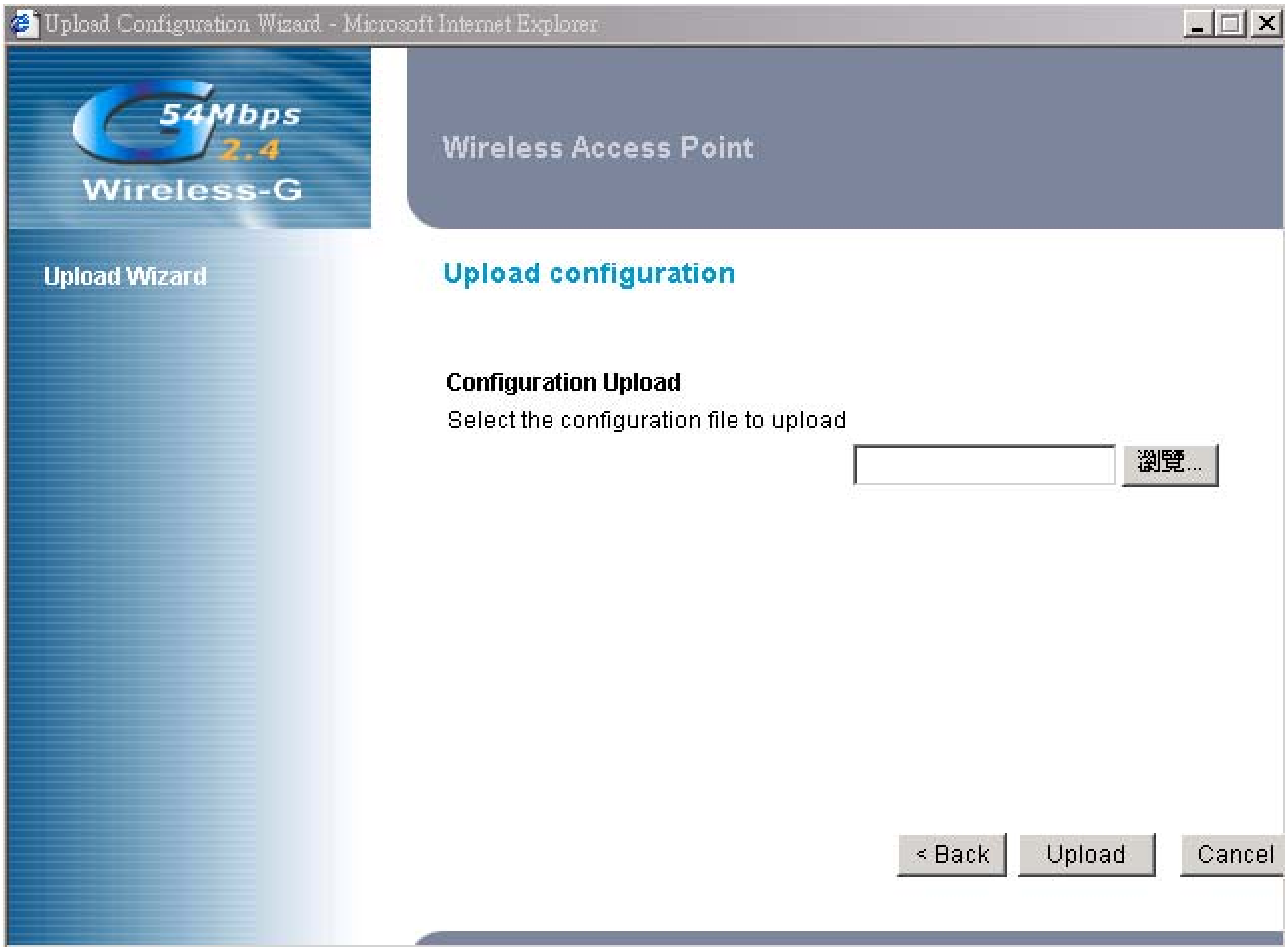
Please right click on the following URL, use "Save Link Target As" to save the configuration file. (If you do not download by this way, the format of configuration file may be changed by web browser.)

configuration file

Note. When the configuration is factory defaults, there is **no** configuration file for downloading.

4.11 Configuration Profile Upload

This function provides AP configuration upload, user can use profile that saved before for restore this unit.



Upload configuration

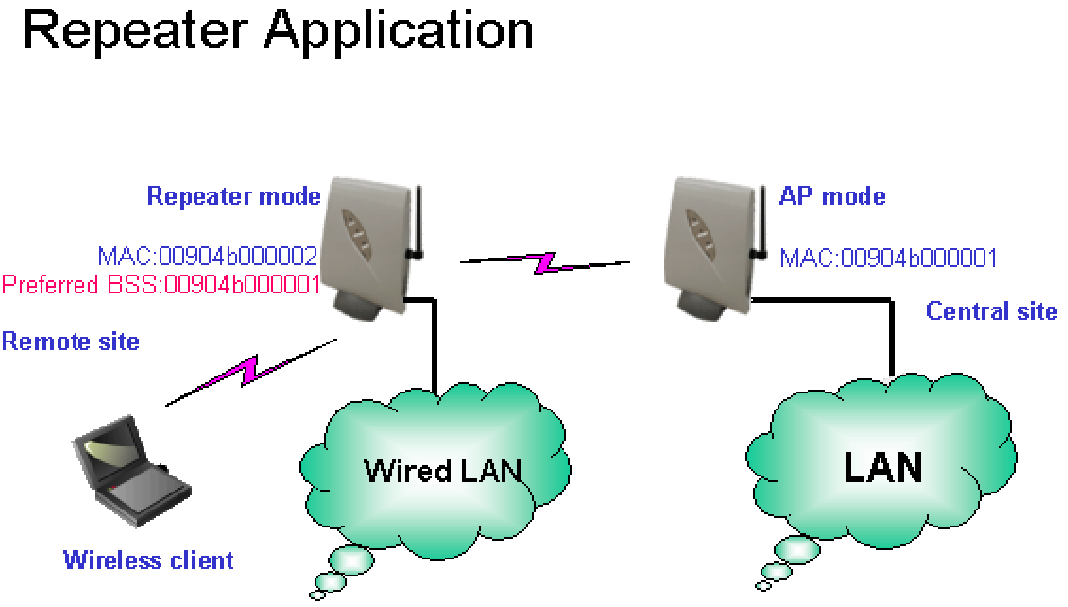
Configuration Upload

Select the configuration file to upload

5. Appendix

WDS Links Application: Enable WDS function can perform following application

WDS (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.



6. Troubleshooting

Basic Functions

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

Cause:

- The power is not connected.

Resolution:

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

Note: Only use the power 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.