LevelOne

WAP-0003

11g Wireless Access Point

User`s Manual

Contents

1. Overview

LevelOne WAP-0003 11g Wireless Access Point is designed to meet the need of wireless clients who use 2.4GHz 802.11b/g compliant wireless networking devices such as PC Card. With the Dual-Standard capability, not only seamless but also simultaneous wireless data transmission between AP and all wireless client using both b and g cab be sustained. Network setup can be installed by the simple setup wizard, which is provided as part of the web management utility or by manually configured for the advanced settings. SNMP management is also supported to make central network management an easy task for corporation IT personnel.

Wireless network protection can be ensured by WEP encryption, Wi-Fi Protected Access(WPA) and 802.1x authentication to achieve maximum level of security.

LevelOne WAP-0003, 2.4GHz 802.11g/b Wireless Access Point offers unbeatable performance for both data throughput and range coverage, which is an ideal device to be deployed not only in complex Enterprise corporations networking infrastructure and metropolitan area but also in simple SOHO and home environments

1.1 Product Feature

- Compliance with IEEE 802.11g and 802.11b standards
- Highly efficient design mechanism to provide unbeatable performance
- Achieving data rate up to 54Mbps for 802.11g and 11Mps for 802.11b with wide range coverage; high performance to deliver up to 108Mbps raw data rate for 802.11g
- Strong network security with WEP and 802.1X encryption
- 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
- One CD-ROM drive
- At least one RJ-45 Ethernet network adapter installed.

2. Getting Start

2.1 Know the WAP-0003, 11g Wireless Network Access Point

Ports:

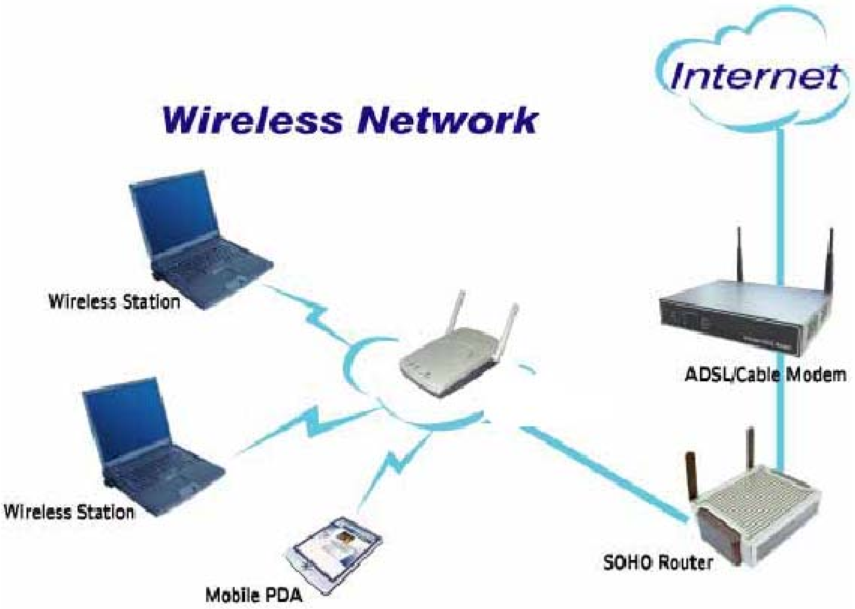
- Power Receptor
- Reset Button
- RJ-45 Ethernet Port
  Straight through cable is required to connect with router or switch
  Cross-over cable is required to connect to computer directly

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 WAP-0003, 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, you will need the following:

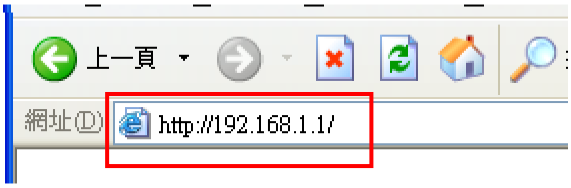
1. A broadband Internet connection.
2. ADSL or Cable modem provided by your ISP as part of the broadband connection installation.
3. A Router that connects to the ADSL/Cable modem for Internet connection sharing.
4. An Access Point to connect with the Router to form a wireless infrastructure network.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

2.3 Quick Setup with Wizard

2.3.1 Access the Setting Menu

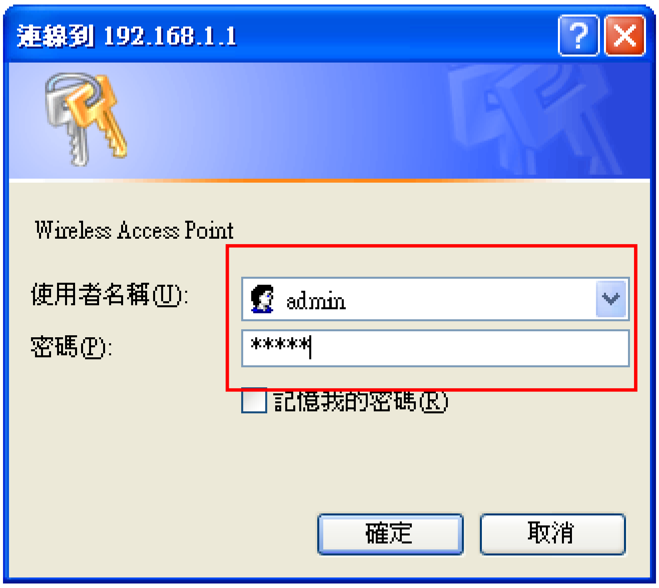
You could start to access the configuration menu anytime by opening a web browser window by typing the IP address of this access point. The default IP is 192.168.1.1.

Be sure that the IP of your PC is 192.168.1.XXX



網址(D) http://192.168.1.1/

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

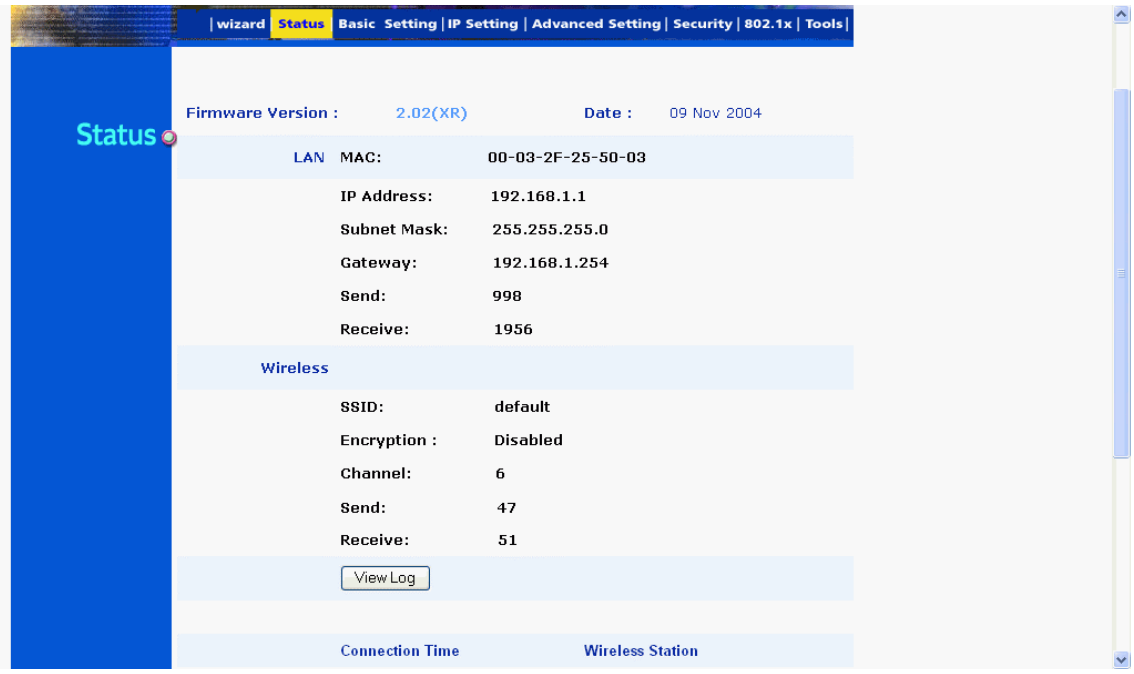

連線到 192.168.1.1

Wireless Access Point

使用者名稱(U): admin

密碼(P): *****

□ 記憶我的密碼(R)


| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
Status

Firmware Version : 2.02(XR) Date : 09 Nov 2004

LAN

MAC:	00-03-2F-25-50-03
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.254
Send:	998
Receive:	1956

Wireless

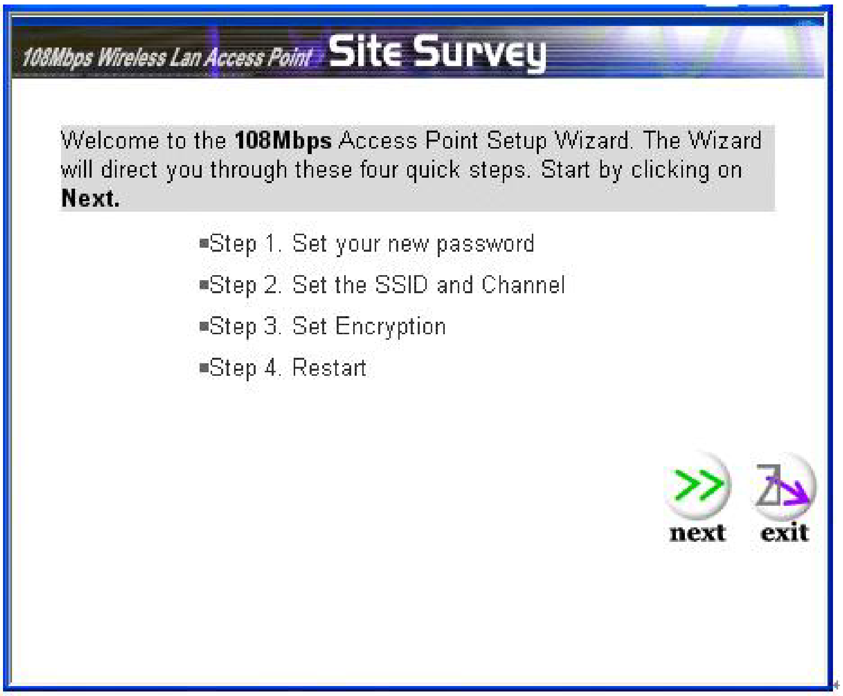
SSID:	default
Encryption :	Disabled
Channel:	6
Send:	47
Receive:	51

View Log
Connection Time
Wireless Station

Now, the main menu screen is popup.

2.3.2 Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. You can simply follow the step-by-step process to get your 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.

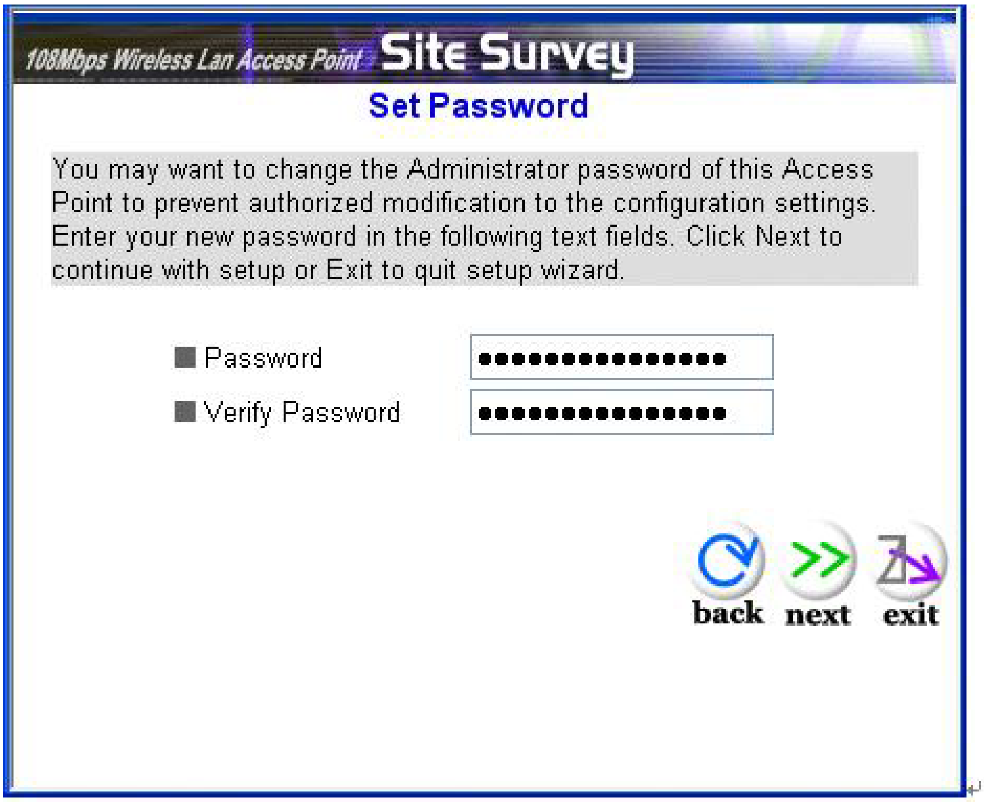


Welcome to the **108Mbps** Access Point Setup Wizard. The Wizard will direct you through these four quick steps. Start by clicking on **Next.**

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

Step 1: Set Password

You can change the password as you like and then click “**Next”** to continue.



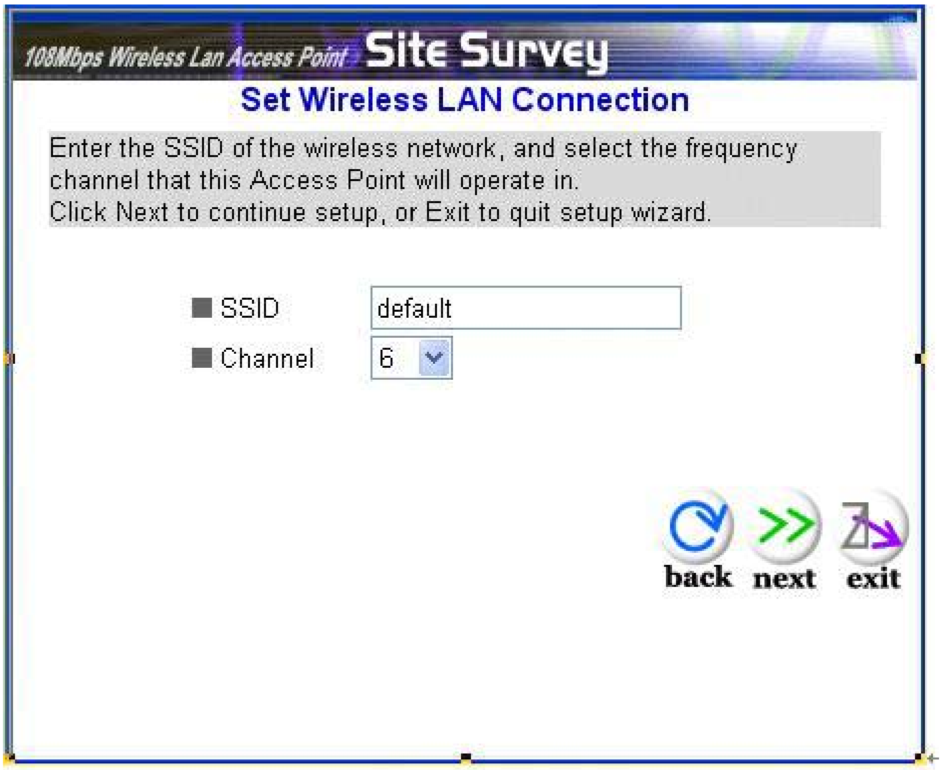
Set Password

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 you like and select the channel. Then, click "**Next**" to continue.



Set Wireless LAN Connection

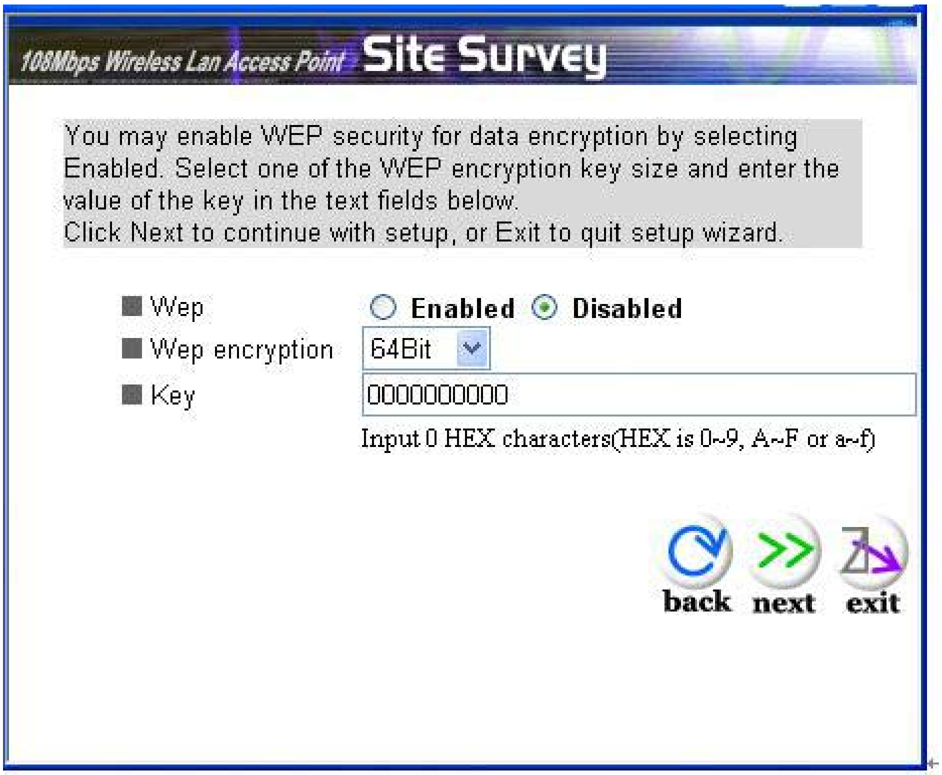
Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in.
Click Next to continue setup, or Exit to quit setup wizard.

■ SSID: default

■ Channel: 6

Step 3: Set WEP Encryption

If you like 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.



108Mbps Wireless Lan Access Point Site Survey

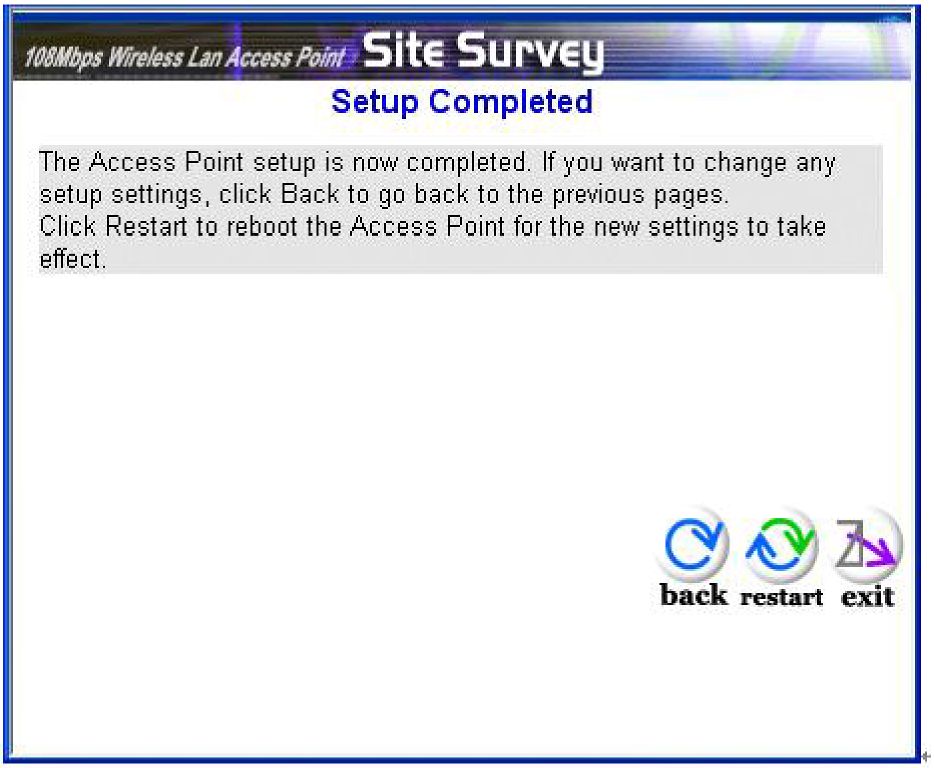
You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below.
Click Next to continue with setup, or Exit to quit setup wizard.

- Wep ○ Enabled ● Disabled
- Wep encryption 64Bit
- Key 0000000000

Input 0 HEX characters(HEX is 0~9, A~F or a~f)

Step 4: 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 you do not want to make any changes, please click “**exit**” to quit without any changes. You also can go back to modify the setting by clicking “**Back**”.



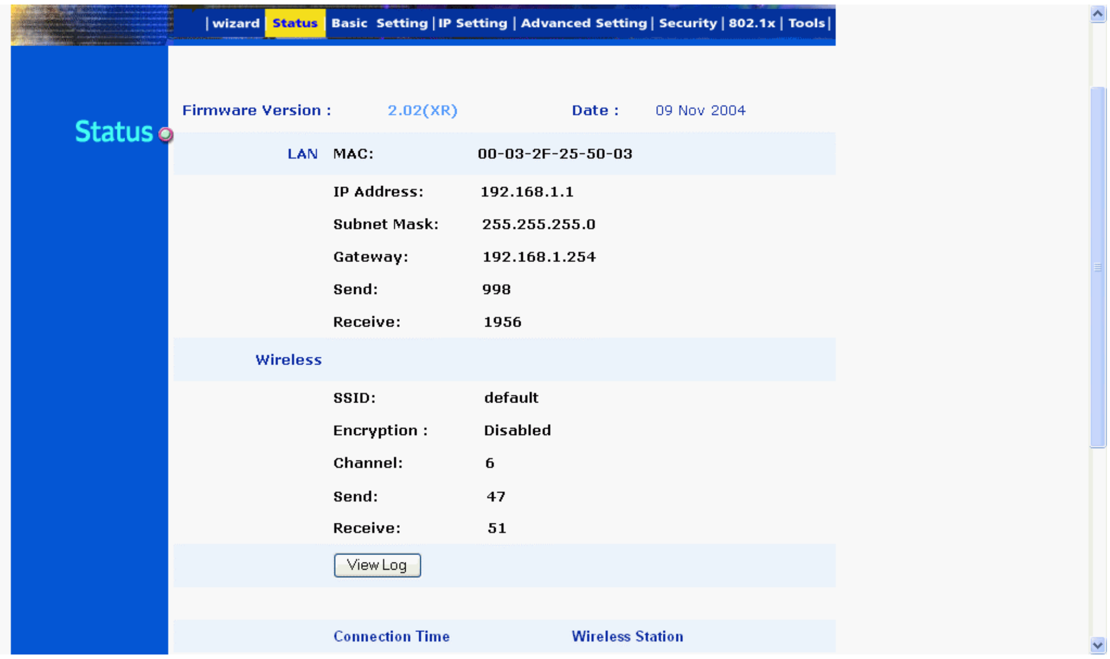
Setup Completed

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.

3. Configuration through WEB Browser

3.1 Status

This page as below shows you the following information.


| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
Status
View Log

Firmware Version : 2.02(XR) Date : 09 Nov 2004

LAN MAC: 00-03-2F-25-50-03

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Send: 998

Receive: 1956

Wireless

SSID: default

Encryption : Disabled

Channel: 6

Send: 47

Receive: 51

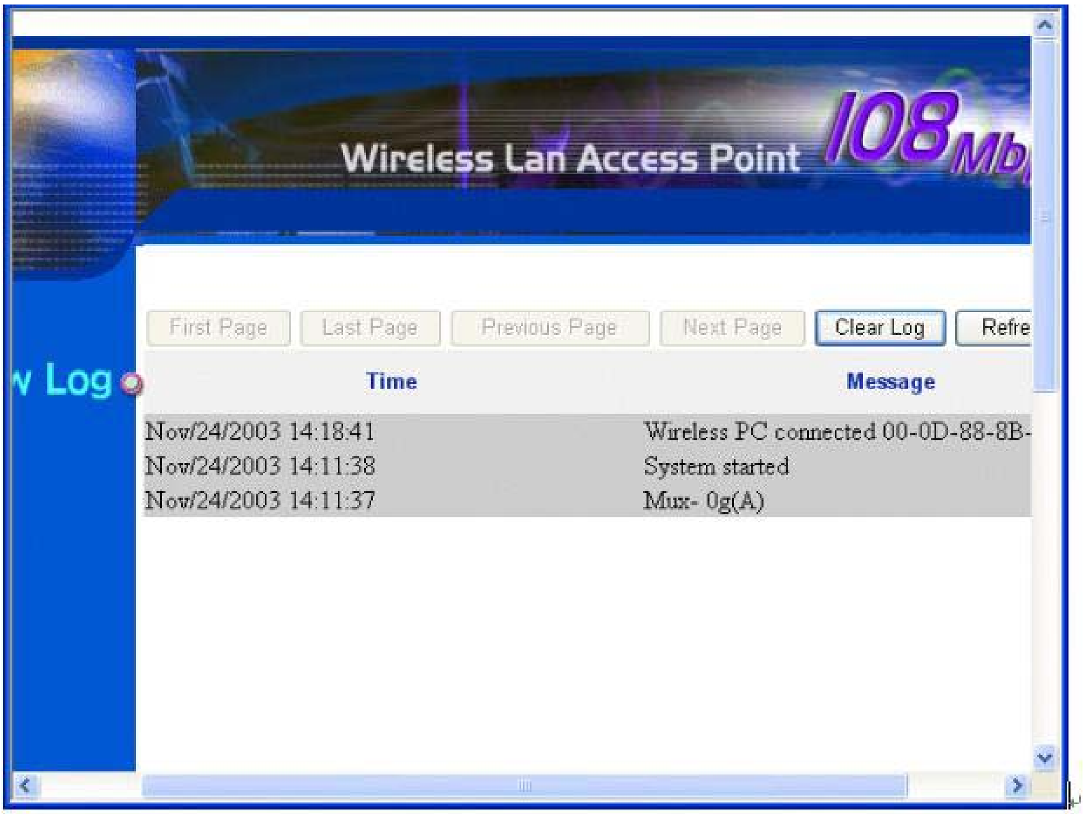
Connection Time Wireless Station

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

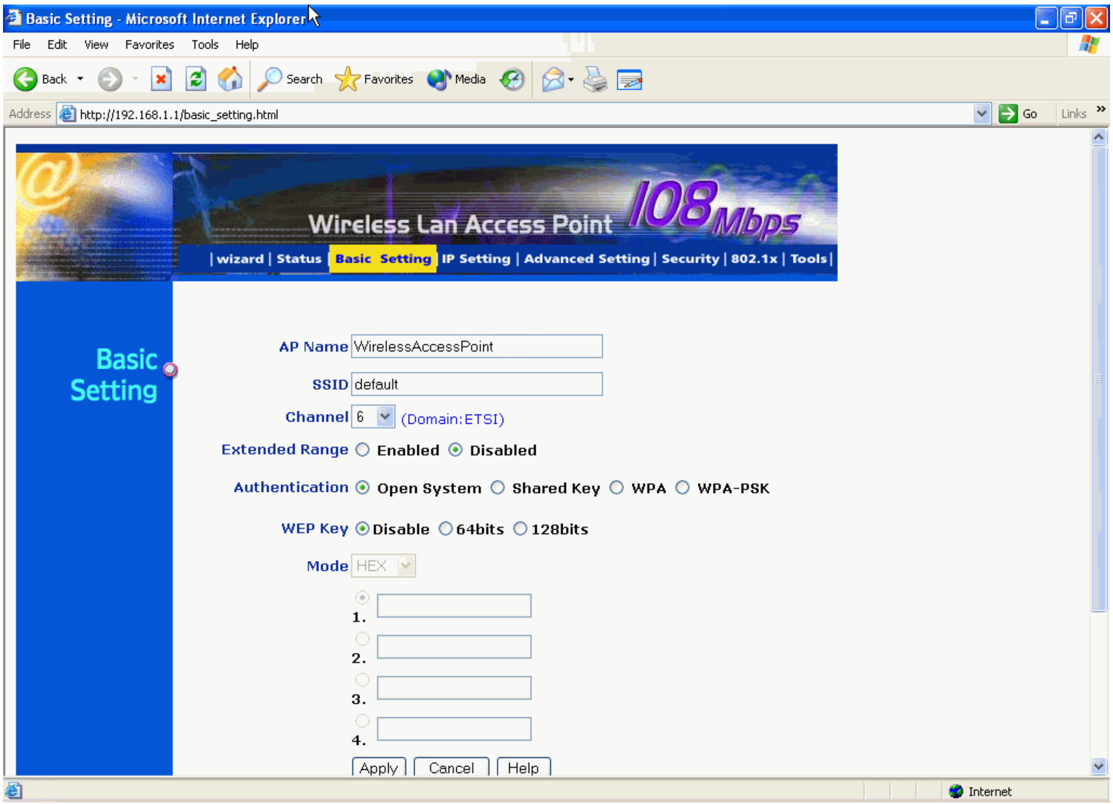


Time	Message
Nov/24/2003 14:18:41	Wireless PC connected 00-0D-88-8B-
Nov/24/2003 14:11:38	System started
Nov/24/2003 14:11:37	Mux- 0g(A)

You 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 you to change the access point.


Basic Setting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.1.1/basic_setting.html
Go
Links
Wireless Lan Access Point
108Mbps
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
Basic Setting
Internet

AP Name WirelessAccessPoint

SSID default

Channel 6 (Domain:ETSI)

Extended Range ○ Enabled ● Disabled

Authentication ● Open System ○ Shared Key ○ WPA ○ WPA-PSK

WEP Key ● Disable ○ 64bits ○ 128bits

Mode HEX

● 1.

○ 2.

○ 3.

○ 4.

Apply Cancel Help

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. You 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.

Extended Range: When you enable this function, AP will reduce data rate with a long distance. Please be noted that once you enable the Extended Range, Super G will be disabled or none-functional.

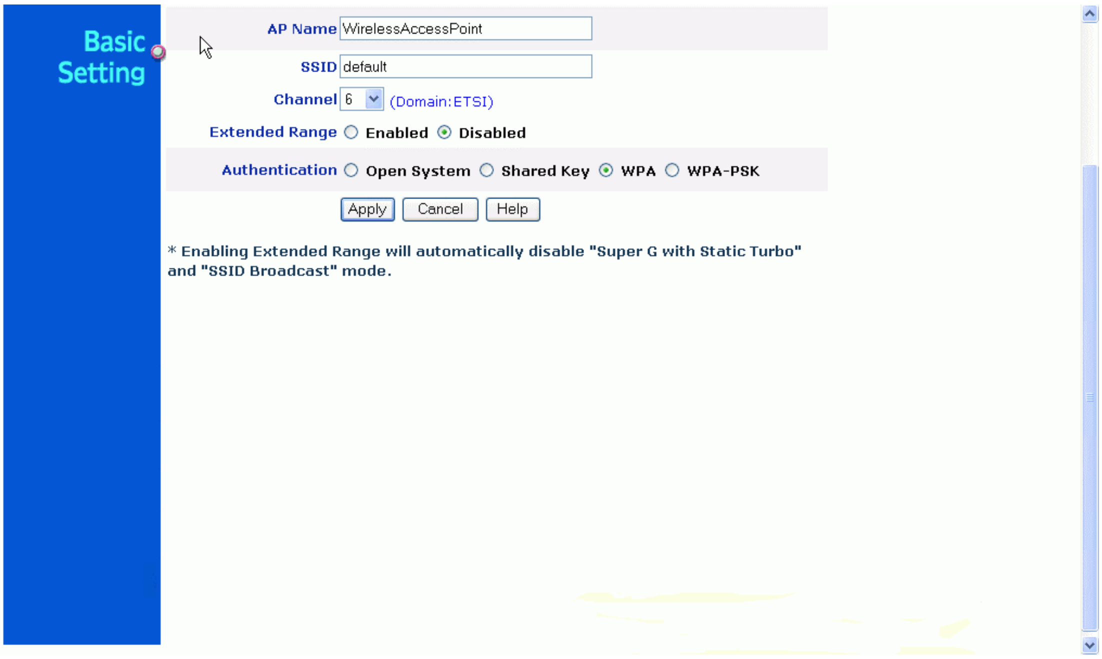
Authentication Type: The authentication type default is set to open system. There are four options: open system; shared key; WPA; WPA-PKS. You may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use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

WPA is available in authentication mode as the below screen. It is required to set 802.1X setting first before you use WPA.



AP Name WirelessAccessPoint

SSID default

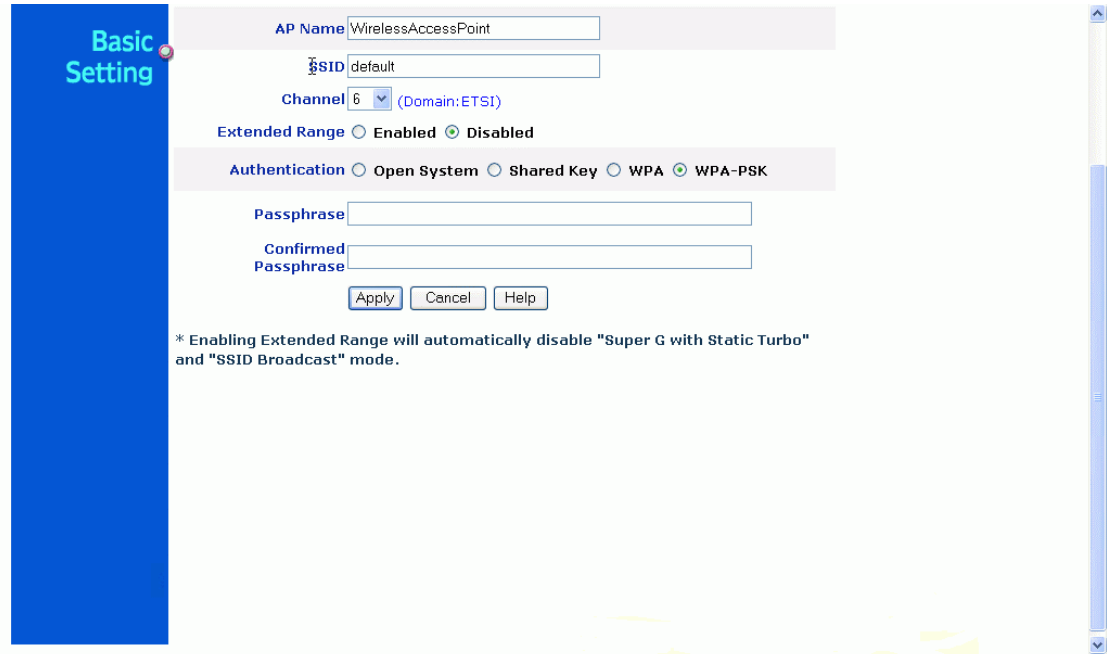
Channel 6 (Domain:ETSI)

Extended Range ○ Enabled ● Disabled

Authentication ○ Open System ○ Shared Key ● WPA ○ WPA-PSK

* Enabling Extended Range will automatically disable "Super G with Static Turbo" and "SSID Broadcast" mode.

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.



AP Name: WirelessAccessPoint

SSID: default

Channel: 6 (Domain:ETSI)

Extended Range: ○ Enabled ● Disabled

Authentication: ○ Open System ○ Shared Key ○ WPA ● WPA-PSK

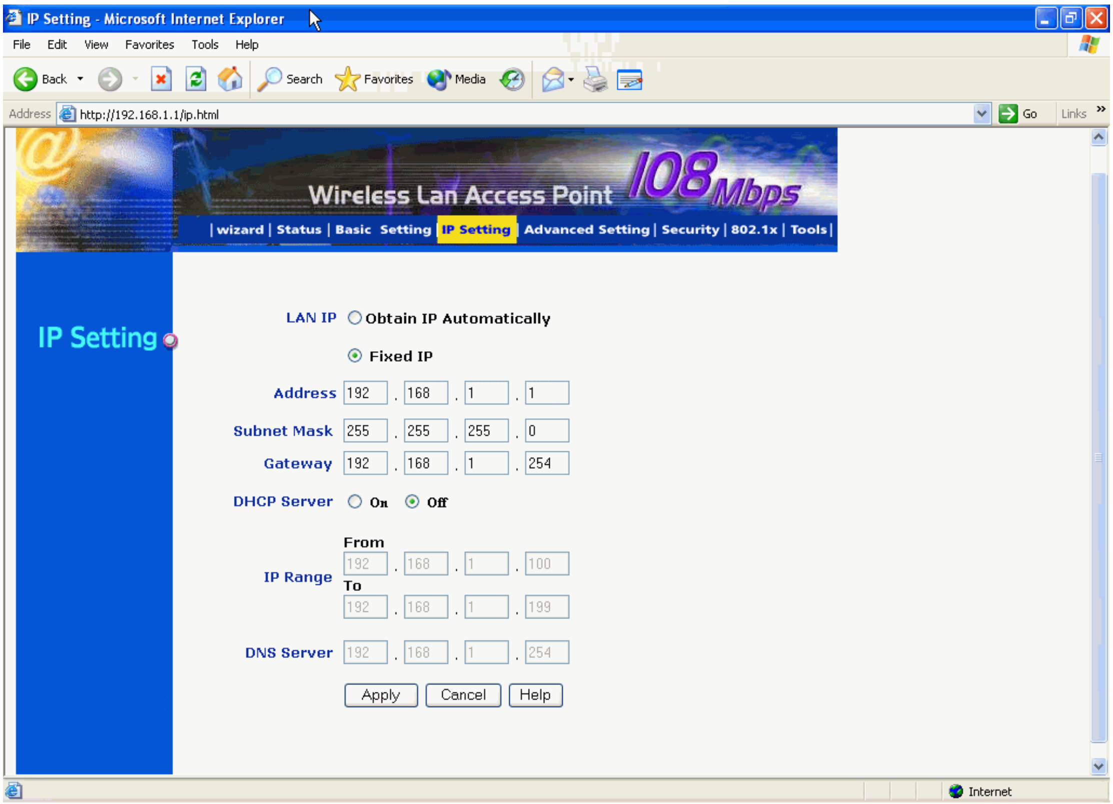
Passphrase:

Confirmed Passphrase:

* Enabling Extended Range will automatically disable "Super G with Static Turbo" and "SSID Broadcast" mode.

3.3 IP Setting

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


IP Setting - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://192.168.1.1/ip.html
Go
Links
Wireless Lan Access Point
108Mbps
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
IP Setting
Internet

LAN IP: ○ Obtain IP Automatically ● Fixed IP

Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 254

DHCP Server: ○ On ● Off

IP Range: From 192 . 168 . 1 . 100 To 192 . 168 . 1 . 199

DNS Server: 192 . 168 . 1 . 254

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

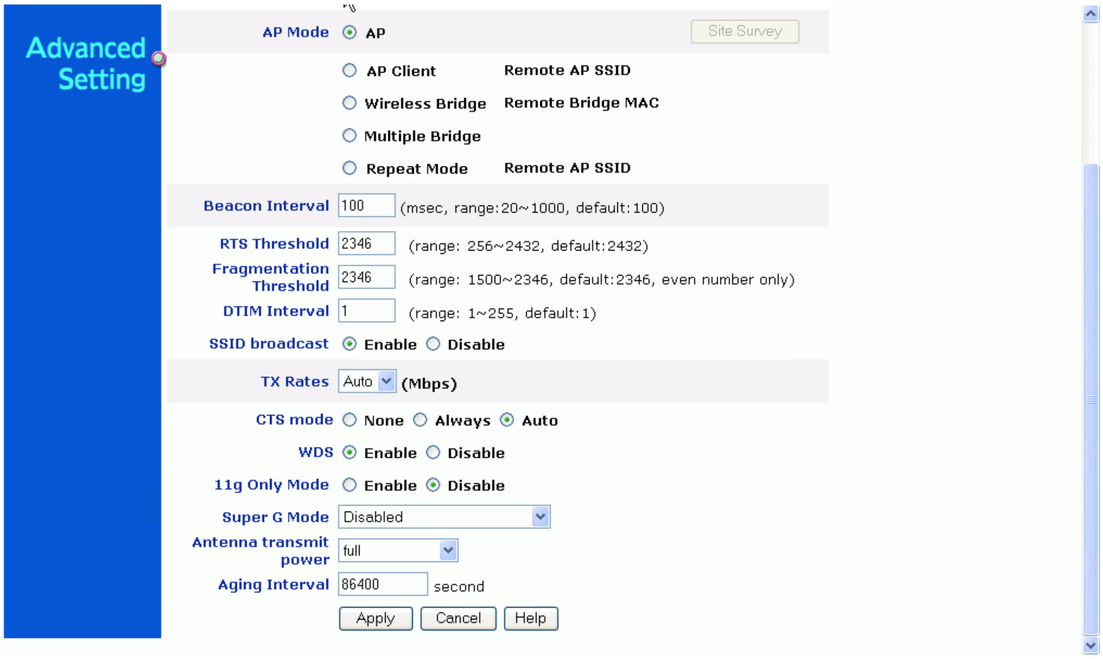
You can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server: It is not recommended to enable the DHCP Server if you have a DHCP server running in your 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.

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

3.4 Advanced Setting

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



AP Mode ● AP
○ AP Client Remote AP SSID
○ Wireless Bridge Remote Bridge MAC
○ Multiple Bridge
○ Repeat Mode Remote AP SSID

Beacon Interval 100 (msec, range:20~1000, default:100)

RTS Threshold 2346 (range: 256~2432, default:2432)

Fragmentation Threshold 2346 (range: 1500~2346, default:2346, even number only)

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

SSID broadcast ● Enable ○ Disable

TX Rates Auto (Mbps)

CTS mode ○ None ○ Always ● Auto

WDS ● Enable ○ Disable

11g Only Mode ○ Enable ● Disable

Super G Mode Disabled

Antenna transmit power full

Aging Interval 86400 second

AP Mode: Select one of the AP operating modes for different application of Access Point.

1. **AP** – The normal Access Point operating mode which forms a wireless ESS network with its wireless clients.

2. **AP Client** – Acts as an Ethernet-to-Wireless Bridge, which allows a LAN or a single computer station to join a wireless ESS network through it. You must make sure SSID and Channel is set the same as that AP you wish to connect.

Remote AP BSS ID: key in the LAN Mac address (NOT wireless Mac address) of the AP that you wish to get connected. Please note that if you leave Mac address as 000000000000, then you will get connected by the SSID that is set in you AP.

3. **Wireless Bridge** – A pair of APs operating under Bridge mode to act as the bridge that connect two Ethernet networks or Ethernet enabled clients together. You must make sure that the SSID and Channel is set the same as that AP you wish to connect.

Remote Bridge MAC filed: key in the **LAN Mac address** (NOT wireless Mac address) of the AP that you wish to get connected.

4. **Multiple Bridge** – A group of APs which consists of two or more APs operating under Multiple Bridge mode, that can connect two or more Ethernet networks or Ethernet enabled clients together.

5. **Repeat Mode**: It is able to extend the effective range and coverage of the wireless network. Please make sure the SSID is the same as that AP you want to extend.

Note**:** All APs have to use the same **Channel** and **SSID** in order to set a Multiple Bridge network.

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 2436 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, you may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point.

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.

CTS Mode(clear to send): None- disable CTS function. Always- Regardless of wireless environment (11b or 11g), platform will always transfer 11b packet.

Auto- AP soon detected the wireless environment and decided the transmission packet, either 11b or 11g.

WDS (Wireless Distribution System): Only use in AP mode. WDS mode allows WAP-0003 to communicate with other Wireless AP in repeater or bridge mode. It is convenient for you to set up your wireless environment.

11g mode only: User can use 11g only when he selects “enable”.

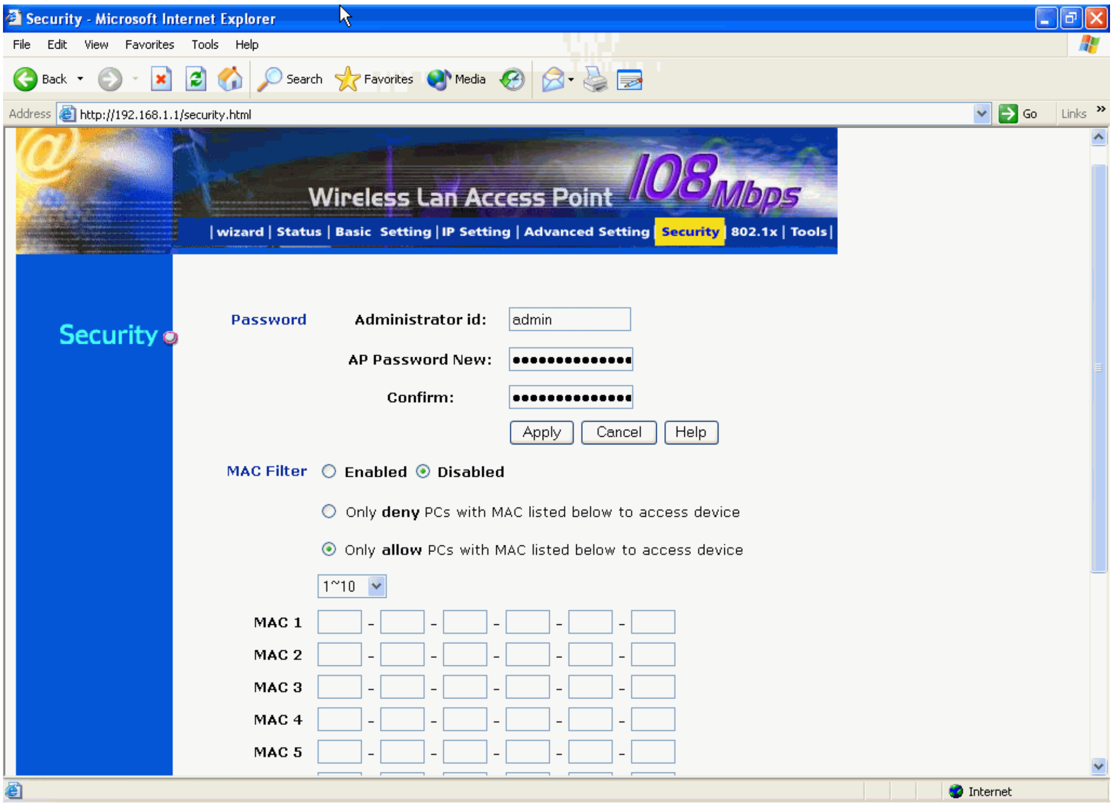
Super G mode: Super G mode is disabled if selecting “Disable” from the drop list. If you like to use Super G to enhance the speed, there are three options on Super G mode: Super G without turbo; Super G with Dynamic turbo and Super G with Static turbo. Turbo mode indicates the combination of two channels to enhance the throughput. Super G without turbo indicates that it is on Super G mode without the channel’s combination. Dynamic turbo is able to automatically detect if any ‘SuperG based’ product is available. If no, the connection is via ‘normal’ G.. Static turbo means it will not go back to ‘normal’ G once it starts.

Antenna Transmit Power: Adjust the power of the antenna transmission by selecting from the dropping list.

Aging Interval: To limited STA connect timing.

3.5 Security

This page is where you configure the security features supported by this Access Point.



Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
Wireless Lan Access Point 108Mbps
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
Security
Apply
Cancel
Help
Internet

Address: http://192.168.1.1/security.html

Password

Administrator id: admin

AP Password New: ••••••••••••••

Confirm: ••••••••••••••

MAC Filter ○ Enabled ● Disabled

○ Only **deny** PCs with MAC listed below to access device

● Only **allow** PCs with MAC listed below to access device

1~10

MAC 1 __ - __ - __ - __ - __ - __

MAC 2 __ - __ - __ - __ - __ - __

MAC 3 __ - __ - __ - __ - __ - __

MAC 4 __ - __ - __ - __ - __ - __

MAC 5 __ - __ - __ - __ - __ - __

Password: Allow you 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

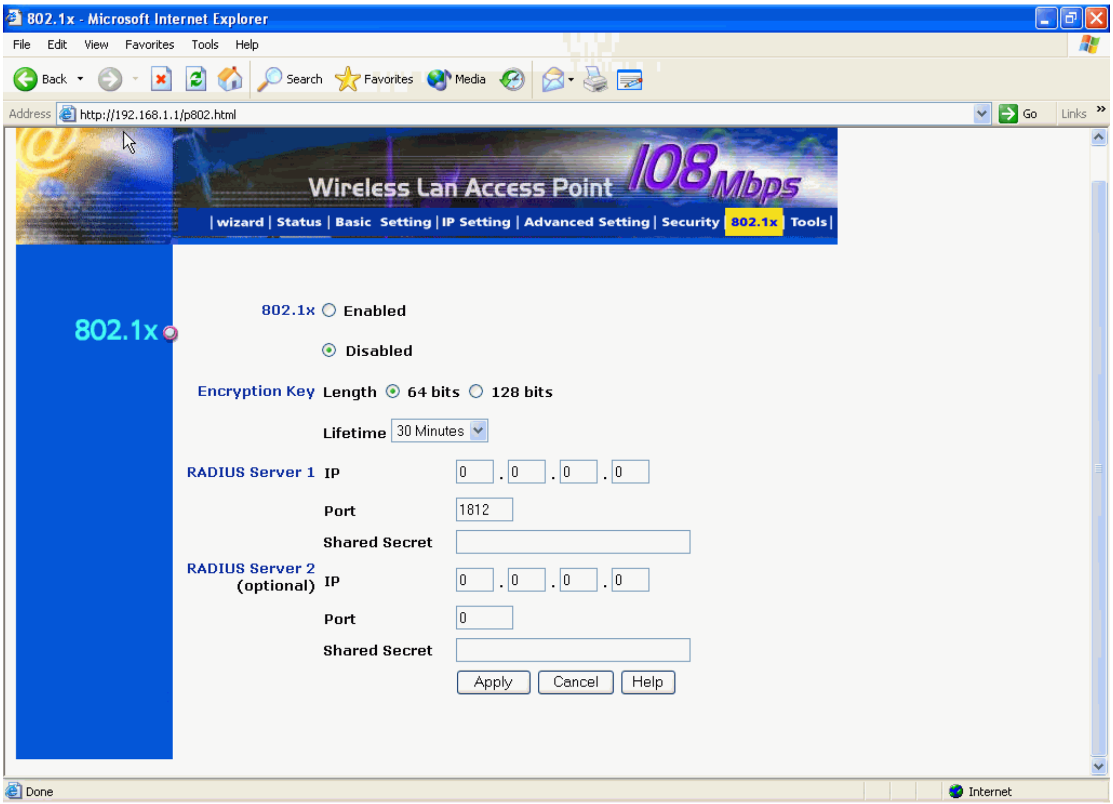
●Only allow PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. You 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.

3.6 802.1x

There are three essential components to the 802.1x infrastructure: (1) Supplicant, (2) Authenticator and (3) Server. The Access Point serves as an Authenticator, and the EAP methods used must be supported by the backend Radius Server. The 802.1x security supports MD5 and TLS Extensive Authentication Protocol (EAP). Please follow the steps below to configure 802.1x security.


802.1x - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/p802.html
Go Links
Wireless Lan Access Point 108Mbps
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools |
802.1x
Done
Internet

802.1x ○ Enabled
● Disabled

Encryption Key Length ● 64 bits ○ 128 bits

Lifetime 30 Minutes

RADIUS Server 1 IP 0 . 0 . 0 . 0

Port 1812

Shared Secret

RADIUS Server 2 (optional) IP 0 . 0 . 0 . 0

Port 0

Shared Secret

Apply Cancel Help

1. Enable 802.1x security by selecting “**Enable**”.

2. If **MD5** EAP method is used then you can skip step 2 and go to step 3.

3. Select the **Encryption Key Length Size** ranging from 64 to 128 Bits that you would like to use. Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.

4. Enter the **IP address,** the **Port** and the **Shared Secret** used by the **Primary** Radius Server.

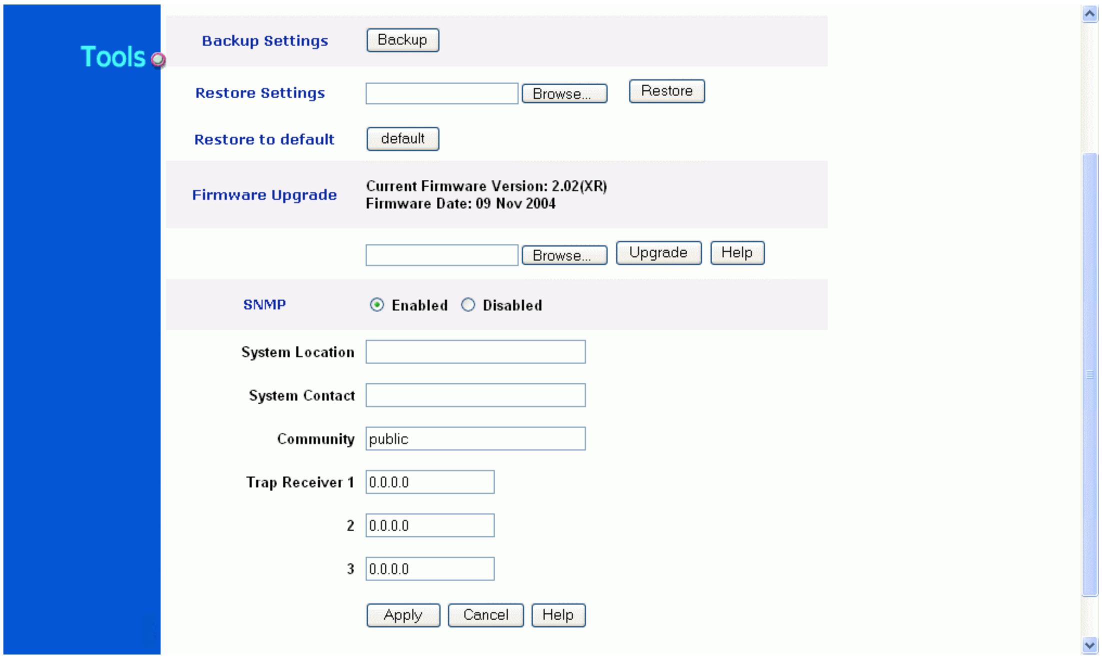
5. Enter the **IP address**, the **Port** and the **Shared Secret** used by the **Secondary** Radius Server.

6. Click “**Apply**” button for the 802.1x settings to take effect after Access Point reboots itself.

Note: As soon as 802.1x security is enabled, all the wireless client stations that are connect to the Access Point currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

3.7 Tools

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



Backup Settings

Restore Settings

Restore to default

Firmware Upgrade: Current Firmware Version: 2.02(XR)
Firmware Date: 09 Nov 2004

SNMP: ● Enabled ○ Disabled

System Location:

System Contact:

Community: public

Trap Receiver 1: 0.0.0.0

2: 0.0.0.0

3: 0.0.0.0

Backup Settings: Click on “**Backup**” button, which will open a FileSave Dialog box, where you get 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 you get to select the file, which you save 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.

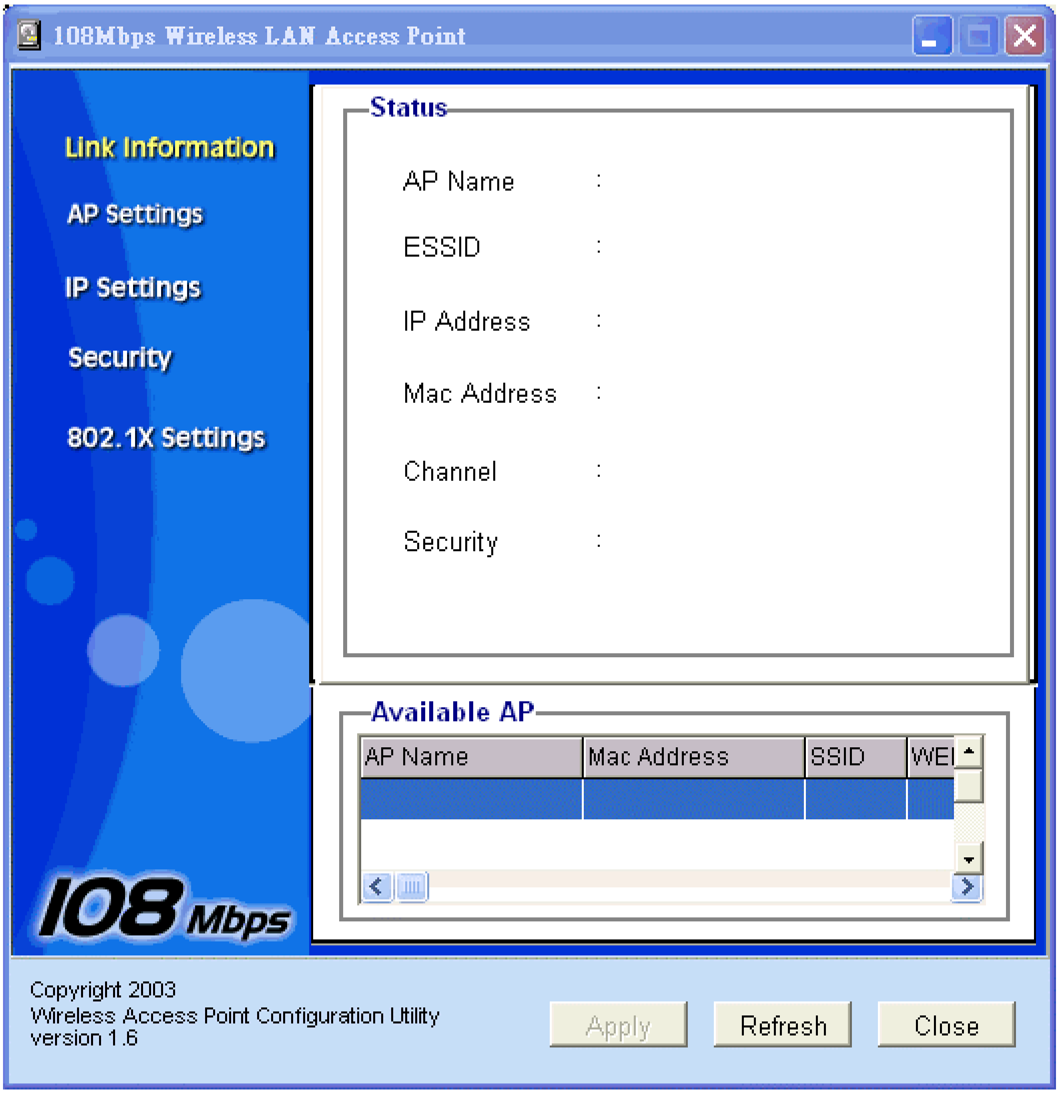
Firmware Upgrade: Click on the “**Browse**” button to open a File Open Dialog box, where you get to select the firmware file, which you download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates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

SNMP: Enable or disable.

4. Configuration through AP Utility

4.1 Link Information

Link information is showing you the related current setting of the first AP.



AP Name :

ESSID :

IP Address :

Mac Address :

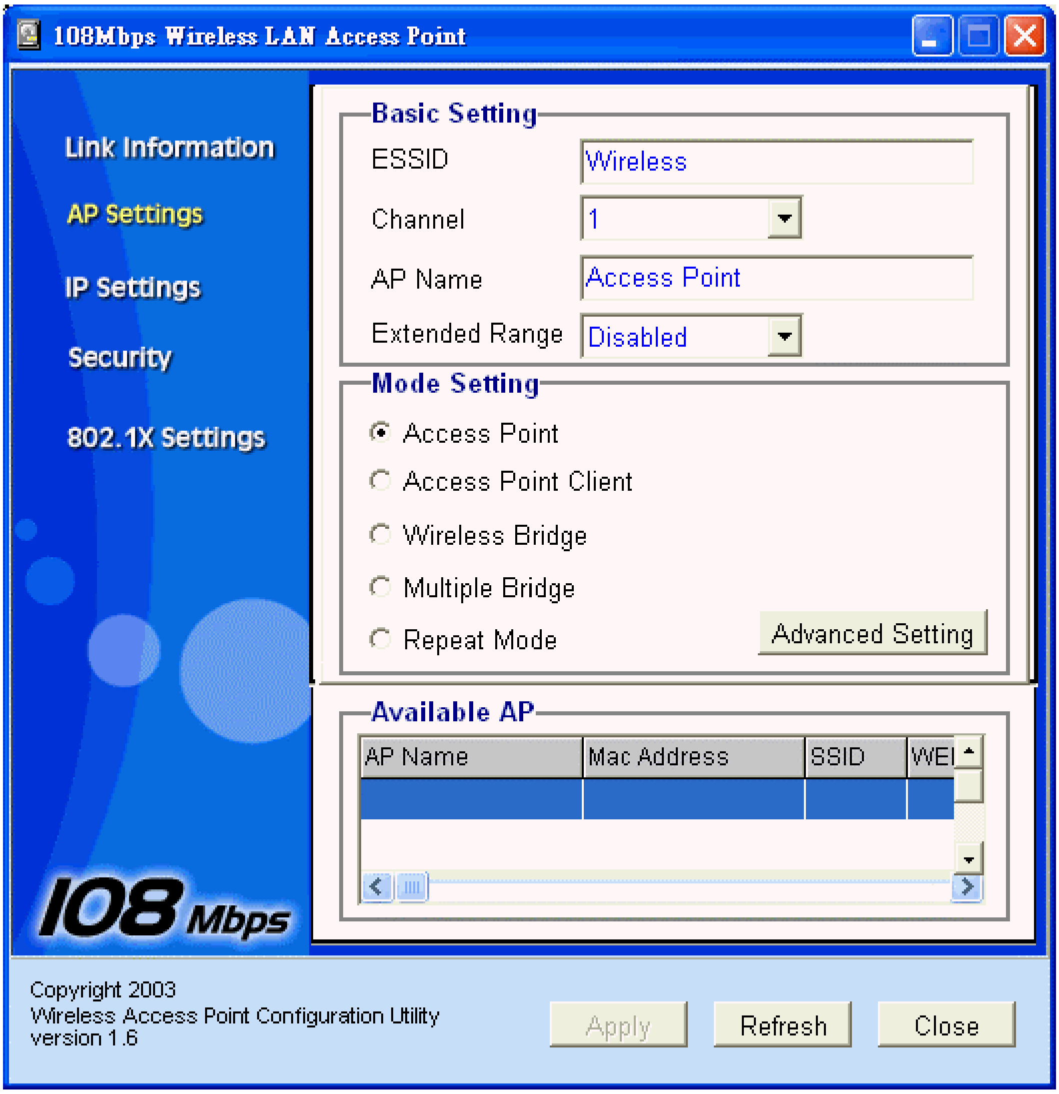
Channel :

Security :

AP Name	Mac Address	SSID	WEI

Copyright 2003
Wireless Access Point Configuration Utility
version 1.6

4.2 AP Settings



Basic Setting

ESSID: Wireless

Channel: 1

AP Name: Access Point

Extended Range: Disabled

Mode Setting

● Access Point
○ Access Point Client
○ Wireless Bridge
○ Multiple Bridge
○ Repeat Mode

Available AP

AP Name	Mac Address	SSID	WEI

Copyright 2003
Wireless Access Point Configuration Utility
version 1.6

Basic Setting:

ESSID: It is used by all wireless devices within the wireless network.

Channel: Select the appropriate channel from the dropping list. All wireless devices with the same ESSID will automatically use this channel to communicate with this access point.

AP Name: users can set the name for access point so as to easily manage the access points while there are several access points in the network.

Extended Range: When you enable this function, AP will reduce data rate with a long distance.

Mode Setting:

Access Point: This is the default for this access point. It connects the wireless PCs to wired network.

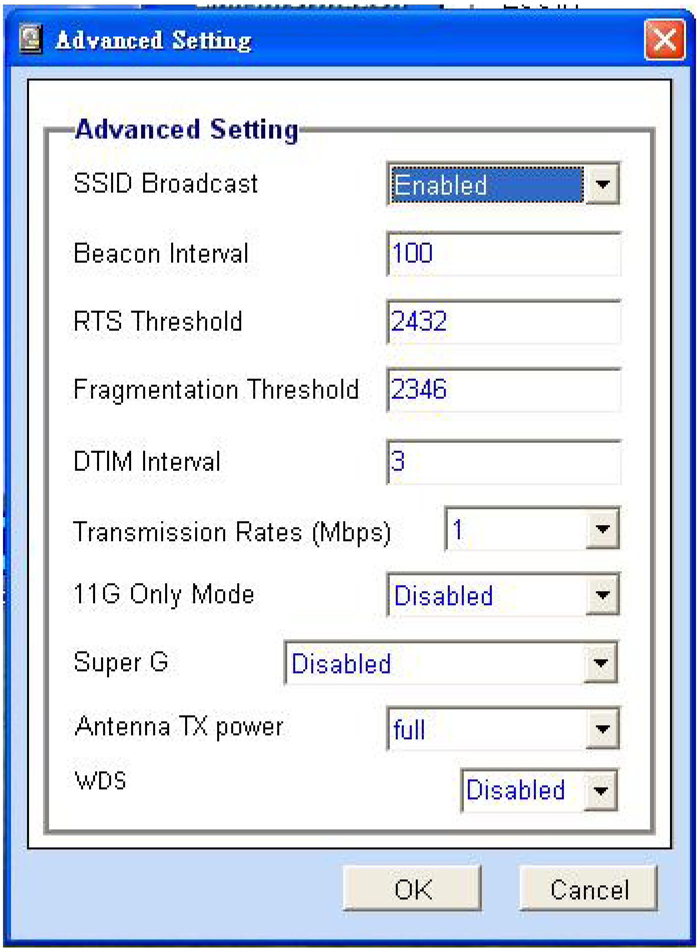
Access Point Client: Acts as an Ethernet-to-Wireless Bridge, which allows a LAN or a single computer station to join a wireless ESS network through it. You must make sure SSID and Channel is set the same as that AP you wish to connect.

Wireless Bridge: A pair of APs operating under Bridge mode to act as the bridge that connect two Ethernet networks or Ethernet enabled clients together. You must make sure that the SSID and Channel is set the same as that AP you wish to connect.

Multiple Bridge: A group of APs that consists of two or more APs operating under Multiple Bridge mode, that can connect two or more Ethernet networks or Ethernet enabled clients together.

Repeat Mode: It is able to extend the effective range and coverage of the wireless network. Please make sure the SSID is the same as that AP you want to extend.

Advanced Setting:



Advanced Setting

SSID Broadcast: Enabled

Beacon Interval: 100

RTS Threshold: 2432

Fragmentation Threshold: 2346

DTIM Interval: 3

Transmission Rates (Mbps): 1

11G Only Mode: Disabled

Super G: Disabled

Antenna TX power: full

WDS: Disabled

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

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 2436 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.

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.

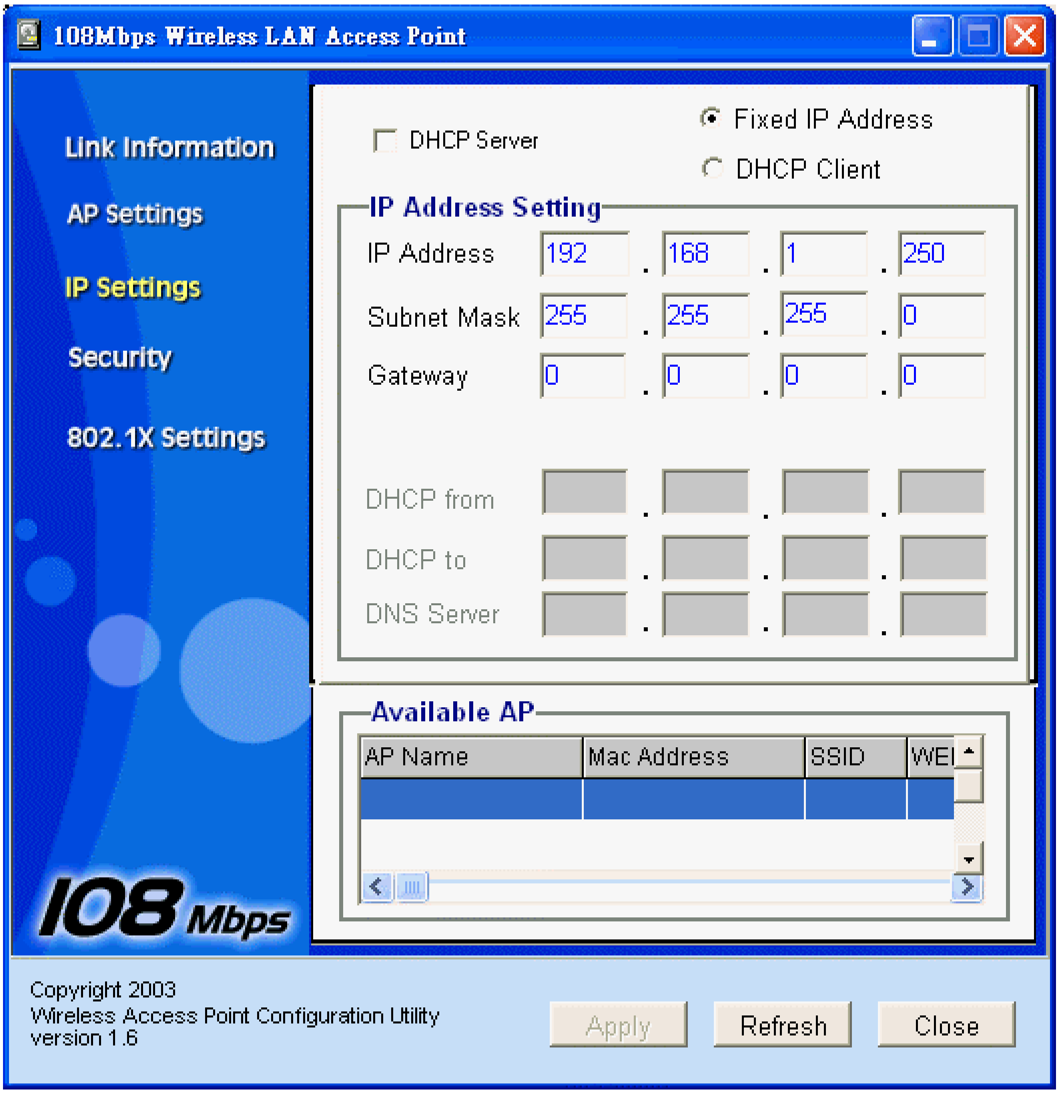
11G Only Mode: enable or disable.

Super G: Super G mode is disabled if selecting “Disable” from the drop list. If you like to use Super G to enhance the speed, there are three options on Super G mode: Super G without turbo; Super G with Dynamic turbo and Super G with Static turbo. Turbo mode indicates the combination of two channels to enhance the throughput. Super G without turbo indicates that it is on Super G mode without the channel’s combination. Dynamic turbo is able to automatically detect if any ‘SuperG based’ product is available. If no, the connection is via ‘normal’ G.. Static turbo means it will not go back to ‘normal’ G once it starts.

Antenna TX Power: Adjust the power of the antenna transmission by selecting from the dropping list.

WDS (Wireless Distribution System): Only use in AP mode. WDS mode allows WAP-0003 to communicate with other Wireless AP in repeater or bridge mode. It is convenient for you to set up your wireless environment.

4.3 IP Setting



□ DHCP Server

● Fixed IP Address

○ DHCP Client

IP Address Setting

IP Address	192	168	1	250
Subnet Mask	255	255	255	0
Gateway	0	0	0	0
DHCP from				
DHCP to				
DNS Server				

Available AP

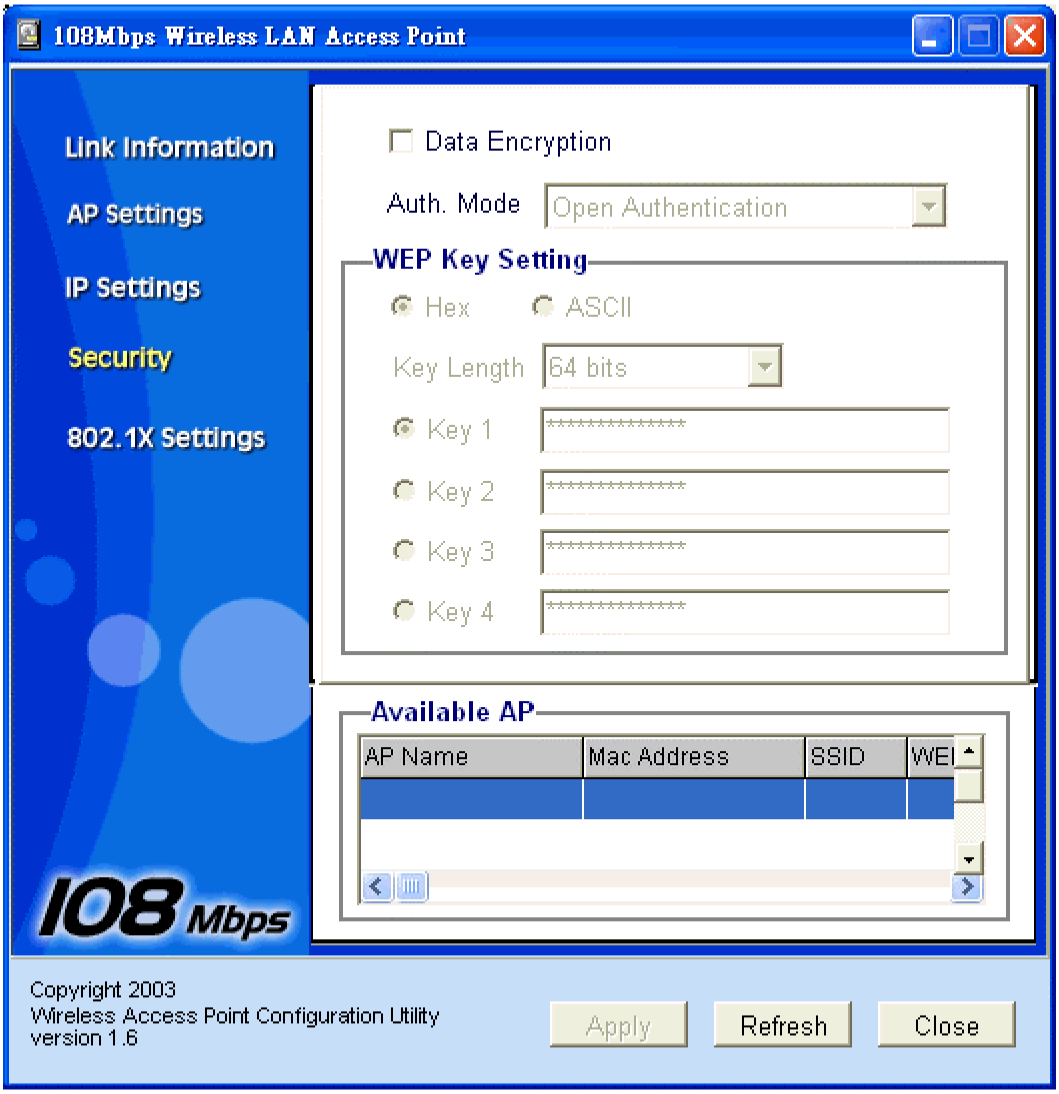
AP Name	Mac Address	SSID	WEI

Copyright 2003
Wireless Access Point Configuration Utility
version 1.6

Fixed IP Address: Users can assign a fixed IP address to this AP manually.

DHCP Client: Enable the DHCP server function by clicking the radio button if you have the DHCP server running in your LAN network. It is not recommended because it probably will cause possible the conflict of IP assignment.

4.4 Security



□ Data Encryption

Auth. Mode: Open Authentication

WEP Key Setting

● Hex ○ ASCII

Key Length: 64 bits

● Key 1 **************

○ Key 2 **************

○ Key 3 **************

○ Key 4 **************

Copyright 2003
Wireless Access Point Configuration Utility
version 1.6

Data Encryption: please tick it if you like to have WEP key as the encryption mechanism.

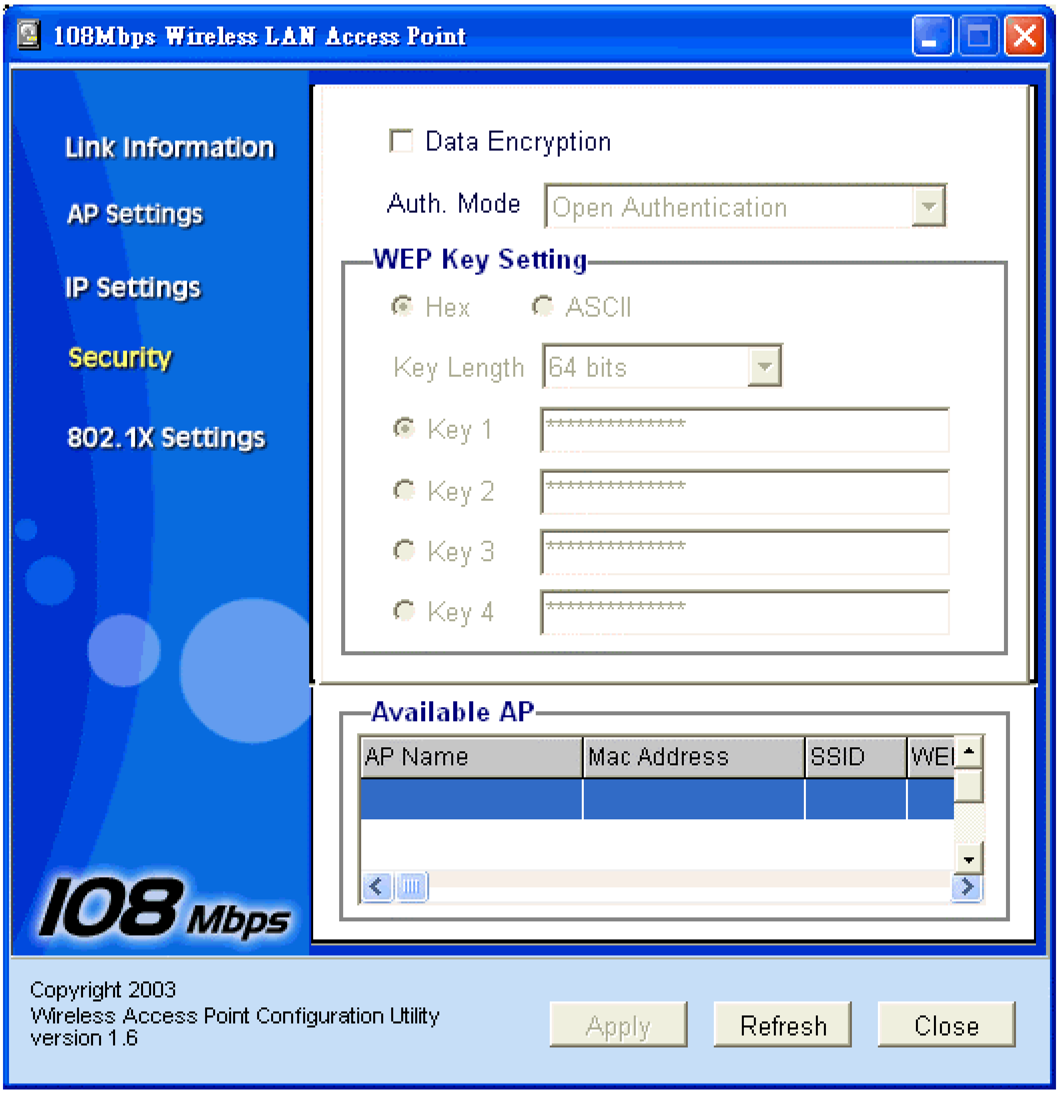
Authentication Type: There are four options: Open System; Shared Key; WPA; WPA-PKS. You may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: This will be enabled only while data encryption is selected.
The key value must be entered in ASCII or HEX format by clicking the radio button. Besides, there are two options for the key length: 64bits or 128bits.
There are four key sets are available to assign.
If the authentication type is WPA-PSK, users should input the key in the

passphrase as the below screen.

If the authentication type is WPA, users need to set the 802.1X in the following setting.

4.5 802.1X Settings



108Mbps Wireless LAN Access Point

□ Data Encryption

Auth. Mode: Open Authentication

WEP Key Setting

● Hex ○ ASCII

Key Length: 64 bits

● Key 1 **************

○ Key 2 **************

○ Key 3 **************

○ Key 4 **************

Available AP

AP Name	Mac Address	SSID	WE

Copyright 2003
Wireless Access Point Configuration Utility
version 1.6

If users like to set 802.1X or the authentication type is set to WPA, please enable 802.1X function by ticking it.

Encryption Key: Select the Encryption Key Length Size ranging from 64 to 128 Bits that you would like to use.

Lifetime: Select the Lifetime of the Encryption Key from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.

RADIUS Server1: Enter the **IP address** of and the **Port** used by the **Primary** Radius Server Enter the **Shared Secret**, which is used by the Radius Server.

Note: As soon as 802.1X security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

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.

AP Client: One of the additional AP operating modes offered by 54Mbps Access Point, which allows the Access Point to act as an Ethernet-to-Wireless Bridge, thus a LAN or a single computer station can join a wireless ESS network through it.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that you 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 **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers, 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.

Multiple Bridge – One of the additional AP operating modes offered by 54Mbps Access Point, which allows a group of APs that consists of two or more APs to connect two or more Ethernet networks or Ethernet enabled clients together. The way that multiple bridge setups is based on the topology of Ad-Hoc mode.

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 **T**o **S**end. 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 you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you 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.

Wireless Bridge – One of the additional AP operating modes offered by 54mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.