LINKSYS®

A Division of Cisco Systems, Inc.

USER GUIDE

BUSINESS SERIES

Wireless-G Exterior Access Point with Power Over Ethernet

Model: WAP200E

CISCO™

About This Guide

Icon Descriptions

While reading through the User Guide you may encounter various icons designed to call attention to a specific item. Below is a description of these icons:

NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.

WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.

WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Most web browsers allow you to enter the web address without adding the http:// in front of the address. This User Guide will refer to websites without including http:// in front of the address. Some older web browsers may require you to add it.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Chapter 1: Introduction

Thank you for choosing the Wireless-G Exterior Access Point with Power Over Ethernet.

The Linksys Wireless-G Exterior Access Point with Power Over Ethernet lets you connect Wireless-G (802.11g) or Wireless-B (802.11b) devices to your wired network so you can add PCs to the network with no cabling hassle. This weather-proof Access Point creates a "wireless bubble" in exterior spaces, like patios, pool areas, and outdoor cafés. Power over Ethernet support makes it easy to install, and you can create multiple SSIDs that connect to individual VLANs to keep your traffic separated.

It's also perfect for use as a bridge, a kind of "cable-less cable" to connect remote areas together. Maybe your warehouse is in a separate building from your offices. Or maybe you need to connect the separate buildings of a college campus. With one Wireless-G Exterior Access Point on each building, you're connected with no cable to run. The exterior-rated case protects the access point, and contains an internal antenna.

To protect your data and privacy, the Wireless-G Exterior Access Point with Power Over Ethernet supports both Wired Equivalent Privacy (WEP) and the industrial-strength wireless security of Wi-Fi Protected Access™ (WPA), encoding all your wireless transmissions with powerful encryption. The MAC Address filter lets you decide exactly who has access to your wireless network, and advanced logging keeps you appraised. Configuration is a snap with the web browser-based configuration utility.

The Linksys Wireless-G Exterior Access Point with Power Over Ethernet is the best way to add wireless access to the outdoor areas of your home or business.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one or more wireless adapters. Computers in a wireless network must be configured to share the same radio channel to talk to each other. Several PCs equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point.

Linksys wireless adapters also provide access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired or wireless network via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled (depending on antenna characteristics).

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same wireless channel, SSID, and wireless security settings.

Before you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

✓ **NOTE:** Spanning Tree Protocol should be disabled on the switches connecting to the APs to allow roaming to work without disruption.

Network Layout

The Access Point has been designed for use with 802.11g and 802.11b products, such as the Notebook Adapters for your laptop computers, PCI Adapters for your desktop PCs, and USB Adapters.

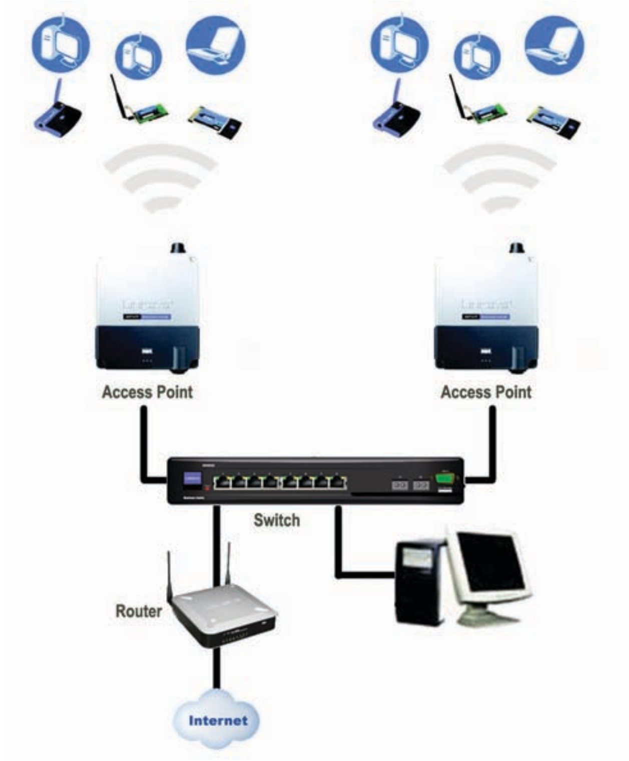
These wireless products can also communicate with a 802.11g or 802.11b Wireless PrintServer.

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router with Power over Ethernet (PoE)—or a PoE injector, such as the Linksys WAPPOE or WAPPOE12.

✓ **NOTE:** 12 VDC on WAPPOE12 is for the splitter output. Both PoE Injectors provide 48 VDC power output.

Go to the Linksys website at **www.linksys.com** for more information about wireless products.

Example of a Simple Wireless Network



Example of Simple Wireless Network

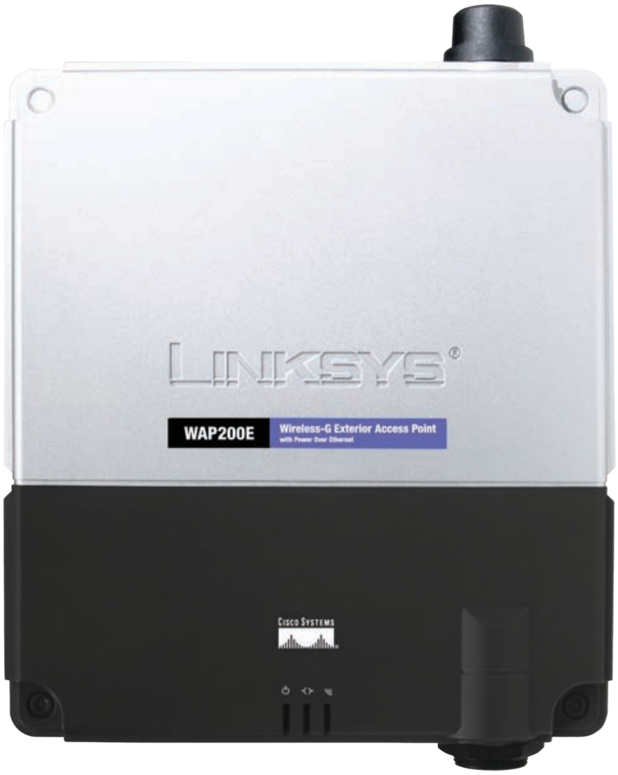
The above diagram shows a typical infrastructure wireless network setup. The Wireless Access Points are connecting to a Linksys switch that provides power to the Access Points. Each Access Point can connect multiple wireless devices to the network. This network will provide connectivity among wireless network devices and PCs that have a wired connection to the switch.

The switch then can connect to a router that can connect to an ISP for Internet access.

Chapter 3: Product Overview

Front Panel

The Access Point's LEDs, where information about network activity is displayed, are located on the front panel.



Front Panel

Power (Green) The Power LED lights up when the Access Point is powered on.

Wired (Green) The Wired LED lights up when the Access Point is successfully connected to a device through the Ethernet network port. If the Wired LED is flashing, the Access Point is actively sending to or receiving data from one of the devices over the Ethernet network port.

Wireless (Green) The Wireless LED lights up when the wireless module is active on the Access Point. If the Wireless LED is flashing, the Access Point is actively sending to or receiving data from a wireless device.

Bottom Panel

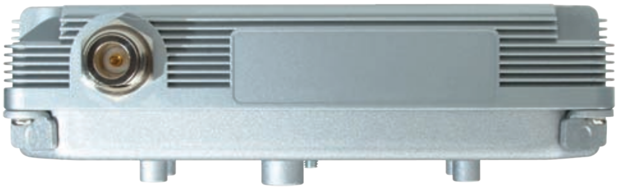
The Ethernet network port is located on the bottom panel of the Access Point.

Bottom Panel

Ethernet network port The Ethernet network port connects to Ethernet network devices, such as a switch or router. The Access Point is powered using Power Over Ethernet. If the switch or router doesn't support Power Over Ethernet, then a Power Over Ethernet Injector must be installed.

Top Panel

The antenna port is located on the top panel of the Access Point.

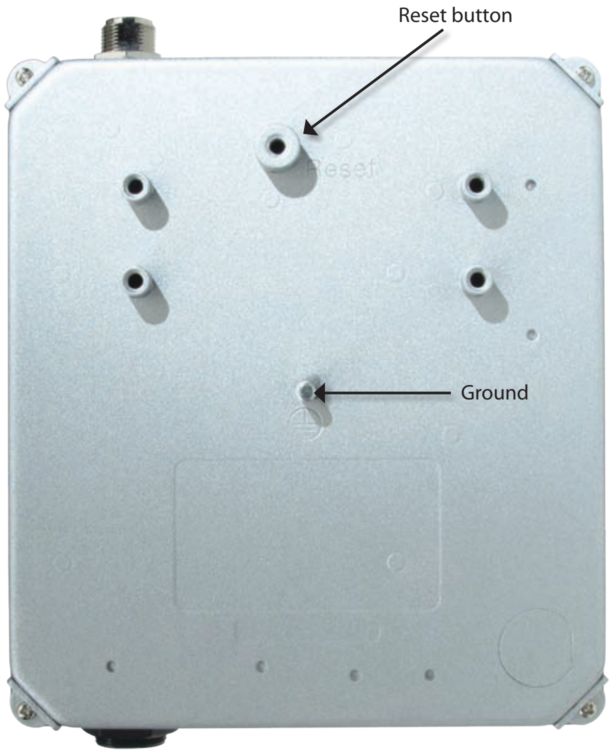


Top Panel

Antenna Port The Access Point has built-in, 1x2 MIMO 9dBi directional antennas. It also has a reverse polarity female N-type antenna port for an optional, high-gain external antenna such as the HGA9N. One of the two internal antennas will be disabled automatically when an external antenna is connected.

Back Panel

The Access Point's Reset button and ground are located on the back panel.



Back Panel

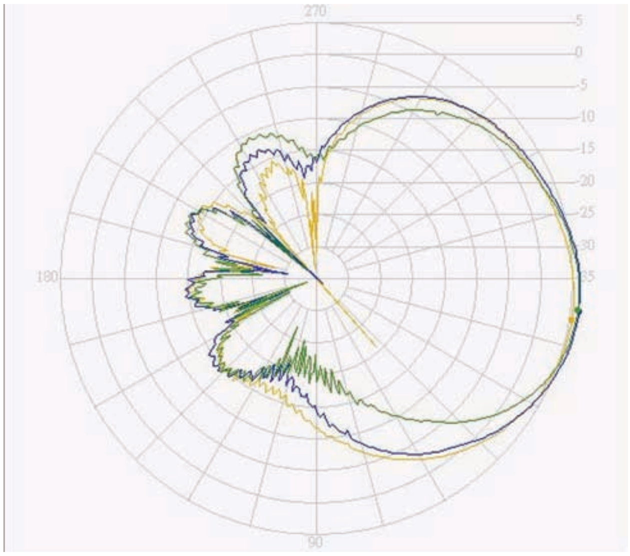
Reset Button There are two ways to Reset the Access Point's factory defaults. Either press the Reset button, for approximately ten seconds, or restore the defaults using the Access Point's web-based utility.

IMPORTANT: Resetting the Access Point will erase all of your settings (including wireless security, IP address, and power output) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Ground Before you mount the Access Point, you must ground the Access Point (to a large piece of metal) as a precaution against electric shock.

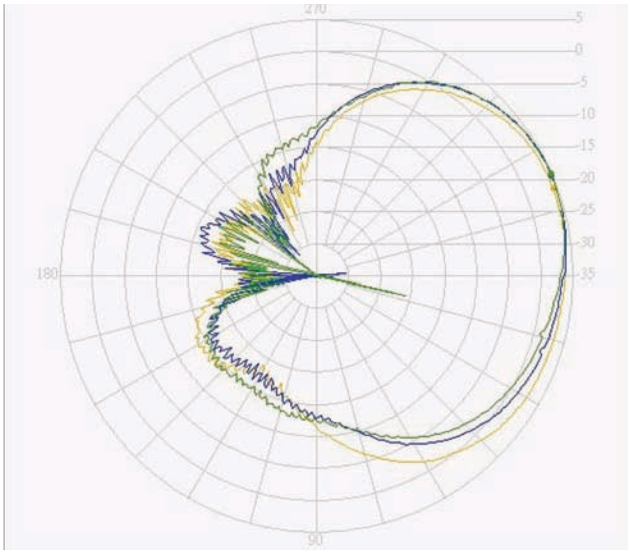
The Antenna Pattern

The Wireless-G Exterior Access Point uses 1X2 MIMO (1Tx, 2Rx) so it has two built-in antennas. The right antenna is the main antenna for Tx traffic. When an external antenna is attached, the right antenna is disabled and the external antenna is used for Tx traffic. Currently, only the HGA9N (9dBi omni-directional antenna) is compatible with the Wireless-G Exterior Access Point.



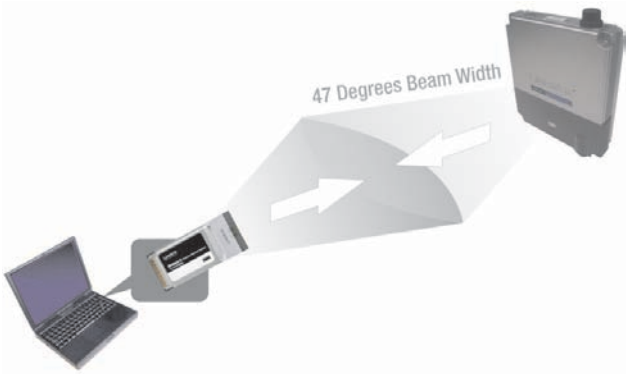
Right Antenna Pattern

3dB BW: 50 degree, peak gain: 6.3 dBi



Left Antenna Pattern

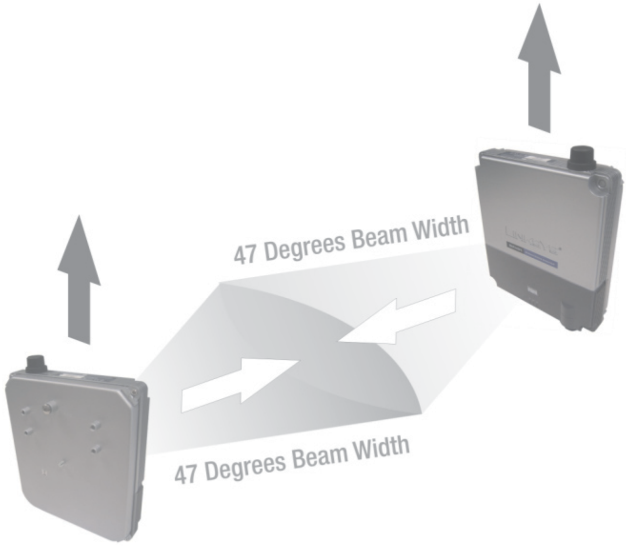
3dB BW: 63 degree, peak gain: 4.9 dBi



Radio Coverage of the Access Point to Client Devices

When using the Access Point to connect client devices, adjust it so the client devices are on the same horizontal plane as the Access Point and within a 3dB angle of 47 degrees. This will ensure the strongest signal and maximum reach.

If the Access Point is used inside a building, put it in a corner of the building for maximum coverage.



Access Point to Access Point (bridging) Radio Coverage

If the Access Point is used as a bridge or repeater, adjust the Access Points so they face each other, this will ensure the strongest signal and maximum reach.

Make sure that the orientation of the two Directional Antennas is the same. The radio wave is polarized so a 90 degree rotation will result in no received power.

Due to its directional characteristics, the internal antenna is ideal for point-to-point bridge mode or the spoke side of point-to-multipoint bridge mode. An external omni-directional antenna (e.g. HGA9N) is recommended for repeater mode applications.

Chapter 4: Installation

Overview

This chapter explains how to mount and connect the Access Point.

Depending on your application, you might want to set up the IP address of the device first before mounting the device. Refer to “Chapter 5: Quick Configuration Overview”.

Personal Installation

This product should be installed by a qualified installation professional with RF and related rule knowledge. General users should not attempt to install this product or modify the settings.

Installation Location

The product should be installed in a location where the radiating antenna is at least 20 cm from anyone under normal operating conditions. This is required to meet regulatory RF exposure requirements.

External Antenna

Use only antennas approved by Linksys. Antennas that have not been approved by Linksys may produce unwanted spurious or excessive RF transmitting power, this may lead to violation of FCC limitations and is prohibited.

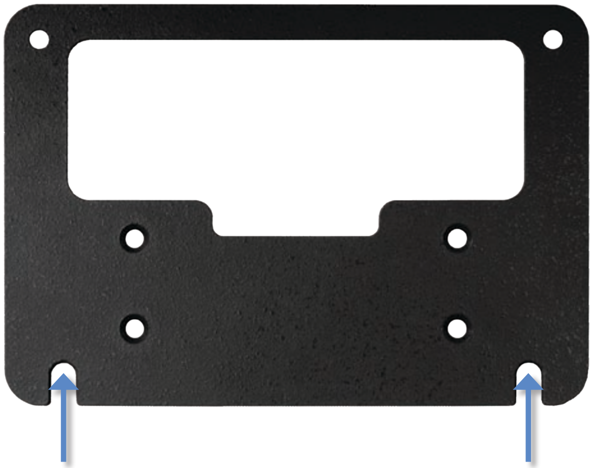
Installation Procedure

Follow the Hardware Installation instructions for details on installing this product.

WARNING: Please carefully select the installation position and make sure that the final output power does not exceed the limit defined in US Rule CFR 47 Part 15, section 15.247 and 15.407. Violation of the rule could lead to serious federal penalties.

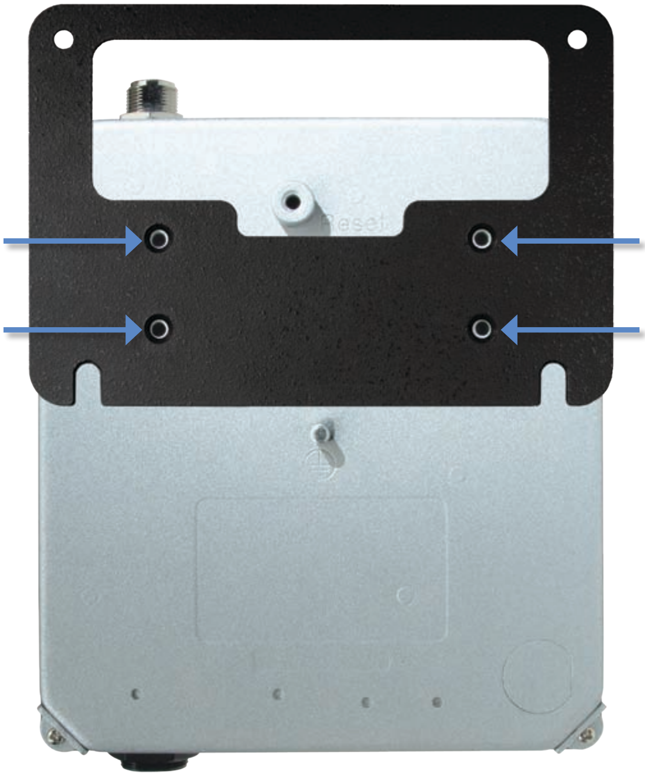
Hardware Installation

1. Locate an optimum location on a wall for the Access Point. Refer to the antenna pattern in “Chapter 3: Product Overview” to adjust the angle of the Access Point for your application.
2. Using the mounting plate as a template, mark the locations of the two wall-mount slots that are on the bottom of the mounting plate. Then, install a screw into each location.



Mark the Locations of the Two Wall-Mount Slots

3. Use four screws (included with the Access Point) to attach the mounting plate to the back panel of the Access Point.

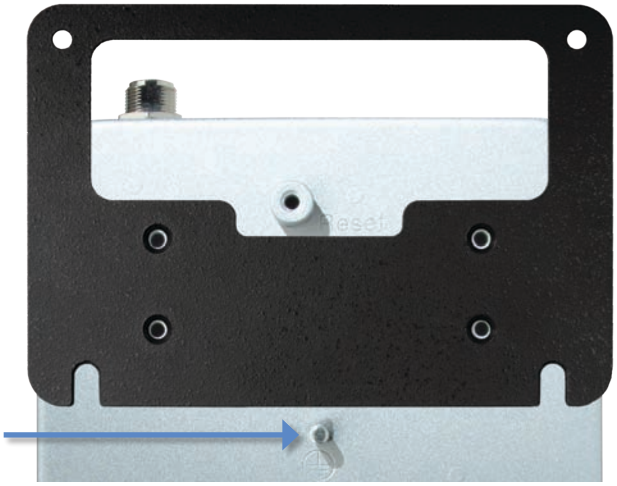


Attach the Mounting Plate

4. Connect the included Category 5e Ethernet network cable to the Ethernet network port of the Access Point.

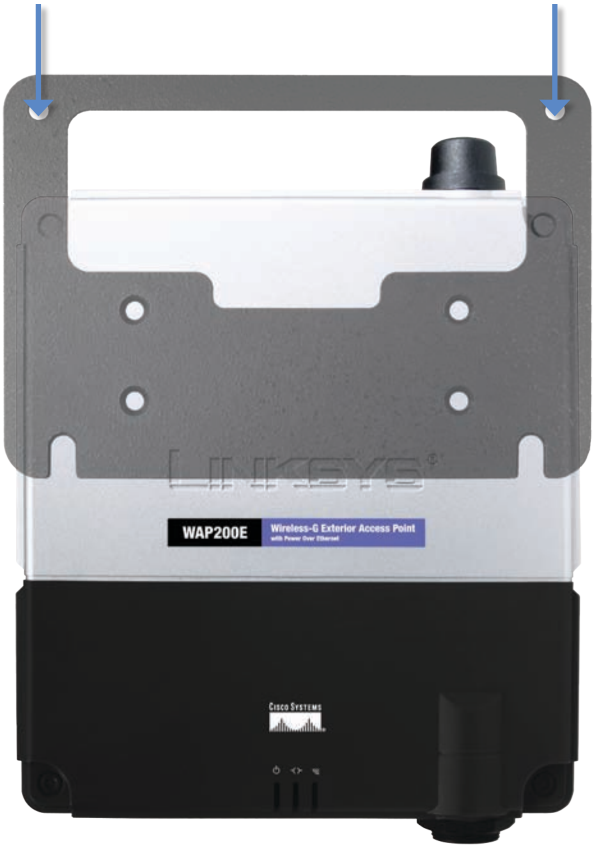
Then, screw the connector cap tightly onto the port, so the Access Point has a water-resistant seal.

5. If you want to connect an optional, high-gain external antenna, remove the cap that protects the antenna port, then, connect your antenna cable to this port.
6. Make sure that you properly ground the Access Point.



Ground the Access Point

7. Line up the Access Point's wall-mount slots with the two screws on the wall. Then, slide the Access Point down so that the screws fit snugly in the slots.
8. Attach a screw (not included) in each of the two holes on the top of the mounting plate so that the Access Point is securely mounted to the wall.



Attach the Access Point to the Wall

9. Connect the other end of the Ethernet network cable to a switch, router, or other device that supports Power over Ethernet. The Access Point will then be connected to your wired network.

Now that the hardware installation is complete, proceed to "Chapter 5: Quick Configuration Overview" for directions on how to configure the Access Point.

Chapter 5: Quick Configuration Overview

Overview

The Access Point has been designed to be functional right out of the box with the default settings. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the web-based utility. This chapter explains how to use the utility.

The utility can be accessed via web browsers, such as Microsoft Internet Explorer or Mozilla Firefox through the use of a computer that is networked with the Access Point.

For a basic network setup, most users only have to use the following screens of the Utility:

- **Setup** On the Setup screen, enter your basic network settings (IP address) here.
- **Management** Click the *Administration* tab and then select the *Management* screen. The Access Point's default password is **admin**. To secure the Access Point, change the AP Password from its default.

Most users will also customize their wireless settings:

- **Wireless** On the Wireless screen, change default SSID under the *Basic Wireless Settings* tab. Select the level of security under the *Wireless Security* tab.

Accessing the Web-Based Utility

There are two ways to power your Access Point.

- **48V Power Injector (e.g. Linksys WAPPOE)** Power up your Access Point first then connect the cable on your Injector to your PC.
- **PoE switch (e.g. Linksys SRW224P)** Connect your Access Point and your PC to the same LAN.

To access the web-based utility, perform the following steps:

1. Configure your PC with a static IP address in the same subnet as the Access Point's default IP address (192.168.1.245). If there is DHCP server connected to the switch, configure it to assign the IP address in 192.168.1.0/24 subnet. Your PC will get an IP address in the subnet through the DHCP.
2. Launch your web browser, such as Internet Explorer or Mozilla Firefox and enter the Access Point's default IP address, **192.168.1.245**, in the Address field. Press the Enter key.
3. Enter **admin** in the User Name field. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from *Administration* > *Management*) Then click the **OK** button.

After setting up the Access Point to use DHCP or manually configure a new IP address, move your Access Point to the desired network. You will have to use the new IP address the next time you access the Web-based Utility.

Navigating the Web-Based Utility

The web-based utility consists of the following five main tabs: **Setup**, **Wireless**, **AP Mode**, **Administration**, and **Status**. Additional screens (sub tabs) will be available from most of the main tabs.

The following briefly describes the main and sub tabs of the Utility.

Setup

Basic Setup Enter the Host Name and IP Address settings on this screen.

Time You can set the time either manually or automatically from a time server if the Access Point can access the public Internet.

Wireless

You will use the Wireless tabs to enter a variety of wireless settings for the Access Point.

Basic Wireless Settings Choose the wireless network mode (e.g. wireless-G), wireless channel, and SSID configuration on this screen.

Wireless Security Use this screen to configure the Access Point's security settings including access authentication, data encryption, and wireless isolation.

Wireless Connection Control Use this screen to populate your Access List to permit or block certain MAC address access to your wireless network.

Advanced Wireless Settings Use this screen to configure the Access Point's more advanced wireless settings such as Beacon interval, Output Power, etc.

VLAN & QoS Use this screen to configure the VLAN and QoS related settings for the Access Point.

AP Mode

Use this screen to configure the Access Point operation mode with WDS (Wireless Distribution System).

Administration

You will use the Administration tabs to manage the Access Point.

Management This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings.

Log Configure the Log settings for the Access Point on this screen.

Factory Default Use this screen to reset the Access Point to its factory default settings.

Firmware Upgrade Upgrade the Access Point's firmware on this screen.

Reboot Use this screen to reboot the Access Point.

Config Management You can back up the configuration file for the Access Point, as well as save the backup configuration file to the Access Point.

Status

You will be able to view status information for your local network, wireless networks, and network performance.

Local Network This screen displays system information, including software & hardware version, MAC address, and IP address on the LAN side of the Access Point.

Wireless This screen displays wireless network settings including SSID, network mode, and wireless channel.

System Performance This screen displays the current traffic statistics of the Access Point's Wireless and LAN ports.

Chapter 6: Advanced Configuration

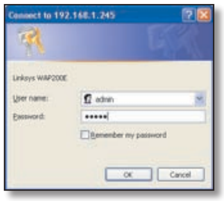
Open your web browser and enter **http://192.168.1.245** into the *Address* field. Press the **Enter** key and the *Password* screen will appear.

Address http://192.168.1.245

Address Bar

NOTE: The default IP address is **192.168.1.245**. If the IP address has been changed using DHCP or via the console interface, enter the assigned IP address instead of the default.

The first time you open the web-based utility, enter **admin (**the default username) in the *User name* field and enter it again in the *Password* field. Click the **OK** button. You can change the Access Point's password later from the *Administration > Management* screen.



Connect to 192.168.1.245

Linksys WAP200E

User name: admin

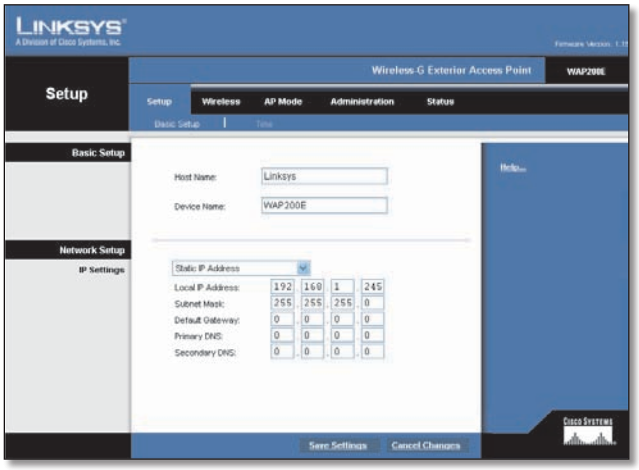
Password: •••••

Login Screen

Web-Based Utility

The first screen that appears in the web-based utility is the Setup screen. This allows you to change the Access Point's general settings. There are five tabs across the top of the screen: **Setup**, **Wireless**, **AP Mode**, **Administration**, and **Status**. Each tab contains screens that will help you configure and manage the Access Point.

Setup > Basic Setup



Host Name: Linksys

Device Name: WAP200E

Static IP Address

Local IP Address: 192 . 168 . 1 . 245

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Setup > Basic Setup

Enter names for the Access Point. The host name can be used to access the Web Utility through the network if DNS has been set up. The device name is for the benefit of identifying your Access Point after you log in.

Setup

Host Name This is the host name assigned to the Access Point. This host name will be published to your DNS server if the Access Point is configured to acquire the IP address through DHCP. In that case, Linksys recommends to follow the company policy on the host name assignment. The default name is Linksys.

Device Name You may assign any device name to the Access Point. This name is only used by the Access Point administrator for identification purposes. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. The default name is **WAP200E**.

Network Setup

The selections under this heading allow you to configure the Access Point's IP address setting(s).

IP Settings

Static IP Address Selected by default, this option is used to assign a static or fixed IP address to the Access Point.

- **Local IP Address** The IP address must be unique to your network. The default IP address is **192.168.1.245**.
- **Subnet Mask** The Subnet Mask must be the same as that set on the LAN that your Access Point is connected to. The default is **255.255.255.0**.
- **Default Gateway** Enter the Default Gateway Address, typically this is the IP address of your router.

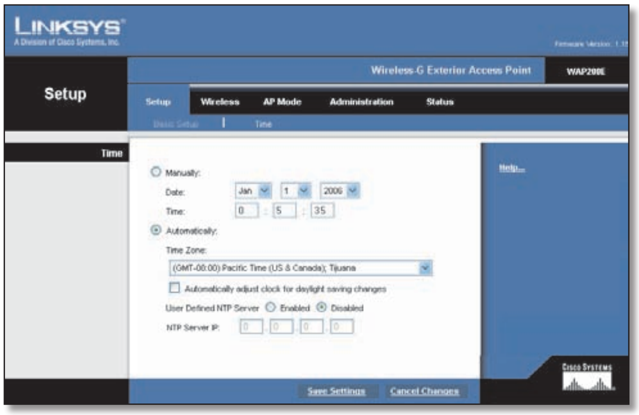
- **Primary DNS (Required) and Secondary DNS (Optional)** Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Automatic Configuration - DHCP If you have a DHCP server enabled on the LAN and want it to assign an IP address to the Access Point, the select this option.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

Setup > Time

This allows you to change the Access Point's time settings. The correct time setting can help the administrator to search the system log to identify problems.



○ Manually:
Date: Jan 1 2006
Time: 0 : 5 : 35
● Automatically:
Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana
☐ Automatically adjust clock for daylight saving changes
User Defined NTP Server ○ Enabled ● Disabled
NTP Server IP: 0 . 0 . 0 . 0

Setup > Time

Time

You can set the time either manually or automatically from a time server if the Access Point can access the public Internet. The default is to set the time **Automatically**.

Manually Select this option to set the date and time manually.

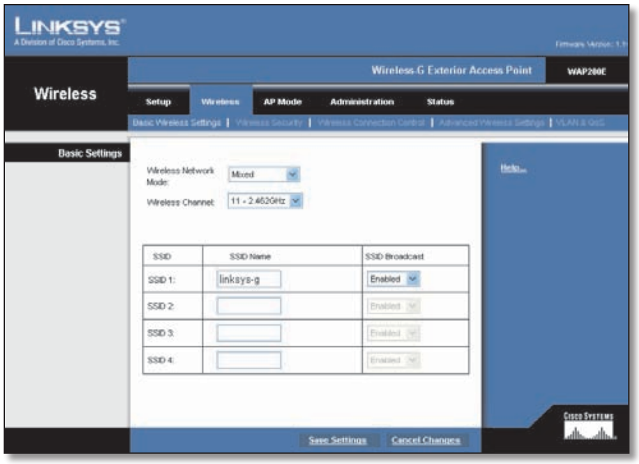
Automatically Select this option and time zone. The Access Point will contact the public time server to get the current time.

- **Automatically adjust clock for daylight saving changes** Select this option if you are in using the Access Point in a location that observes daylight saving time.
- **User Defined NTP Server** Enable this option if you have set up local NTP server. Default is Disabled.
- **NTP Server IP** Enter the IP address of user defined NTP Server.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

Wireless > Basic Wireless Settings

Change the basic wireless network settings on this screen. The Access Point can connect to up to four wireless networks (SSIDs) at the same time, so this screen offers settings for up to four different SSIDs. Each SSID owns its own MAC address on this Access Point.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Basic Settings
Help...
Save Settings
Cancel Changes
Cisco Systems

Wireless Network Mode: Mixed
Wireless Channel: 11 - 2.462GHz

SSID	SSID Name	SSID Broadcast
SSID 1:	linksys-g	Enabled
SSID 2:		Enabled
SSID 3:		Enabled
SSID 4:		Enabled

Wireless > Basic Wireless Settings

Basic Settings

Configure the Wireless Network basic attributes for the entire system and for each SSID.

Wireless Network Mode Select one of the following modes. The default is Mixed.

- **Disable** To disable wireless connectivity completely. This might be useful during system maintenance.
- **B-Only** All the wireless client devices can be connected to the Access Point at Wireless-B data rates with maximum speed at 11Mbps.
- **G-Only** Wireless-G client devices can be connected at Wireless-G data rates with maximum speed at 54Mbps. Wireless-B clients cannot be connected in this mode.
- **Mixed** Both Wireless-B and Wireless-G client devices can be connected at their respective data rates. Wireless-G devices can be connected at Wireless-G data rates.

Wireless Channel Select the appropriate channel to be used among your Access Point and your client devices. When Auto is selected, your Access Point will select the channel with the lowest amount of wireless interference while the system is powering up. Auto channel selection will start when you click **Save Settings** button, it will take several seconds to scan through all the channels to find the best channel. The default setting is **Auto**.

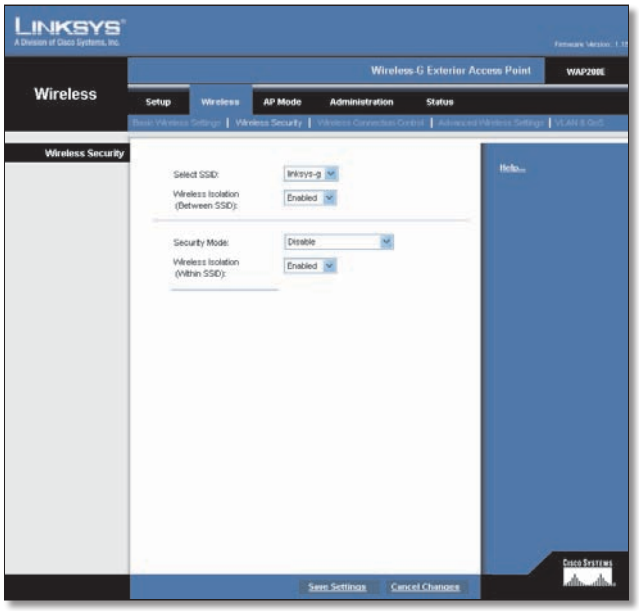
SSID Name The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is **linksys-g**.

SSID Broadcast This option allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network. Click Enabled to broadcast the SSID to all wireless devices in range. Click Disabled to increase network security and prevent the SSID from being seen on networked PCs. The default is **Enabled** in order to help users configure their network before use.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

Wireless > Wireless Security

Change the Access Point's wireless security settings on this screen.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.15
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...
Save Settings
Cancel Changes
Cisco Systems

Select SSID: linksys-g

Wireless Isolation (Between SSID): Enabled

Security Mode: Disable

Wireless Isolation (Within SSID): Enabled

Wireless > Wireless Security

Wireless Security

Select SSID Select any of the SSID names configured on the *Basic Wireless Settings* tab.

Wireless Isolation (between SSID) Wireless Isolation prevents eavesdropping in the network. When it is Enabled, wireless frames received on this Access Point will not be forwarded to other wireless networks (SSIDs). For example, if you have a wireless hotspot, you may want to keep the wireless network (SSID) isolated from your other wireless networks (SSIDs). This is a global option applying to all SSIDs. The default is **Enabled**.

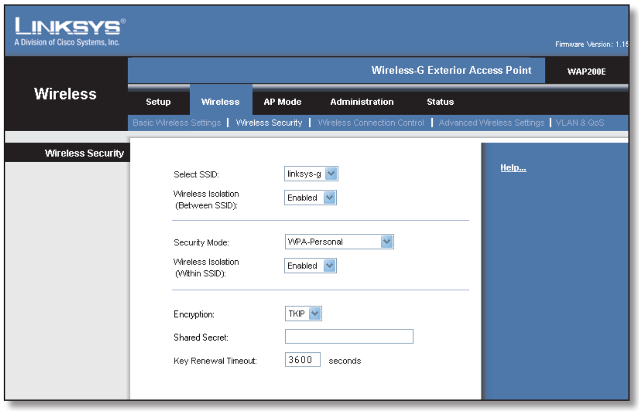
The following options are specific for each SSID:

Security Mode Select the wireless security mode you want to use: WPA-Personal, WPA2-Personal, WPA2-Personal Mixed, WPA-Enterprise, WPA2-Enterprise, WPA2-Enterprise Mixed, RADIUS, or WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11i. WEP stands for Wired Equivalent Privacy, Enterprise modes use a RADIUS server for authentication, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings. For detailed instructions on configuring wireless security for the Access Point, refer to "Appendix B: Wireless Security Checklist". To disable wireless security completely, select **Disabled**. The default is **Disabled**.

Wireless Isolation (within SSID) When disabled, wireless PCs that are associated to the same network name (SSID), can see and transfer files between each other. By enabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. The default is **Disabled**.

Following section describes the detailed options for each Security Mode.

WPA-Personal (aka WPA-PSK)


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.15
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g

Wireless Isolation (Between SSID): Enabled

Security Mode: WPA-Personal

Wireless Isolation (Within SSID): Enabled

Encryption: TKIP

Shared Secret:

Key Renewal Timeout: 3600 seconds

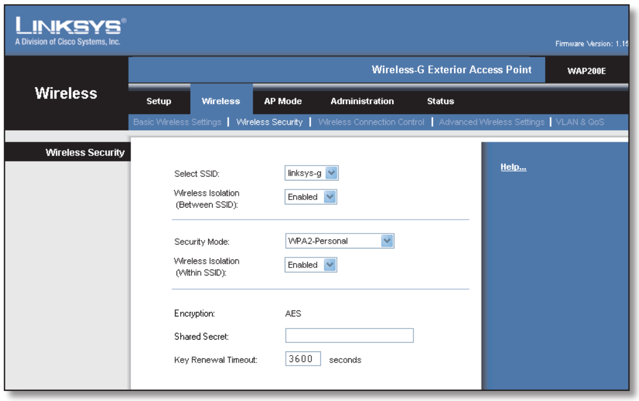
Wireless > Wireless Security > WPA-Personal

Encryption WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is **TKIP**.

Shared Secret Enter a shared secret of 8-63 characters.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Personal


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: WPA2-Personal
Wireless Isolation (Within SSID): Enabled
Encryption: AES
Shared Secret:
Key Renewal Timeout: 3600 seconds

Wireless > Wireless Security > WPA2-Personal

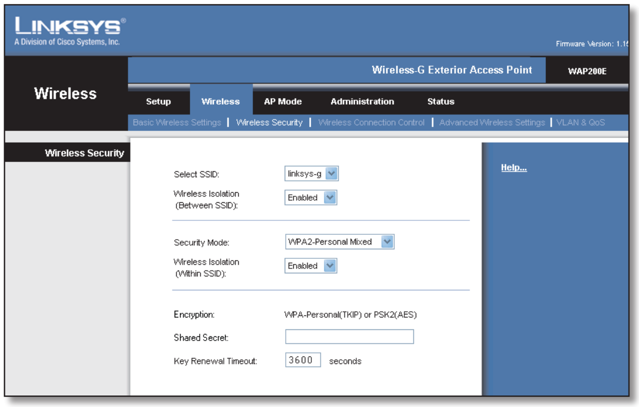
Encryption WPA2 always uses AES for data encryption.

Shared Secret Enter a shared secret of 8-63 characters.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Personal Mixed

This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The Access Point will automatically choose the encryption algorithm used by each client device.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: WPA2-Personal Mixed
Wireless Isolation (Within SSID): Enabled
Encryption: WPA-Personal(TKIP) or PSK2(AES)
Shared Secret:
Key Renewal Timeout: 3600 seconds

Wireless > Wireless Security > WPA2=Personal Mixed

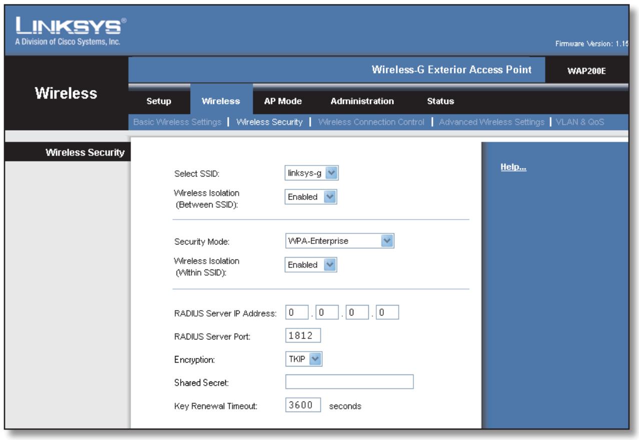
Encryption Mixed Mode automatically chooses TKIP or AES for data encryption.

Shared Secret Enter a shared secret of 8-63 characters.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA-Enterprise

This option features WPA used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: WPA-Enterprise
Wireless Isolation (Within SSID): Enabled
RADIUS Server IP Address: 0 . 0 . 0 . 0
RADIUS Server Port: 1812
Encryption: TKIP
Shared Secret:
Key Renewal Timeout: 3600 seconds

Wireless > Wireless Security > WPA-Enterprise

RADIUS Server IP Address Enter the RADIUS server's IP address.

RADIUS Server Port Enter the port number used by the RADIUS server. The default is **1812**.

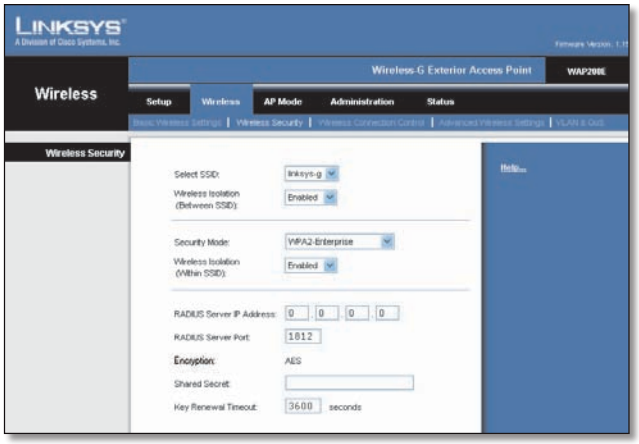
Encryption WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is **TKIP**.

Shared Secret Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Enterprise

This option features WPA2 used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless
Wireless-G Exterior Access Point
WAP200E
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: WPA2-Enterprise
Wireless Isolation (Within SSID): Enabled
RADIUS Server IP Address: 0 . 0 . 0 . 0
RADIUS Server Port: 1812
Encryption: AES
Shared Secret:
Key Renewal Timeout: 3600 seconds

Wireless > Wireless Security > WPA2-Enterprise

RADIUS Server IP Address Enter the RADIUS server's IP address.

RADIUS Server Port Enter the port number used by the RADIUS server. The default is **1812**.

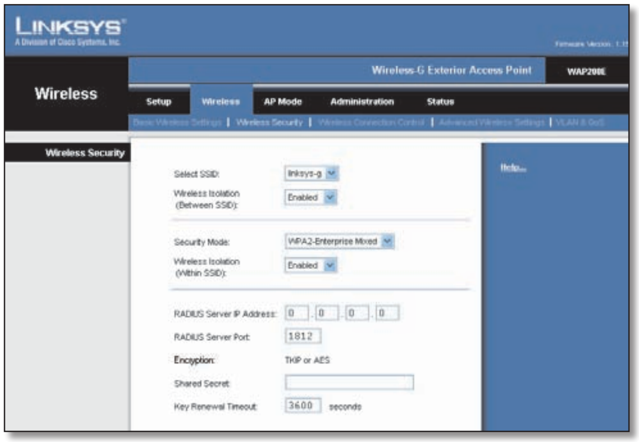
Encryption WPA2 always uses AES for data encryption.

Shared Secret Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Enterprise Mixed

This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The Access Point will automatically choose the encryption algorithm used by each client device.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless
Wireless-G Exterior Access Point
WAP200E
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: WPA2-Enterprise Mixed
Wireless Isolation (Within SSID): Enabled
RADIUS Server IP Address: 0 . 0 . 0 . 0
RADIUS Server Port: 1812
Encryption: TKIP or AES
Shared Secret:
Key Renewal Timeout: 3600 seconds

Wireless > Wireless Security > WPA2-Enterprise Mixed

RADIUS Server IP Address Enter the RADIUS server's IP address.

RADIUS Server Port Enter the port number used by the RADIUS server. The default is 1812.

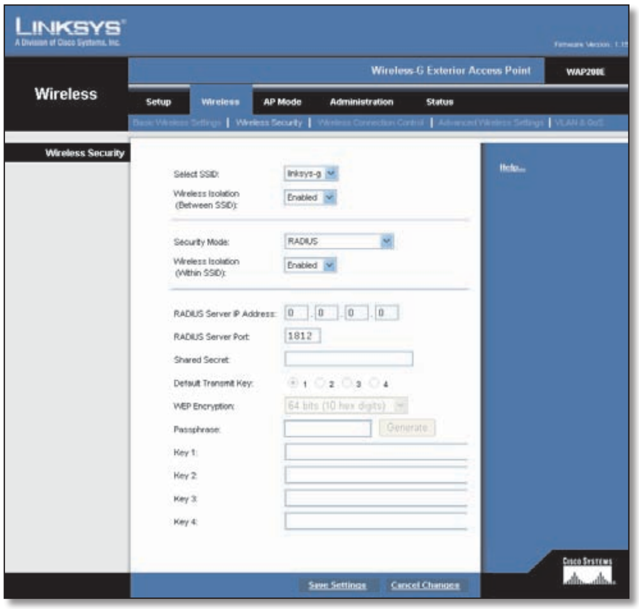
Encryption Mixed Mode automatically chooses TKIP or AES for data encryption.

Shared Secret Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds.

RADIUS

This security mode is also known as Dynamic WEP with IEEE 802.1X. A RADIUS server is used for client authentication and WEP is used for data encryption. The WEP key is automatically generated by the RADIUS server. Manual WEP key is no longer supported to ensure compatibility with Microsoft's Windows implementation.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless
Wireless-G Exterior Access Point
WAP200E
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...
Generate
Save Settings
Cancel Changes
Cisco Systems

Select SSID: linksys-g
Wireless Isolation (Between SSID): Enabled
Security Mode: RADIUS
Wireless Isolation (Within SSID): Enabled
RADIUS Server IP Address: 0 . 0 . 0 . 0
RADIUS Server Port: 1812
Shared Secret:
Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4
WEP Encryption: 64 bits (10 hex digits)
Passphrase:
Key 1:
Key 2:
Key 3:
Key 4:

Wireless > Wireless Security > RADIUS

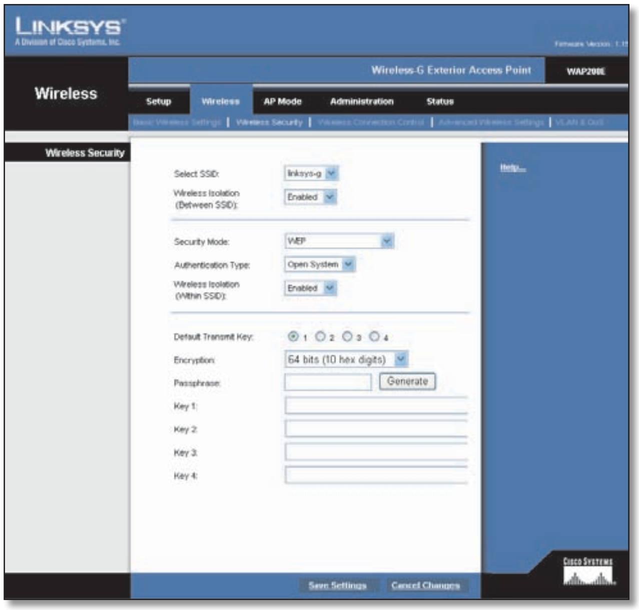
RADIUS Server IP Address Enter the RADIUS server's IP address.

RADIUS Server Port Enter the port number used by the RADIUS server. The default is 1812.

Shared Secret Enter the Shared Secret key used by the Access Point and RADIUS server.

WEP

This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.15
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Security
Help...
Generate
Save Settings
Cancel Changes
Cisco Systems

Select SSID: linksys-g

Wireless Isolation (Between SSID): Enabled

Security Mode: WEP

Authentication Type: Open System

Wireless Isolation (Within SSID): Enabled

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

Encryption: 64 bits (10 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Wireless > Wireless Security > WEP

Authentication Type Choose the 802.11 authentication type as either Open System or Shared Key. The default is Open System.

Default Transmit Key Select the key to be used for data encryption.

Encryption Select a level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits).

Passphrase If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the Generate key. Those auto-generated keys are not as strong as manual WEP keys.

Key 1-4 If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

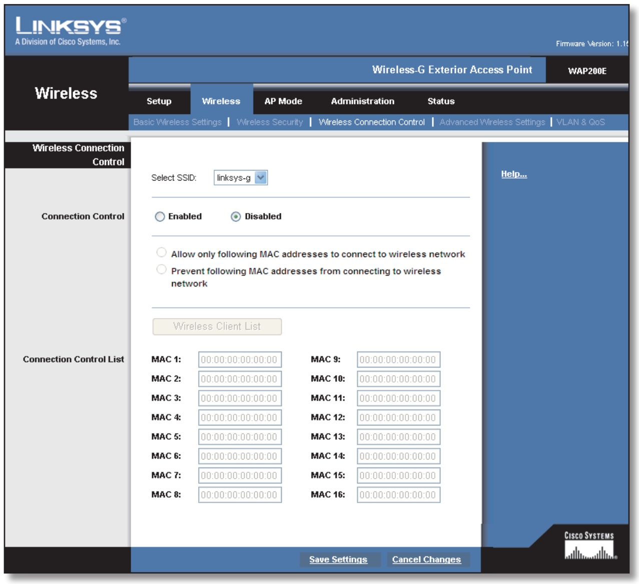
Disable

There is no option to be configured for this mode.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is available on the right side of the screen.

Wireless > Wireless Connection Control

This screen allows you to configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the Access Point.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.15
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Wireless Connection Control
Connection Control
Connection Control List
Help...
Wireless Client List
Save Settings
Cancel Changes
Cisco Systems

Select SSID: linksys-g

Connection Control: ○ Enabled ● Disabled

○ Allow only following MAC addresses to connect to wireless network

○ Prevent following MAC addresses from connecting to wireless network

MAC 1:	00:00:00:00:00:00	MAC 9:	00:00:00:00:00:00
MAC 2:	00:00:00:00:00:00	MAC 10:	00:00:00:00:00:00
MAC 3:	00:00:00:00:00:00	MAC 11:	00:00:00:00:00:00
MAC 4:	00:00:00:00:00:00	MAC 12:	00:00:00:00:00:00
MAC 5:	00:00:00:00:00:00	MAC 13:	00:00:00:00:00:00
MAC 6:	00:00:00:00:00:00	MAC 14:	00:00:00:00:00:00
MAC 7:	00:00:00:00:00:00	MAC 15:	00:00:00:00:00:00
MAC 8:	00:00:00:00:00:00	MAC 16:	00:00:00:00:00:00

Wireless > Wireless Connection Control

Wireless Connection Control

Select SSID Select the SSID of the wireless network that you want to use wireless connection control on.

Enabled/Disabled Enable or disable wireless connection control. The default is disabled.

Connection Control

Allow only following MAC addresses to connect to wireless network When this option is selected, only devices with a MAC address specified in the Connection Control List can connect to the Access Point.

Prevent following MAC addresses from connecting to wireless network When this option is selected, devices with a MAC address specified in the Connection Control List will not be allowed to connect to the Access Point.

Wireless Client List

Instead of manually entering the MAC addresses of each client, the Access Point provides a convenient way to select a specific client device from the client association table. Click this button and a window appears to let you select a MAC address from the table. The selected MAC address will be entered into the Connection Control List.

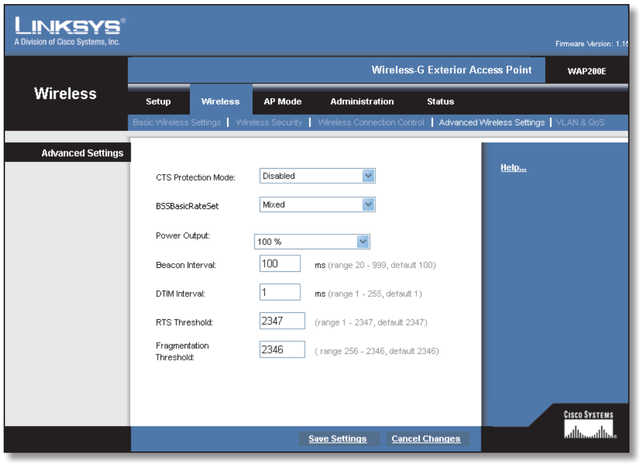
Connection Control List

MAC 01-16 Enter the MAC addresses of the wireless client devices you want to control.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

Wireless > Advanced Wireless Settings

This screen allows you to configure the advanced settings for the Access Point. Linksys recommends to let your Access Point automatically adjust the parameters for maximum data throughput.



LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: 1.15
Wireless
Wireless-G Exterior Access Point
WAP200E
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
Advanced Settings
Help...
Save Settings
Cancel Changes
Cisco Systems

CTS Protection Mode: Disabled

BSSBasicRateSet: Mixed

Power Output: 100 %

Beacon Interval: 100 ms (range 20 - 999, default 100)

DTIM Interval: 1 ms (range 1 - 255, default 1)

RTS Threshold: 2347 (range 1 - 2347, default 2347)

Fragmentation Threshold: 2346 (range 256 - 2346, default 2346)

Wireless > Advanced Wireless Settings

Advanced Settings

CTS Protection Mode CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all wireless transmissions, but will severely decrease performance. Keep the default setting, **Auto**, so the Access Point can use this feature as needed, when the Wireless-G products are not able to transmit to the Access Point in an environment with heavy 802.11b traffic. Select **Disabled** if you want to permanently disable this feature.

BSSBasicRateSet This setting is a series of rates that are advertised to other wireless devices as defined in IEEE 802.11 specifications, so they know which data rates the Access Point can support. One of the rates is picked from the list for transmitting control frames, broadcast/multicast frames, or ACK frames. To support both 802.11b & 802.11g devices, use the Default (**Mixed mode**) setting so that frames can be decoded by all devices. To support 802.11g devices only, use the All (G-only mode) setting to achieve higher frame rates. For regular data frames, the transmission rate is configured through the Tx Rate Limiting on the *Wireless > VLAN & QoS* tab.

Power Output You can adjust the output power of the Access Point to get the appropriate coverage for your wireless network. Select the level you need for your environment. If you are not sure of which setting to choose, then keep the default setting, **100%**.

Beacon Interval This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless networks service area, the Access Point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). The default is **100 ms**.

DTIM Interval This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions. The default is **1 ms**.

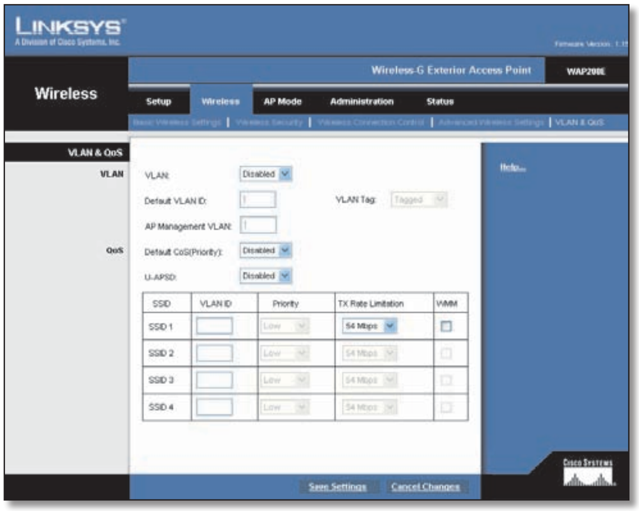
RTS Threshold This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.

Fragmentation Threshold This specifies the maximum size a data packet can be before splitting and creating a new packet. It should remain at its default setting of **2346**. A smaller setting means smaller packets, which will create more packets for each transmission. If you experience high packet error rates, you can decrease this value, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.

Wireless > VLAN & QoS

This screen allows you to configure the VLAN and QoS related settings for the Access Point.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 1.1
Wireless-G Exterior Access Point
WAP200E
Wireless
Setup
Wireless
AP Mode
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless Connection Control | Advanced Wireless Settings | VLAN & QoS
VLAN & QoS
VLAN
QoS
Help...
Save Settings
Cancel Changes
Cisco Systems

VLAN: Disabled
Default VLAN ID: 1
VLAN Tag: Tagged
AP Management VLAN: 1
Default CoS(Priority): Disabled
U-APSD: Disabled

SSID	VLAN ID	Priority	TX Rate Limitation	WMM
SSID 1		Low	54 Mbps	□
SSID 2		Low	54 Mbps	□
SSID 3		Low	54 Mbps	□
SSID 4		Low	54 Mbps	□

Wireless > VLAN & QoS

VLAN

The following options are global VLAN settings for the Access Point.

VLAN Select Enabled if you want to pass 802.1q VLAN tagged traffic between the wired LAN and wireless LAN. Your Access Point will map the VLAN tag (wired side) to different SSIDs (wireless side) according to your specified settings. Select Disabled and your Access Point will drop all tagged traffic coming in from the wired LAN. The default is **Disabled**.

Default VLAN ID Enter the default VLAN ID number (1 - 4094), the default value is **1**. The default VLAN number should match with your Switch's settings. For example, the SRW2024 has Trunk port mode which set default VLAN (PVID) to 1 untagged, while General port mode can set PVID to any VLAN either tagged or untagged.

VLAN Tag Set the tagging option for the default VLAN ID. This has to match your Switch's settings. The default is **untagged**.

AP Management VLAN When the VLAN option is enabled, the value entered (VLAN ID) in this field defines the VLAN that connects to the Access Point. The default value is **1**. The VLAN should be accessible from the wired side in order to use web-based utility. To access the web-based utility from wireless side, the SSID needs to map to the same VLAN ID. Remember to enable wireless web access on the *Administration > Management* tab.

QoS

The following options are VLAN global settings for the Access Point.

Default CoS (Priority) Select Enabled if you want to assign a default CoS value to each SSID. This option is automatically enabled when the VLAN option is enabled. The default is **Disabled**.

U-APSD (Unscheduled Automatic Power Save Delivery) This option is only available when WMM is enabled on any of the SSIDs. Select Enabled if you want client devices with U-APSD capability to take advantage of the power save mode. The default is **Disabled**.

SSID Name Displays the SSIDs defined under the Basic Wireless Settings tab. If an SSID has been disabled, the options cannot be configured.

VLAN ID Select a VLAN ID (1 - 4094) for the SSID where you want to map the traffic to on the wired side. The wireless traffic will not carry VLAN information. Multiple SSIDs can map to the same VLAN on the wired side.

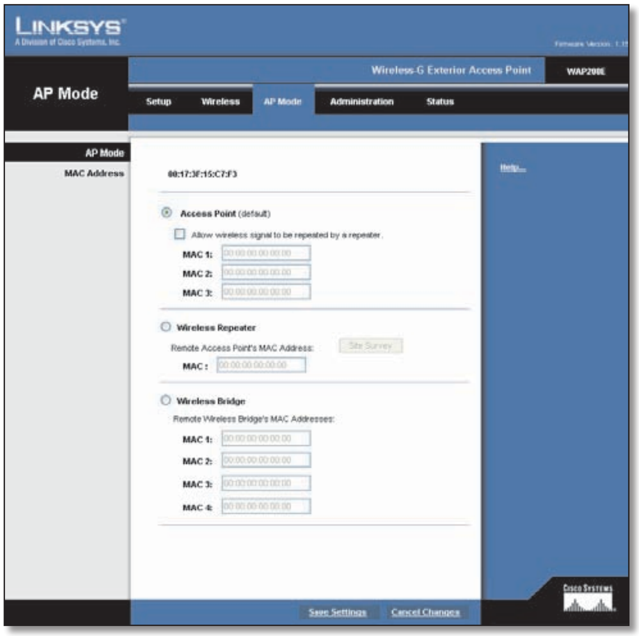
Priority You can assign the default priority (802.1p COS bits) for packets coming in from each wireless network by selecting a number from the drop-down menu. The higher the number, the higher the priority will be. The default is 0.

Tx Rate Limitation You can limit the maximum data rate used in your network to save bandwidth and power consumption on client devices. The actual data rate is determined by the Auto-Fallback mechanism between your Access Point and a client device. The default is 54 Mbps for Mixed or G-Only wireless mode, 11 Mbps for B-Only mode.

WMM Wi-Fi Multimedia is a QoS feature defined by the WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When this is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in the IP or layer 2 header). WMM provides the capability to prioritize wireless traffic in your environment. The default is **Disabled** (unchecked).

AP Mode

On this screen you can change the Access Point's mode of operation. In most cases, you can keep the default setting - Access Point. You may wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless repeater to extend the range of your wireless network. You may also wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless bridge; for example, you can use two Access Points in Wireless Bridge mode to connect two wired networks that are in two different buildings.



AP Mode

MAC Address: 00:17:3F:15:C7:F3

● Access Point (default)

□ Allow wireless signal to be repeated by a repeater.

MAC 1: 00:00:00:00:00:00
MAC 2: 00:00:00:00:00:00
MAC 3: 00:00:00:00:00:00

○ Wireless Repeater

Remote Access Point's MAC Address: Site Survey

MAC : 00:00:00:00:00:00

○ Wireless Bridge

Remote Wireless Bridge's MAC Addresses:

MAC 1: 00:00:00:00:00:00
MAC 2: 00:00:00:00:00:00
MAC 3: 00:00:00:00:00:00
MAC 4: 00:00:00:00:00:00

AP Mode

The Access Point offers three modes of operation: Access Point, Wireless Repeater, and Wireless Bridge. For the Repeater and Bridge modes, make sure the SSID, channel, and security settings are the same for the other wireless access points/devices.

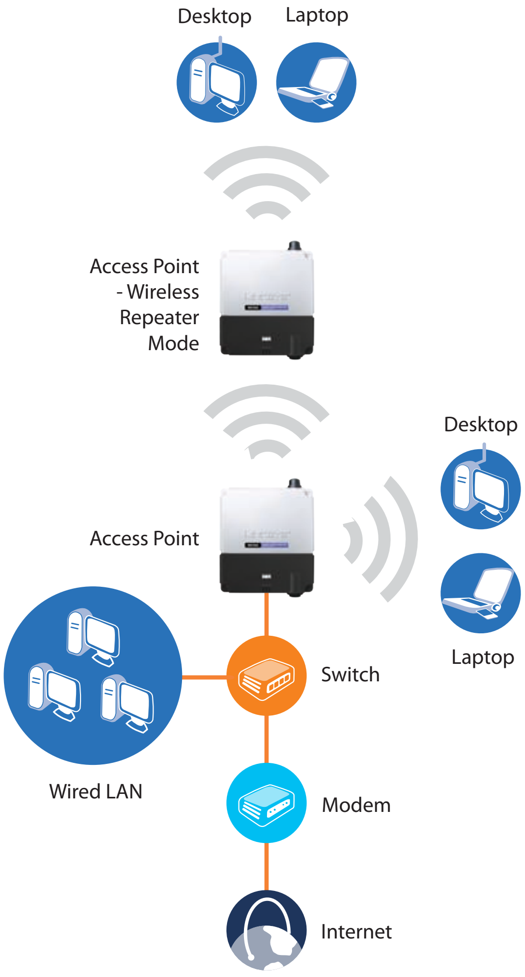
MAC Address

The MAC address of the Access Point is displayed here.

Access Point The Mode is set to Access Point by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary.

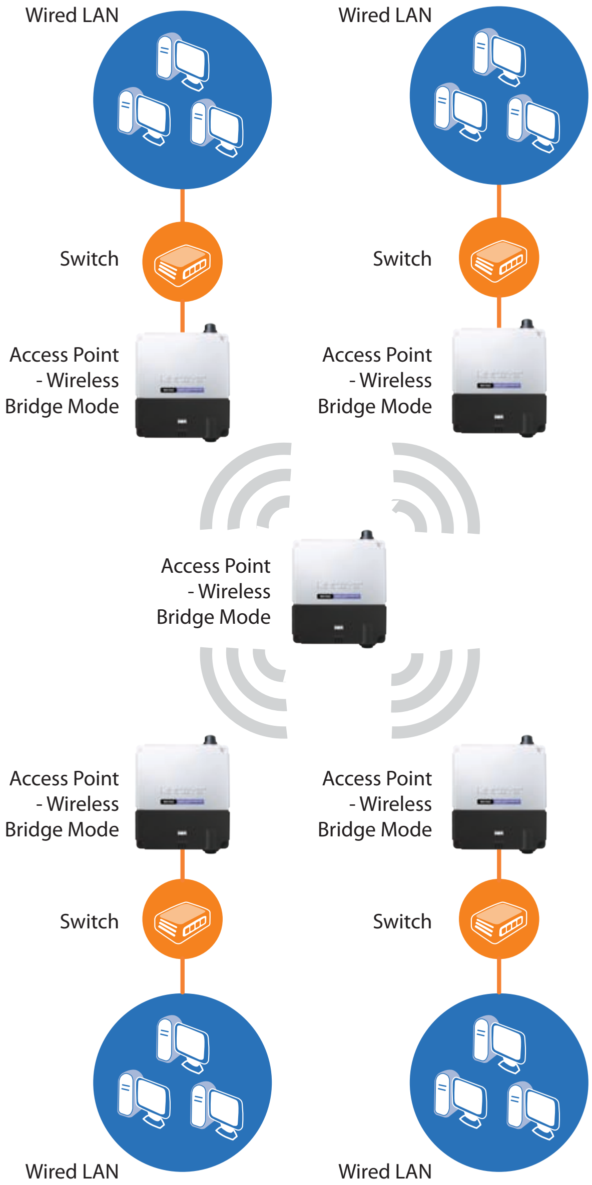
- **Allow wireless signal to be repeated by a repeater** Select this option if you want to use another wireless device to repeat the signal of this Access Point. You will need to enter the MAC address(es) of the repeating device(s). Up to 3 repeaters can be used.

Wireless Repeater When set to Wireless Repeater mode, the Wireless Repeater is able to talk to up a remote access point within its range and retransmit its signal. Click **Site Survey** to select the access point that will have its signal repeated by this Access Point or enter the MAC address of the access point manually.



Wireless Repeater Mode

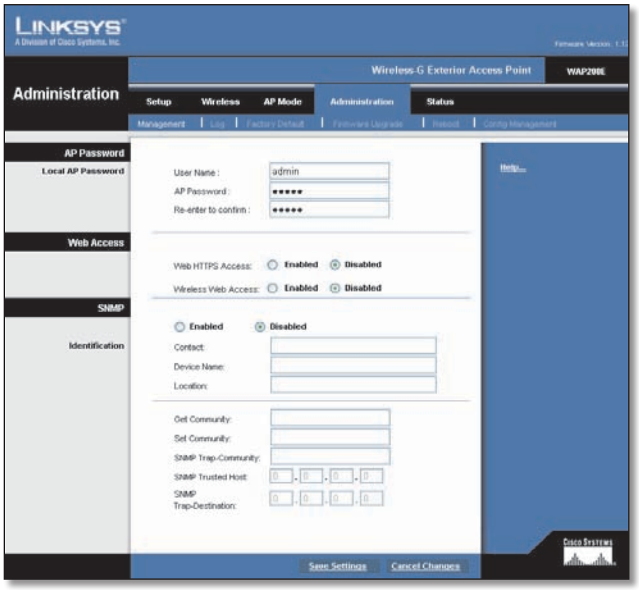
Wireless Bridge This mode connects physically separated wired networks using multiple access points. Wireless clients will not be able to connect to the access point in this mode. Enter the MAC address(es) of the access point(s) that will bridge to this access point.


Wired LAN
Wired LAN
Switch
Switch
Access Point - Wireless Bridge Mode
Access Point - Wireless Bridge Mode
Access Point - Wireless Bridge Mode
Access Point - Wireless Bridge Mode
Access Point - Wireless Bridge Mode
Switch
Switch
Wired LAN
Wired LAN

Wireless Bridge Mode

Administration > Management

On this screen you can configure the password, Web Access, and SNMP settings.



AP Password

Local AP Password

User Name : admin

AP Password : *****

Re-enter to confirm : *****

Web Access

Web HTTPS Access: ○ Enabled ● Disabled

Wireless Web Access: ○ Enabled ● Disabled

SNMP

○ Enabled ● Disabled

Identification

Contact:

Device Name:

Location:

Get Community:

Set Community:

SNMP Trap-Community:

SNMP Trusted Host: 0 . 0 . 0 . 0

SNMP Trap-Destination: 0 . 0 . 0 . 0

Administration > Management

AP Password

You should change the username/password that controls access to the Access Point's web-based utility.

Local AP Password

User Name Modify the administrator username. The default is admin.

AP Password Modify the administrator password for the Access Point's web-based utility. The default is admin.

Re-enter to confirm To confirm the new Password, enter it again in this field.

Web Access

To increase the security on accessing web-based utility. You can enable HTTPS. Once enabled, users need to use https:// when accessing the web-based utility.

Web HTTPS Access Use secured HTTP session to access Web based Utility. The default is **Disabled**.

Wireless Web Access Allow or deny wireless clients to access Web based Utility. The default is **Enabled**.

SNMP

SNMP is a popular network monitoring and management protocol. It provides network administrators with the ability to monitor the status of the Access Point and receive notification of any critical events as they occur on the Access Point.

To enable the SNMP support feature, select **Enabled**. Otherwise, select **Disabled**. The default is **Disabled**.

Identification

Contact Enter the name of the contact person, such as a network administrator, for the Access Point.

Device Name Enter the name you wish to give to the Access Point.

Location Enter the location of the Access Point.

Get Community Enter the password that allows read-only access to the Access Point's SNMP information.

Set Community Enter the password that allows read/write access to the Access Point's SNMP information.

SNMP Trap-Community Enter the password required by the remote host computer that will receive trap messages or notices sent by the Access Point.

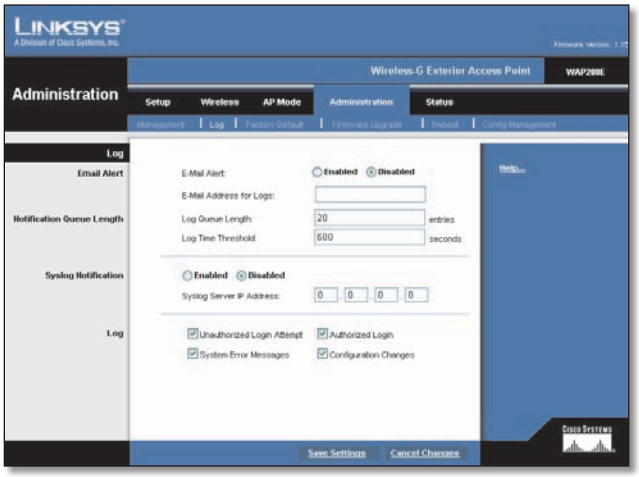
SNMP Trusted Host You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.

SNMP Trap-Destination Enter the IP address of the remote host computer that will receive the trap messages.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **Help** for additional details.

Administration > Log

On this screen you can configure the log settings and alerts of particular events.



Log

Email Alert

E-Mail Alert: ○ Enabled ● Disabled

E-Mail Address for Logs:

Notification Queue Length

Log Queue Length: 20 entries

Log Time Threshold: 600 seconds

Syslog Notification

○ Enabled ● Disabled

Syslog Server IP Address: 0 . 0 . 0 . 0

Log

☑ Unauthorized Login Attempt ☑ Authorized Login

☑ System Error Messages ☑ Configuration Changes

Administration > Log

Log

You can have logs that keep track of the Access Point's activities.

Email Alert

E-Mail Alert If you want the Access Point to send e-mail alerts in the event of certain activities, select **Enabled**. The default is **Disabled**.

E-Mail Address for Logs Enter the e-mail address that will receive logs.

Notification Queue Length

Log Queue Length You can designate the length of the log that will be e-mailed to you. The default is 20 entries.

Log Time Threshold You can designate how often the log will be emailed to you. The default is 600 seconds (10 minutes).

Syslog Notification

Syslog is a standard protocol used to capture information about network activity. The Access Point supports this protocol and sends its activity logs to an external server. To enable Syslog, select **Enabled**. The default is **Disabled**.

Syslog Server IP Address Enter the IP address of the Syslog server. In addition to the standard event log, the Access Point can send a detailed log to an external Syslog server. The Access Point's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP server, and number of bytes transferred.

Log

Select the events that you want the Access Point to keep a log.

Unauthorized Login Attempt If you want to receive alert logs about any unauthorized login attempts, click the checkbox.

Authorized Login If you want to log authorized logins, click the checkbox.

System Error Messages If you want to log system error messages, click the checkbox.

Configuration Changes If you want to log any configuration changes, click the checkbox.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is available on the right side of the screen.