

802.11g Wireless LAN

Access Point

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

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.

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.

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.

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 availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 60 950-1: 2001 +A11: 2004

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.6.1 (2004-11)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.6.1: (2005-09)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.2.1 (2002-08)


Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE05600!

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erklärt <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoją, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

[sl] Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
[fi] Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

TABLE OF CONTENT

About This Guide.....	1
Purpose.....	1
Overview of this User's Guide.....	1
Unpacking and Setup	2
Unpacking.....	2
Setup	2
Hardware Instalation.....	3
Front panel	3
Rear Panel	3
Hardware connections.....	4
Connect to the Switch/Hub	4
Check the installation.....	4
Configuring the Wireless LAN Access Point	5
Login to the Wireless AP through WLAN.....	5
Login.....	5
Main Screen of the Access Point	6
Wizard.....	7
Status.....	9
Basic Setting	11
Access Point Mode	11
AP Client mode.....	14
WDS mode.....	17
AP+WDS mode	20
Repeater mode	21
IP Setting.....	24
Advanced Setting.....	25
Security	26
Tools	27
Technical Specifications	28

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless LAN Access Point. This manual helps to features the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11g) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to Fifty-four megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User's Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- ◆ One Wireless Access Point
- ◆ One external power adapter
- ◆ One CD-Rom (User's guide)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

- ◆ Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
- ◆ Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's Ethernet switch/hub port.
- ◆ Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
- ◆ Visually inspect if the Power Adapter was fully plugged to the device power jack.

HARDWARE INSTALATION

Front panel

The figure below shows the LED Indicator of the Wireless LAN Access Point.



Power:

This indicator lights green when the Access Point receives power. Otherwise, it turns off.

WLAN:

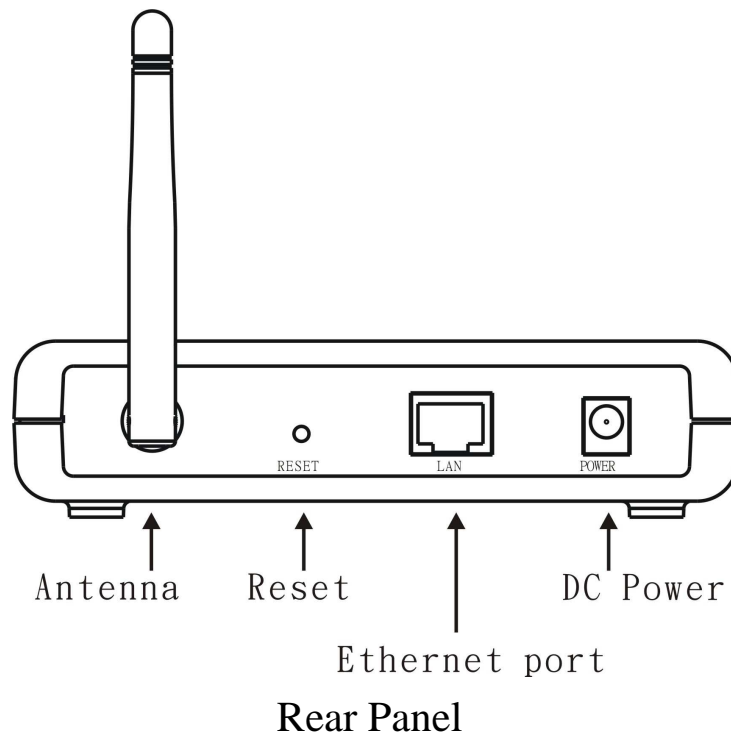
The indicator blinking green whiles the wireless LAN activity.

LAN (Link/ACT):

The indicator lights green when the LAN port is connected to a Ethernet network successful. Otherwise, the indicator blinking green while transmitting or receiving data on the Ethernet network.

Rear Panel

The figure below shows the rear panel of the Access Point



LAN

Ethernet port with 10/100Mbps Fast Ethernet connections, connect this port to switch/hub.

RESET

The Reset function is to reset the setting back to factory default setting, once you press the “RESET” button more than 5 seconds.

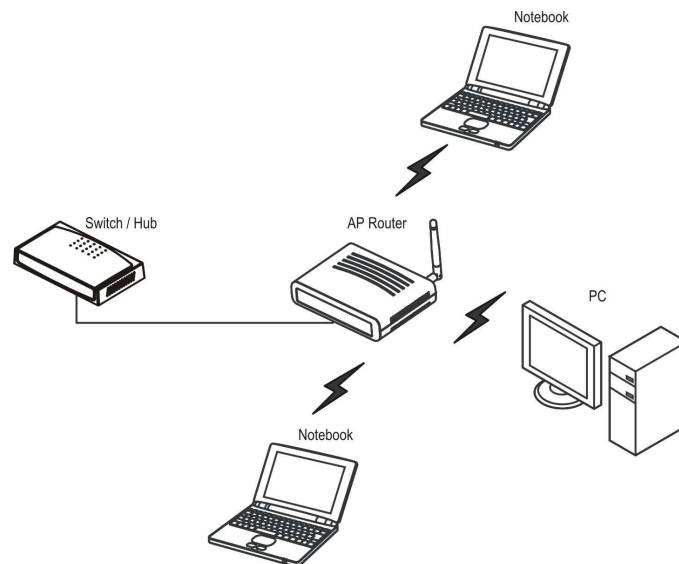
Power

Connect the Power Adapter DC plug to the AP’s power jack.

Antenna

One external dipole antenna.

Hardware connections



Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port LEDs will light up indicating a normal status.
2. If the LAN Port’s Link indicator does not light up then check the RJ-45 cable if it is firmly feed to the RJ45 port, while the LAN is link up to the Switch/Hub, the LAN port’s LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has a Web GUI interface for the configuration. The AP can be configured through the Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP to enable its functions.

Login to the Wireless AP through WLAN

Before configuring the Wireless AP through WLAN, make sure that the SSID, Channel and the WEP was set properly.

The default setting of the Wireless AP that you will use:

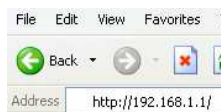
- ◆ SSID: default
 - ◆ Channel: 6
 - ◆ WEP Encryption: disable
 - ◆ IP address: 192.168.1.1
-

Login

Before you configure this device, note that when the AP is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP network**. For example, when the default network address of the default IP address of the AP is **192.168.1.1**, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

Enter IP address **http://192.168.1.1** (the factory-default IP address setting) to the address location.



When there is a screen needs to enter the User name and Password, both of the default Username and Password is “admin”



Main Screen of the Access Point

The screen will show the status of the AP when you login to the AP.

There are seven main functions included in the top side of the main screen: Wizard, Status, Basic Setting, IP Setting, Advanced Setting, Security and Tools. Point the selections in the top side of the menu screen.



The screenshot displays the main interface of an 802.11g Wireless LAN Access Point. At the top, there is a green header with the text "802.11g Wireless LAN Access Point" and a navigation menu with options: Wizard, Status (highlighted), Basic Setting, IP Setting, Advanced Setting, Security, and Tools. Below the header, a green sidebar on the left contains the word "Status" in yellow. The main content area shows the following information:

- Firmware Version: 1.02
- LAN**
 - MAC: 00-03-2F-24-F7-C2
 - IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
 - Gateway: 0.0.0.0
 - Send: 97
 - Receive: 343
- Wireless**
 - SSID: default
 - Encryption Function : Disabled
 - Channel: 6
 - Send: 1
 - Receive: 19

At the bottom of the Wireless section, there is a "View Log" button.

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.



Step 1: Set Password

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



Step2: Set WLAN Connection

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



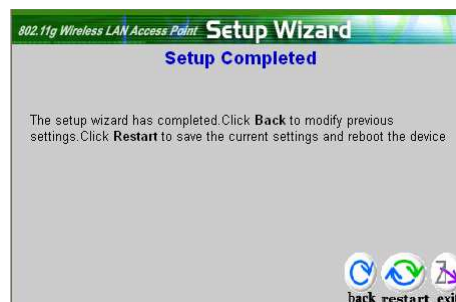
Step 3: Set WEP Encryption

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.



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 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”**.



Status

This page as below shows the following information.

802.11g Wireless LAN Access Point

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

Status

Firmware Version 1.02

LAN MAC:00-03-2F-24-F7-C2

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Send: 97

Receive: 343

Wireless

SSID: default

Encryption Function : Disabled

Channel: 6

Send: 1

Receive: 19

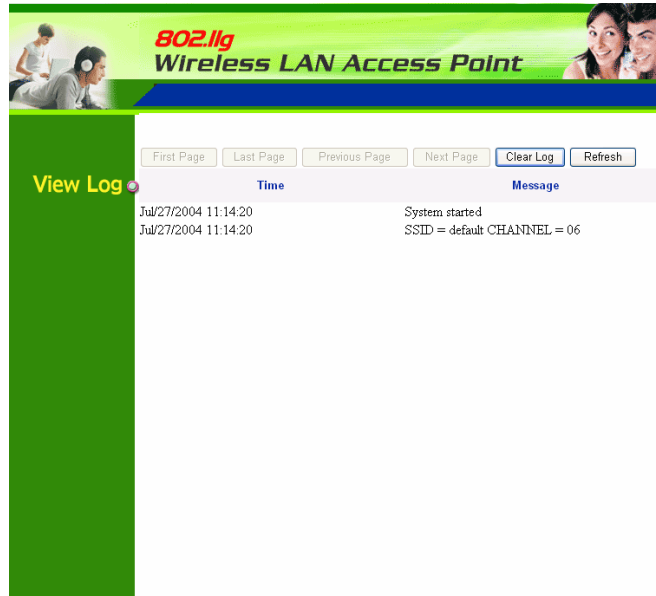
[View Log](#)

Firmware Version: Shows the current firmware version and released date code.

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 SSID, 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.



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.

Basic Setting

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

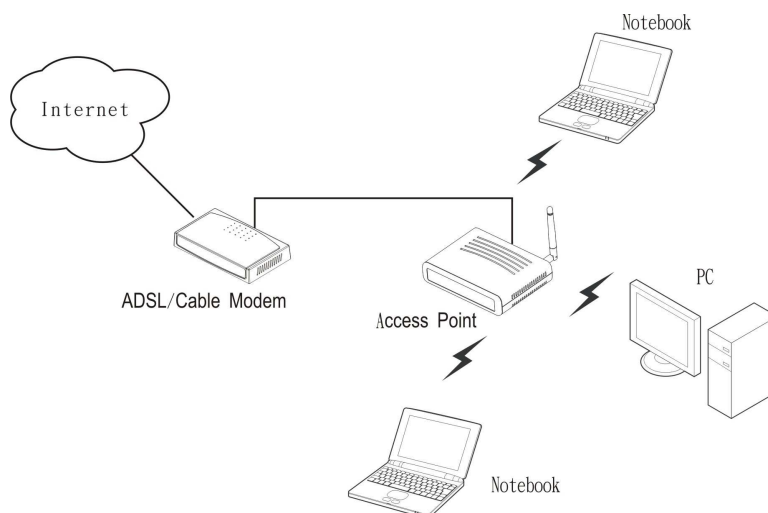


AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

Mode: The WLAN AP supports five operation mode for Access Point, AP Client, WDS (Wireless Distribution System), AP+WDS and Repeater mode.

Access Point Mode

Configure the AP to Access Point mode; with this mode, WLAN clients can access LAN or other WLAN clients through this AP.



AP mode application

The screenshot shows a configuration window for an Access Point (AP) in 'AP mode'. The 'AP Name' is '802.11g Wireless LAN'. The 'Mode' is set to 'Access Point'. The 'Channel' is set to '9'. The 'SSID' is 'OM-TEST'. Under 'Authentication', 'Open System' is selected. Under 'WEP Key', 'Disabled' is selected. Buttons for 'Apply', 'Cancel', and 'Help' are at the bottom.

AP mode configuration

Channel: The channel that AP will operate in. User can select the channel range from 1 to 11 when the domain of AP is North America (FCC).

And user can select the channel range from 1 to 13 when the domain of AP is European (ETSI).

User can select the channel range from 1 to 14 when the domain of AP is Japanese.

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.

Authentication Type: The authentication type default is set to Open system. There are six options: Open system; Shared Key; WPA-PSK, WPA2-PSK, WPA and WPA2. User may want to set to Shared Key when the clients and AP in the same wireless network enable the 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 the 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.



WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



WPA / WPA2:

If WPA or WPA2 is selected, the below screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.



RADIUS Server 1:

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.

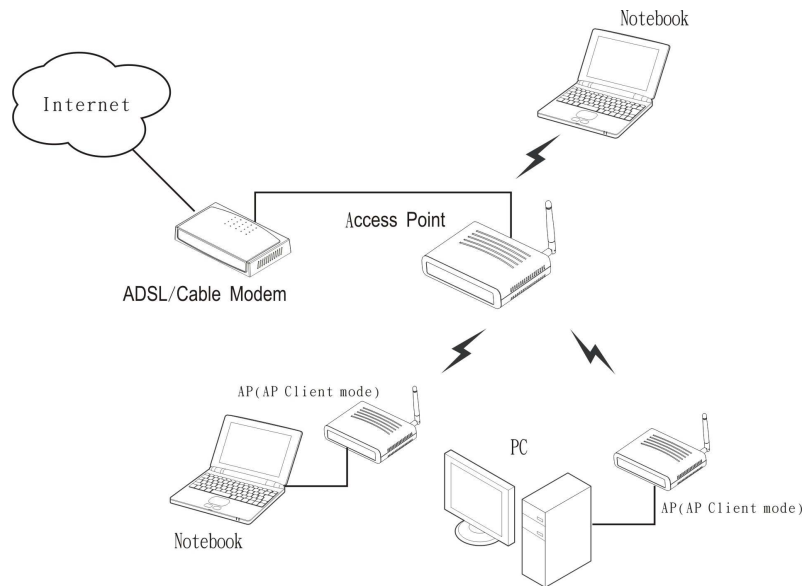
RADIUS Server 2: (optional)

Enter the IP address of and the Port used by the Secondary Radius Server, enter the Shared Secret, which is used by the Radius Server.

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.

AP Client mode

Configure the AP to AP Client mode; the AP will be a wireless Ethernet adapter transforms any Ethernet-enabled devices to have the wireless function.



AP Client mode application

The screenshot shows the configuration interface for an AP in client mode. The 'AP Name' is '802.11g Wireless LAN'. The 'Mode' is set to 'AP Client'. The 'Channel' is '9'. The 'SSID' is 'OM-TEST'. The 'Authentication' is set to 'Open System'. The 'WEP Key' is 'Disabled'. There are buttons for 'Apply', 'Cancel', and 'Help'.

AP Client mode configuration

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.

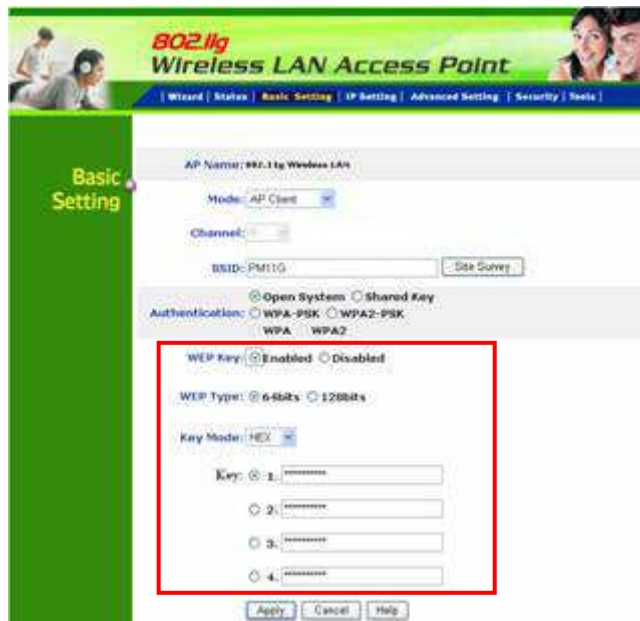
Site Survey: This button allows user to enable the Site Survey function to scan for the available wireless network (wireless clients and Access Points) and establish wireless communications with one. Selected one of them in list to establish communications and click “Connect” button.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
PM11G	00:03:2f2d:9a:9b	9 (B+G)	AP	yes	76	<input type="radio"/>
WBR2310	00:13:46:aa:ae:40	6 (B+G)	AP	yes	60	<input type="radio"/>
Weiwei	00:0d:0b:ae:09:35	2 (B+G)	AP	yes	56	<input type="radio"/>
Ethan_524	00:04:88:eb:99:5c	9 (B+G)	AP	yes	55	<input type="radio"/>
aa111111111000000000011111111111	00:13:46:a2:54:18	5 (B+G)	AP	yes	46	<input type="radio"/>
God bless you	00:03:2f1f32:29	6 (B+G)	AP	yes	35	<input type="radio"/>
IntelAP	00:02:b3:92:67:bc	3 (B)	AP	no	27	<input type="radio"/>
DL-624-TEST	00:10:ab:cd:cc:03	6 (B+G)	AP	yes	18	<input type="radio"/>
IBM	02:20:e1:2a:4c:7c	11 (B)	Ad hoc	no	18	<input type="radio"/>

Authentication Type: The authentication type default is set to Open system. There are four options: Open system; Shared Key; WPA-PSK and WPA2-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.

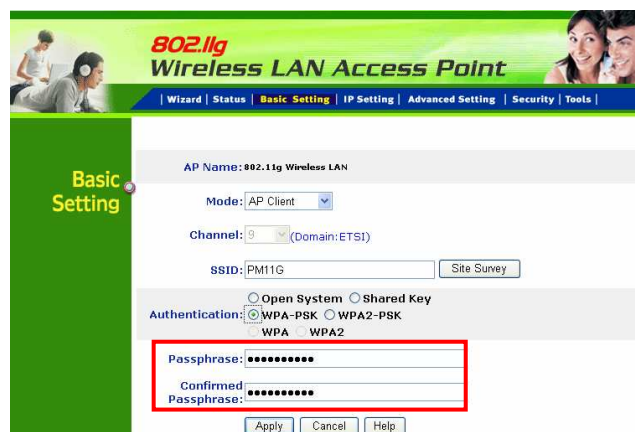
WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

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.



WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



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.

Note: For entering to the Web Setting page after changing to AP Client mode, change your PC/Notebook IP address to 192.168.1.x. After changing your IP address, type 192.168.1.1 on the Web browser to enter the setting of this Wireless AP.

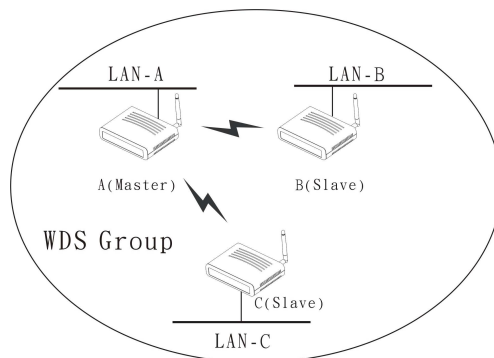
WDS mode

With WDS (Wireless Distribution System) mode, user can use wireless media to communicate two or more LANs through the AP with WDS mode, all of the LAN will be combined in the WDS group, for example:

Single WDS group application:

When there are three APs joined to the WDS group, one of the AP in WDS mode will be the Master, the other two APs will be the Slave, all of the APs in the WDS group must use the same wireless channel and the same security setting, the Master need to fill all the Slave's MAC address in the "Remote AP Mac" list, and the Slave need to fill the Master's MAC address in the "Remote AP Mac" list, the maximum of one Master can join eight Slave to be one WDS group.

In this example, LAN-A can communicate with LAN-B and LAN-C, and LAN-B can communicate with LAN-C through the AP-A. All of LANs will be at the same LAN environment coming through LAN-A.



WDS mode application (Single WDS group)

<p>AP Name: 802.11g Wireless LAN</p> <p>Mode: WDS</p> <p>Channel: 9</p> <p>Remote AP Mac: 1. The MAC address of AP-B 2. The MAC address of AP-C</p> <p>3. 4.</p> <p>5. 6.</p> <p>7. 8.</p> <p>WDS Security: WEP 64bits</p> <p>WEP Key: ASCII</p> <p>Passphrase: (8~63 char.)</p> <p>Apply Cancel Help</p>	<p>AP Name: 802.11g Wireless LAN</p> <p>Mode: WDS</p> <p>Channel: 9</p> <p>Remote AP Mac: 1. The MAC address of AP-A 2.</p> <p>3. 4.</p> <p>5. 6.</p> <p>7. 8.</p> <p>WDS Security: WEP 64bits</p> <p>WEP Key: ASCII</p> <p>Passphrase: (8~63 char.)</p> <p>Apply Cancel Help</p>
---	---

Master setting (AP-A)

Slave setting (AP-B and AP-C)

WDS mode configuration for Example-1

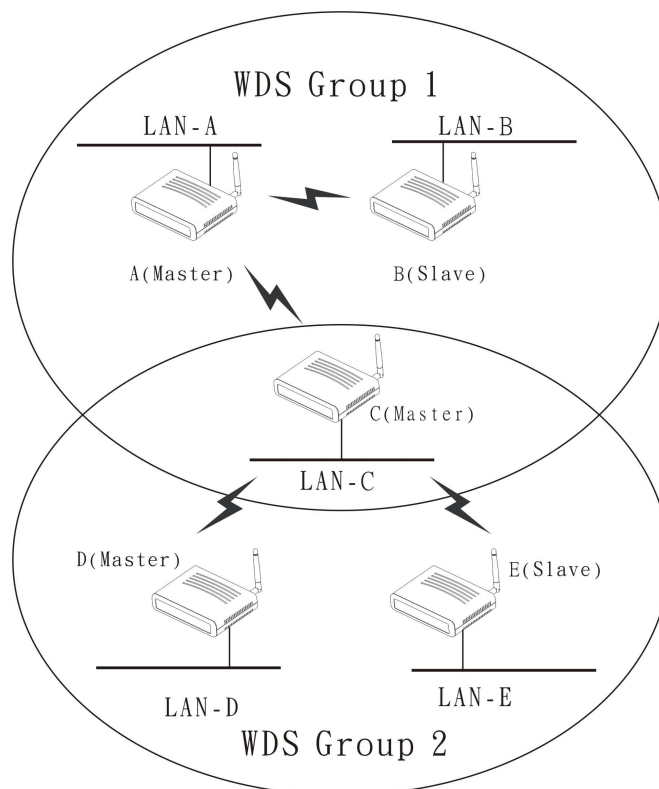
Multiple WDS group application:

When there are five APs to be join into two separated WDS group, the member of WDS group 1 is AP-A, AP-B and AP-C, and member of the WDS group 2 is AP-C, AP-D and AP-E, the AP-C will join both of WDS group 1 and WDS group 2, each WDS Group 1 will be one master and the other will be slave.

The AP-A and AP-C will be both as a Master AP for both WDS Groups, the AP-A represent for the master of WDS Group 1, the AP-C represent for the master of the WDS Group 2 and at the same time AP-C will be the slave of WDS Group 1, so all of the APs in the two WDS groups must use the same wireless channel and same security, the Master need to fill all of Slave's MAC address in the "Remote AP Mac" list, and the Slave need to fill the Master's MAC address in the "Remote AP Mac" list, maximum allow one Master can be join eight Slaves to be one WDS group.

In this example, LAN-A can communicate with LAN-B and LAN-C, and LAN-B can communicate with LAN-C through the AP-A. LAN-B will have the same LAN environment coming through LAN-A.

LAN-E can communicate with LAN-B and LAN-D, LAN-E can communicate with LAN-D through AP-C, LAN-E can communicate with LAN-B through AP-C and AP-A, LAN-E will have the same LAN environment coming through LAN-A.



WDS mode application (Multiple WDS group)

AP Name: 802.11g Wireless LAN

Mode: WDS

Channel: 9

Remote AP Mac: 1. The MAC address of AP-B 2. The MAC address of AP-C

3. 4.

5. 6.

7. 8.

WDS Security: WEP 64bits

WEP Key: ASCII

Passphrase: (8~63 char.)

Apply Cancel Help

Master setting (AP-A, WDS Group 1)

AP Name: 802.11g Wireless LAN

Mode: WDS

Channel: 9

Remote AP Mac: 1. The MAC address of AP-A 2.

3. 4.

5. 6.

7. 8.

WDS Security: WEP 64bits

WEP Key: ASCII

Passphrase: (8~63 char.)

Apply Cancel Help

Slave setting (AP-B, WDS Group 1)

AP Name: 802.11g Wireless LAN

Mode: WDS

Channel: 9

Remote AP Mac: 1. The MAC address of AP-A 2. The MAC address of AP-D

3. The MAC address of AP-E 4.

5. 6.

7. 8.

WDS Security: WEP 64bits

WEP Key: ASCII

Passphrase: (8~63 char.)

Apply Cancel Help

Master setting (AP-C, WDS Group 2)

AP Name: 802.11g Wireless LAN

Mode: WDS

Channel: 9

Remote AP Mac: 1. The MAC address of AP-C 2.

3. 4.

5. 6.

7. 8.

WDS Security: WEP 64bits

WEP Key: ASCII

Passphrase: (8~63 char.)

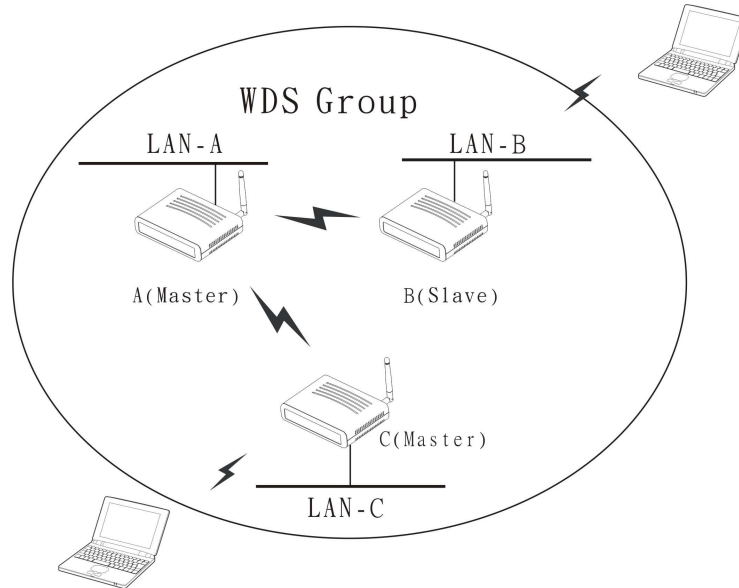
Apply Cancel Help

Slave setting (AP-D and AP-E, WDS Group 2)

WDS mode configuration for Example-2

AP+WDS mode

With WDS+AP mode, user can use wireless media to communicate two or more LANs through the AP with WDS+AP mode, all of LAN will be combined in the WDS group and WLAN client can access to the AP with AP+WDS mode.



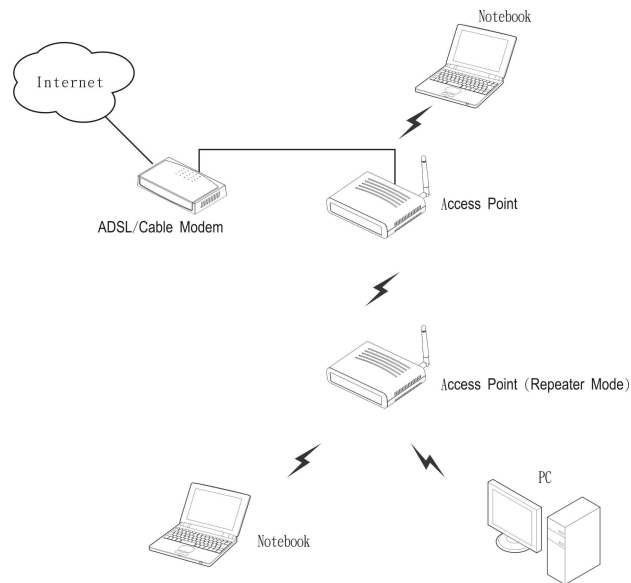
WDS+AP mode application

The screenshot shows the configuration interface for an AP. The top section, highlighted in red, is labeled "AP configuration" and includes the following settings:
- AP Name: 802.11g Wireless LAN
- Mode: AP+WDS
- Channel: 9
- SSID: DM-TEST
- Authentication: WPA2-PSK (selected)
- Passphrase and Confirmed Passphrase fields.
The bottom section, highlighted in blue, is labeled "WDS configuration" and includes:
- Remote AP Mac: 1. 00d88bet995c, 2. [empty], 3. [empty], 4. [empty], 5. [empty], 6. [empty], 7. [empty], 8. [empty].
- WDS Security: WEP 64bits
- WEP Key: ASCII, [empty]
- Passphrase: (8~63 char.) [empty]
- Buttons: Apply, Cancel, Help

Please refer the AP mode and WDS mode for detail configuration.

Repeater mode

Configure the AP to Repeater mode; the AP will be a wireless LAN repeater that will be extended the WLAN coverage range.



Repeater mode application

AP Name: 802.11g Wireless LAN

Mode: Repeater

Channel: 9

SSID: Site Survey

Open System Shared Key

Authentication: WPA-PSK WPA2-PSK
 WPA WPA2

WEP Key: Enabled Disabled

Apply Cancel Help

Repeater mode configuration

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.

Site Survey: This button allows user to enable the Site Survey function to scan for the available wireless network (wireless clients and Access Points) and establish wireless communications with one. Selected one of them in list to establish communications and click “Connect” button.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
PM11G	00:03:2f:2d:9a:9b	9 (B+G)	AP	yes	70	<input type="radio"/>
Weirwei	00:0d:0b:ae:09:35	1 (B+G)	AP	yes	56	<input type="radio"/>
Weirwei	00:0d:0b:ae:09:35	2 (B+G)	AP	yes	56	<input type="radio"/>
Ethan_524	00:0d:88:eb:99:5c	9 (B+G)	AP	yes	55	<input type="radio"/>
WBR2310	00:13:46:aa:ae:40	6 (B+G)	AP	yes	49	<input type="radio"/>
God bless you	00:03:2f:1f:32:29	6 (B+G)	AP	yes	36	<input type="radio"/>
aa11111111110000000000111111111111	00:13:46:a2:54:18	5 (B+G)	AP	yes	36	<input type="radio"/>
IntelAP	00:02:b3:92:67:bc	3 (B)	AP	no	21	<input type="radio"/>
allen	00:03:2d:12:34:59	6 (B+G)	AP	no	18	<input type="radio"/>
802.11g-SSID	00:03:2f:10:32:93	11 (B+G)	AP	no	10	<input type="radio"/>

Authentication Type: The authentication type default is set to Open system. There are four options: Open system; Shared Key; WPA-PSK and WPA2-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.

AP Name: 802.11g Wireless LAN

Mode: Repeater

Channel: []

SSID: [] Site Survey

Open System Shared Key

Authentication: WPA-PSK WPA2-PSK

WPA WPA2

WEP Key: Enabled Disabled

WEP Type: 64bits 128bits

Key Mode: HEX

Key: 1: []

2: []

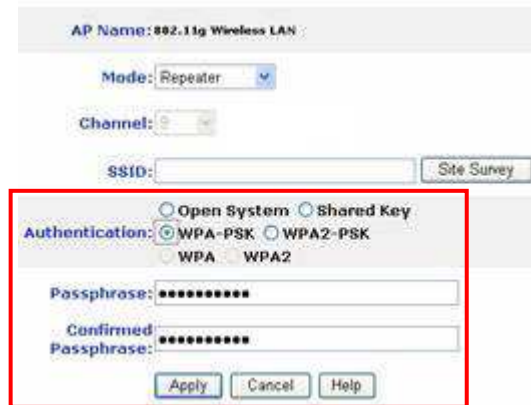
3: []

4: []

Apply Cancel Help

WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, 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 displays a configuration window for an Access Point (AP) named "802.11g Wireless LAN". The "Mode" is set to "Repeater". The "Channel" is set to "0". The "SSID" field is empty, and there is a "Site Survey" button next to it. The "Authentication" section is highlighted with a red box and contains the following options: "Open System" (unselected), "Shared Key" (unselected), "WPA-PSK" (selected), and "WPA2-PSK" (unselected). Below these options, there are two fields for "Passphrase": "Passphrase:" and "Confirmed Passphrase:", both containing eight asterisks. At the bottom of the highlighted area are three buttons: "Apply", "Cancel", and "Help".

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.

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 page title is "802.11g Wireless LAN Access Point". The navigation menu includes "Wizard", "Status", "Basic Setting", "IP Setting" (which is highlighted), "Advanced Setting", "Security", and "Tools". The "IP Setting" section is active, showing the following options and fields:

- LAN IP:** Obtain IP Automatically, Fixed IP
- Address:**
- Subnet Mask:**
- Gateway:**
- DHCP Server:** On, Off
- IP Range:** From to
- DNS Server:**

At the bottom of the form are three buttons: "Apply", "Cancel", and "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.

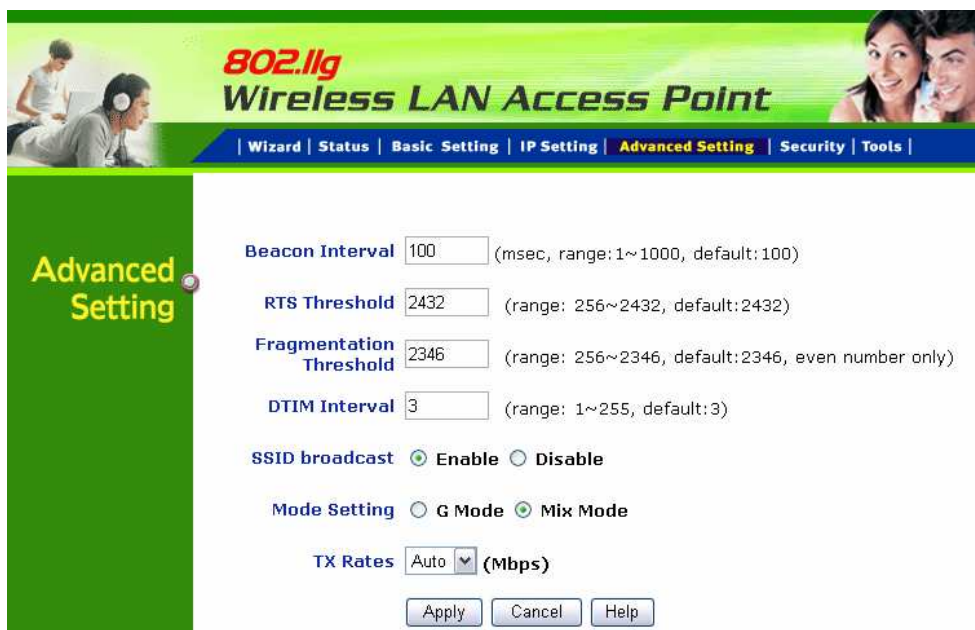
DHCP Server: It is not recommended to enable the DHCP Server if user has a DHCP server running in LAN network because it probably will cause possible the conflict of IP assignment. Enable the DHCP server function by selecting the option “**On**”, and enter the IP range.

DNS Server: Type up to DNS IP address in the text boxes. Your ISP will provide you with this information.

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

Advanced Setting

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



The screenshot shows the configuration interface for an 802.11g Wireless LAN Access Point. The page title is "802.11g Wireless LAN Access Point". The navigation menu includes: Wizard | Status | Basic Setting | IP Setting | **Advanced Setting** | Security | Tools. The "Advanced Setting" section is highlighted in green. The configuration options are:

- Beacon Interval:** 100 (msec, range: 1~1000, default: 100)
- RTS Threshold:** 2432 (range: 256~2432, default: 2432)
- Fragmentation Threshold:** 2346 (range: 256~2346, default: 2346, even number only)
- DTIM Interval:** 3 (range: 1~255, default: 3)
- SSID broadcast:** Enable Disable
- Mode Setting:** G Mode Mix Mode
- TX Rates:** Auto (Mbps)

Buttons: 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.

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: To setting the AP operation mode for 802.11g only or 802.11b/802.11g mix mode

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

Security

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

802.11g Wireless LAN Access Point

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

Security

Password

AP Password New: [masked]

Confirm: [masked]

Apply Cancel Help

MAC Filter

Disabled MAC Filters

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

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

MAC address [] - [] - [] - [] - [] - [] Clear

Connected PCs 00-04-23-4f-30-c6 Clone

Apply Cancel Help

MAC Filter List

MAC Address

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. There have three choices:

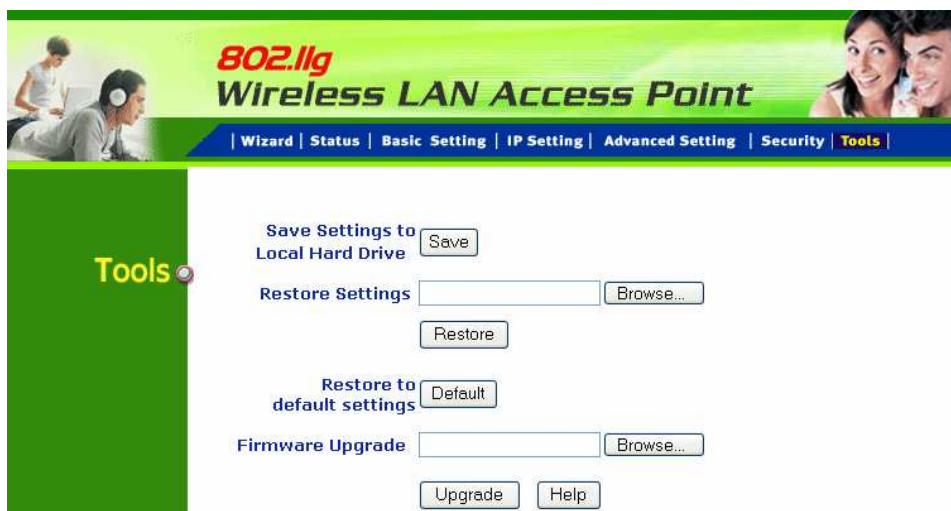
- ◆ Disable MAC Filters
- ◆ Only **allow** PCs with MAC listed below to access device
- ◆ Only **deny** PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. User can browse through the MAC address saved by selecting the MAC Filter List.

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

Tools

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



Save Settings to Local Hard Drive: Click on “Save Settings to Local Hard Drive” 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.

TECHNICAL SPECIFICATIONS

General	
Standards	IEEE 802.11b/g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	DSSS (802.11b) OFDM (802.11g)
Modulation:	QPSK / BPSK / CCK / OFDM
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency	2412 MHz ~ 2462 MHz (FCC) 2412 MHz ~ 2472 MHz (ETSI) 2400 MHz ~ 2484 MHz (Japan)
Channel	1 ~ 11 Channels (FCC) 1 ~ 13 Channels (ETSI) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption, WPA, WPA2, WPA-PSK, WPA2-PSK
Data Transfer Rate	Fast Ethernet: 10/100Mbps Wireless: Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps: Typical -68 dBm @10% PER 11Mbps: Typical -81 dBm @8% PER
Transmit Power	802.11g: Minimum 17dBm typically 802.11b: Minimum 18dBm typically
Transmission Range:	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	2-pair UTP/STP Cat. 3,4,5 (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna:	1 x 2 dBi Dipole Antenna

Physical and Environmental

DC inputs	DC 7.5V /1A
Power Consumption	4.2W (Max)
Temperature	Operating: 0 ~ 40 °C, Storage: -10 ~ 70 °C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B,