ADMINISTRATION GUIDE

Cisco Small Business

WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster

OL-20284-01

Contents

1

Introduction

Thank you for choosing the Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster.

This access point lets you connect Wireless-G (802.11g) or Wireless-B (802.11b) devices to your wired network so you can add computers to the network wirelessly.

The WAP200 also offers the convenience of Power over Ethernet (PoE) capability, so it can receive data and power over a single Ethernet network cable. You can even connect wired networks in two different buildings, by using two access points set to Wireless Bridge mode.

2

Planning Your Wireless Network

Before deploying your Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster, take some time to plan your wireless network.

This chapter includes the following topics:

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 computers equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point.

Cisco 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 computer 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 computer to a wired network, and may double the effective wireless transmission range for two wireless adapter computers.

Because an access point can forward data within a network, the effective transmission range in an infrastructure network may be doubled (depending on antenna characteristics).

Roaming

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

This access point has 802.11F Inter-Access Point Protocol (IAPP) to complete the roaming process in seconds. If your wireless networks share the same IP subnet, this does not disrupt your data connection while moving around.

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.

Network Layout

The WAP200 Access Point supports 802.11g and 802.11b products such as the notebook adapters for your laptop computers, PCI adapters for your desktop computers, and USB adapters.

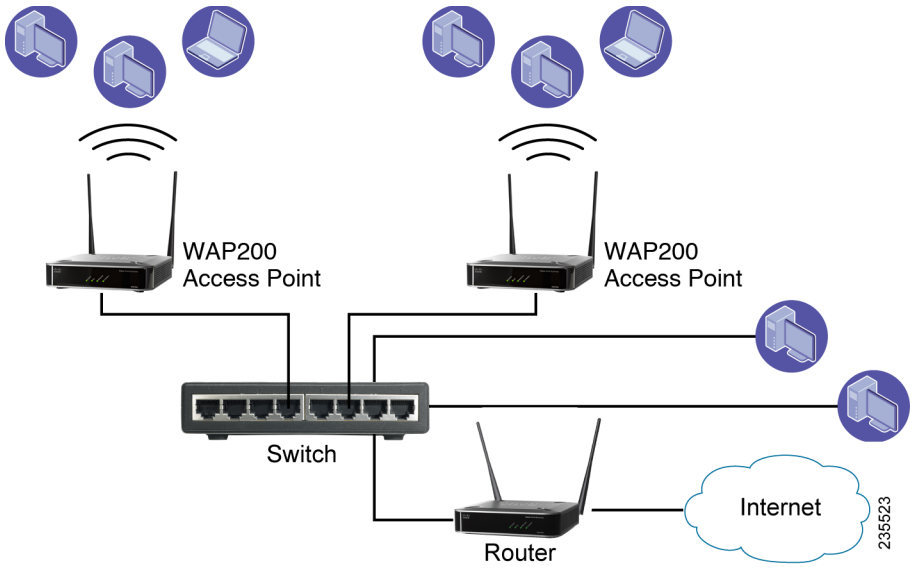
These wireless products can also communicate with a 802.11g or 802.11b wireless print server.

To link your wired network to your wireless network, connect the access point's Ethernet network port to any switch or router with PoE.

For more information about wireless products, visit the Cisco website at www.cisco.com.

Example of a Simple Wireless Network

The following diagram shows a typical infrastructure wireless network setup.



In this example, the wireless access points connect to and receive power from a PoE Cisco switch. Each access point can connect multiple wireless devices to the network.

This network provides connectivity among wireless network devices and computers that have a wired connection to the switch.

The switch connects to a router that connects to the Internet.

3

Product Overview

This chapter describes the physical features of the Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster. The following topics are included:

Front Panel

The LEDs on the front panel of the access point display information about network activity.

- **Power LED**—Lights up and remains lit when the access point is powered on.
- **PoE LED**—Lights up when the access point is powered through an Ethernet cable.
- **Wireless LED**—Lights up when the wireless module is active on the access point.

  This LED flashes when the access point is actively sending to or receiving data from a wireless device.
- **Ethernet LED**—Lights up when the access point successfully connects to a device through the Ethernet network port.

  This LED flashes when the access point is actively sending to or receiving data from one of the devices over the Ethernet network port

Back Panel

The access point's Reset button, Ethernet port and Power port are located on the back panel.

Reset Button—There are two ways to reset the access point's factory default configuration:

- Press the Reset button for approximately ten seconds.
- Restore the default settings using the access point's web-based configuration utility.

CAUTION Resetting the access point erases all of your custom settings and replaces them with the factory defaults. Before resetting the access point, save your settings to disk so you can restore them later, as described in **"Managing the Access Point's Configuration" on page 68**.

ETHERNET Port—Connects the access point to Ethernet network devices, such as a switch or router that may or may not support PoE.

POWER Port—Connects the access point to power using the supplied power adapter. Use this port if you do not have a PoE switch in your network.

Antennas and Positions

The WAP200 access point has two detachable 2dBi omni-directional antennas. These antennas are located on the back of the device.

For best range performance, adjust the two antennas so that they form a 90 degree angle.

4

Installing the Access Point

This chapter explains how to mount and connect the Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster. The following topics are included:

Placement Tips

You can place the access point horizontally on its rubber feet, vertically in a stand, or mount it on the wall.

- **Ambient Temperature**—To prevent the Product Number Here from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow**—Be sure that there is adequate air flow around the Product Number Here.
- **Mechanical Loading**—Be sure that the Product Number Here is level and stable to avoid any hazardous conditions.

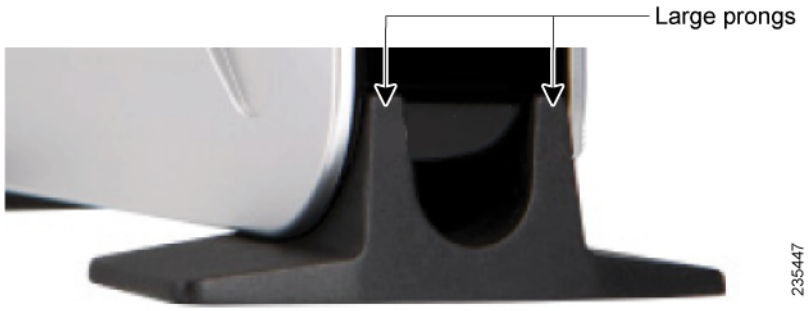
Stand Option

To place the access point vertically in a stand, follow these steps.

STEP 1 Locate the left side panel of the WAP200 access point.

STEP 2 With the two large prongs of one of the stands facing outward, insert the short prongs into the little slots in the WAP200 access point, and push the stand upward until the stand snaps into place.

Repeat this step with the second stand.

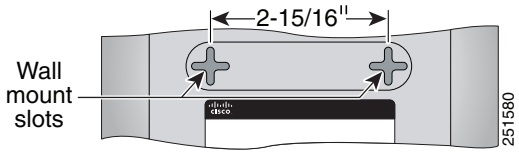


Wall-Mount Option

To mount the WAP200 access point on a wall, follow these steps.

STEP 1 Determine where you want to mount the WAP200 access point and install two screws (not supplied) that are 2-15/16 inches apart (approximately 7.46 cm.).

STEP 2 With the back panel pointing up (if installing vertically), line up the WAP200 access point so that the wall-mount crisscross slots on the bottom of the access point line up with the two screws.



STEP 3 Place the wall-mount slots over the screws and slide the WAP200 access point down until the screws fit snugly into the wall-mount slots.

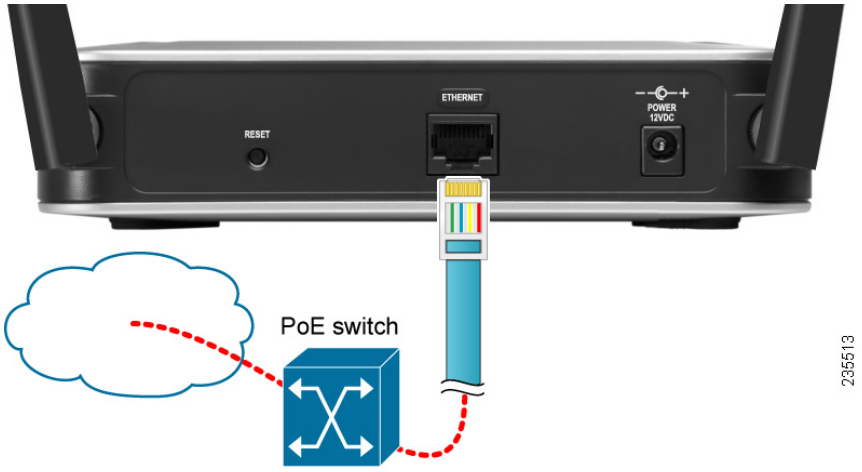
Connecting the Equipment

You can connect the WAP200 access point to your network in one of the following ways:

- Using a PoE switch
- Using a standard switch

Using a PoE Switch to Connect the WAP200 to the Network

To connect the WAP200 access point to your network using a PoE switch, simply connect the Ethernet port of the access point to an Ethernet port on the PoE switch.



The LEDs on the front panel light up when the WAP200 access point powers on.

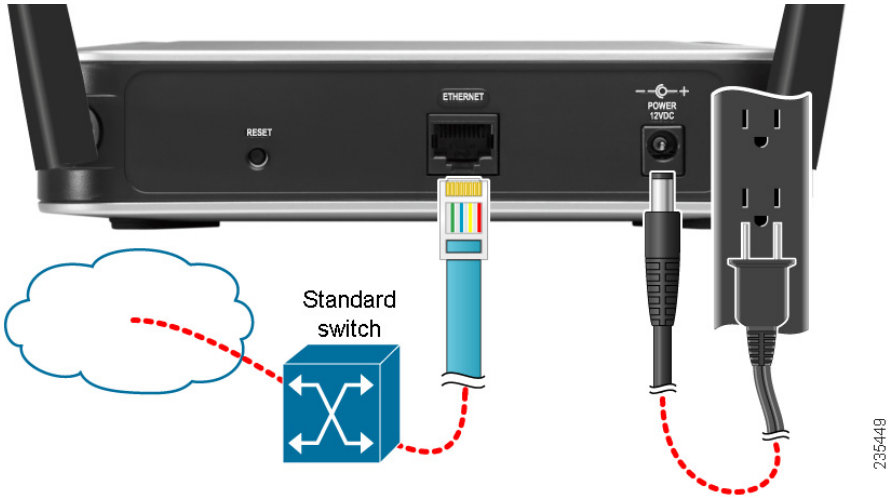
Using a Standard Switch to Connect the WAP200 to the Network

To connect the WAP200 access point to your network using a standard switch, follow these steps.

STEP 1 Use the supplied Ethernet cable to connect the Ethernet port of the access point to an Ethernet port on the switch.

STEP 2 Connect the included power adapter to the Power port of the WAP200 access point.

STEP 3 Plug the power adapter into an electrical outlet.



The LEDs on the front panel light up when the WAP200 access point powers on.

Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the cable connections.
- Check the LED states. See **Chapter 3, "Product Overview."**

NOTE If you need help resolving a problem, visit the Cisco Small Business Support Community at www.cisco.com/go/smallbizsupport. For technical documentation and other links, see **Appendix D, "Where to Go From Here."**

5

Getting Started

The Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster works right out of the box with the default settings. However, you can change these settings using the WAP200 web-based configuration utility.

Before You Begin

Before you begin to use the WAP200 web-based configuration utility, make sure that you have a computer that meets the following requirements:

- Internet Explorer (version 6 or later) or Mozilla Firefox.
- Your computer is connected to the same network as the WAP200. By default, the WAP200 access point has an IP address of 192.168.1.245 and a default mask of 255.255.255.0.

Accessing the Web-Based Configuration Utility

To access the WAP200 configuration utility, follow these steps:

STEP 1 Start a web browser. In the Address bar, enter the default IP address of the WAP200: **192.168.1.245**.

STEP 2 When the login page appears, enter the user name and password.

The default user name is **admin**.

The default password is **admin**. Passwords are case sensitive.

STEP 3 Click **OK**.

Navigating the Web-Based Utility

The web-based utility consists of the following five main windows:

- Setup
- Wireless
- AP Mode
- Administration
- Status

Additional windows branch out from these main windows.

For a basic network setup, you may only need to use the following windows of the web-based configuration utility:

- **Setup**—Enter your basic network settings.
- **Management**—Click **Administration > Management** and create a new password to replace the default password (admin).
- **Wireless**—To change the default SSID, click **Wireless > Basic Settings** and make the necessary changes. To change the level of security, click **Wireless > Security** and make the necessary changes.

Setup

This window allows you to configure the host name and IP address settings and to set the time through the following windows:

- **Basic Setup**—Configures the Host Name and IP Address settings for this access point.
- **Time**—Sets the time either manually, or automatically from a time server if the access point can access the public internet.

Wireless

This window allows you to enter a variety of wireless settings for the access point.

- **Basic Wireless Settings**—Chooses the wireless network mode (for example, wireless-G), wireless channel, and SSID configuration on this window.
- **Wireless Security**—Configures the access point's security settings including access authentication, data encryption, and wireless isolation.
- **Wireless Connection Control**—Populates your access list to permit or block specific MAC addresses from accessing your wireless network.
- **Advanced Wireless Settings**—Configures the access point's more advanced wireless settings such as beacon interval and output power.
- **VLAN & QoS**—Configures the VLAN and QoS related settings for the access point.

AP Mode

This window allows you to configure the access point operation mode with the Wireless Distribution System (WDS).

Administration

This window allows you to manage the access point:

- **Management**—Configures the password and Simple Network Management Protocol (SNMP) settings.
- **Log**—Configures the log settings for the access point.
- **Factory Default**—Resets the access point to its factory default settings.
- **Firmware Upgrade**—Upgrades the access point's firmware on this window.
- **Reboot**—Reboots the access point.
- **Config Management**—Backs up the configuration file for the access point, as well as uploads the backup configuration file to the access point.

Status

This window allows you to view status information about your local network, wireless networks, and network performance.

- **Local Network**—Displays system information, including software and hardware version, MAC address, and IP address on the LAN side of the access point.
- **Wireless**—Displays wireless network settings including SSID, network mode, and wireless channel.
- **System Performance**—Displays the current traffic statistics of the access point's Wireless and LAN ports.

6

Configuring the WAP200 Access Point

This chapter describes how to configure your Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster using the web-based configuration utility. Configuration is not required if you wish to use the access point right out of the box with its default settings.

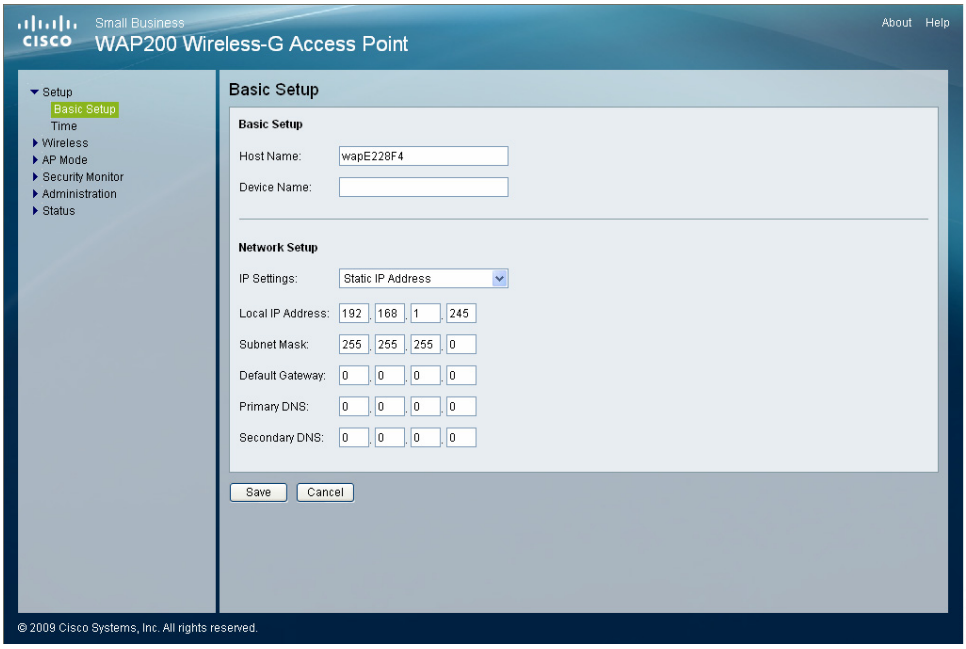
This chapter includes the following sections:

Setting Up Your Access Point

This section describes how to configure the general settings of the access point:

Configuring Basic Setup Settings

The Setup > Basic Setup window displays the general settings of the access point.



You can configure the following basic setup settings:

Configuring Basic Setup Settings

To configure the basic setup settings of the access point, follow these steps:

STEP 1 Click **Setup > Basic Setup**.

STEP 2 In the Basic Setup section, configure the following settings:

- **Host Name**—Enter the host name of the access point.

  You can use the host name to access the web-based configuration utility through the network if a record of the host name exists in your DNS server.

  The access point publishes the host name to your DNS server if you configured the access point to acquire the IP address from a DHCP server.

  Follow your organization's policy when assigning this name. The default name is **Cisco**.

- **Device Name**—Enter the device name for the access point.

  This name is only for identification purposes, for your convenience. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. This name helps you identify the access point after you log in.

  The default name is **WAP200**.

STEP 3 Click **Save**.

Configuring Network Setup Settings

To configure the network setup settings of the access point, follow these steps:

STEP 1 Click **Setup > Basic Setup**.

STEP 2 From the IP Settings drop-down menu, select one of the following options:

- **Static IP Address**—Select this option to assign a static or fixed IP address to the access point.
- **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, select this option.

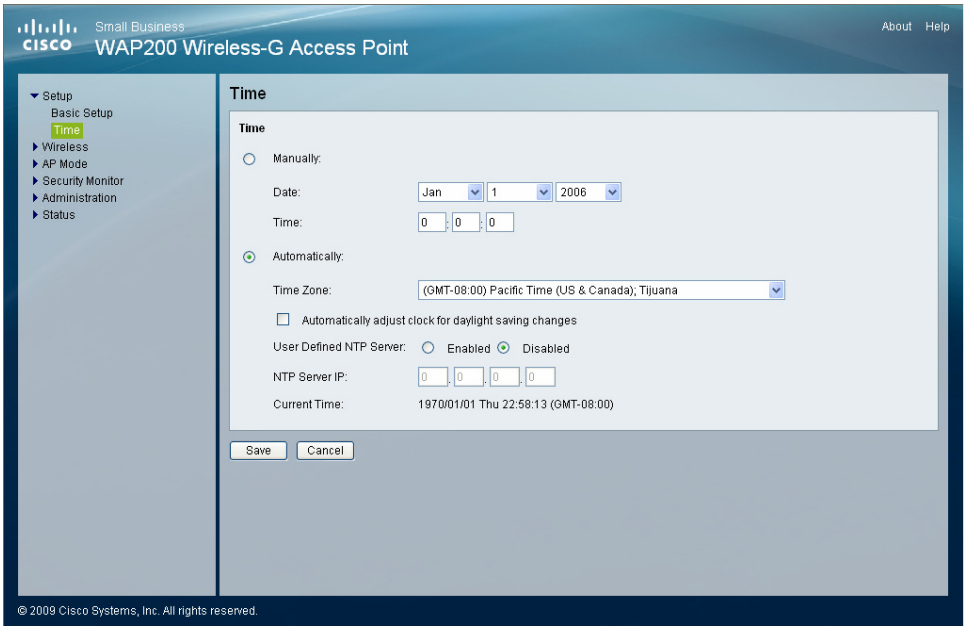
STEP 3 If you selected **Static IP Address**, enter the following information in the Network Setup section:

- **Local IP Address**—Enter the IP address of the access point. Make sure the address is not used by other devices on the network. The default is **192.168.1.245**.
- **Subnet Mask**—Enter the subnet mask of your network. The default is **255.255.255.0**.
- **Default Gateway**—Enter the default gateway address, typically the IP address of your router.
- **Primary DNS**—Enter the IP address of the Domain Name System (DNS) server. This address is typically provided by your Internet Service Provider (ISP).
- **Secondary DNS**—*Optional*. Enter a second DNS server.

STEP 4 Click **Save**.

Configuring Time Settings

The Setup > Time window displays the time settings of the access point. By setting up the correct time, you can help your network administrator accurately search the system log to identify problems.



To configure the time settings for the access point, follow these steps:

STEP 1 Click **Setup > Time**.

STEP 2 To manually configure the time settings:

a. Click **Manually**.

b. In the **Date** field, enter the current date.

c. In the **Time** field, enter the current time.

STEP 3 To automatically configure the time settings so that the access point obtains the time from a public time server:

a. Click **Automatically**.

b. Select a time zone from the **Time Zone** drop-down menu.

c. If you are using the access point in a location that observes daylight saving time, check the **Automatically adjust clock for daylight saving changes** check box.

d. To use a local NTP server, click **Enabled**. The default is **Disabled**.

In the NTP Server IP field, enter the IP address of your NTP Server.

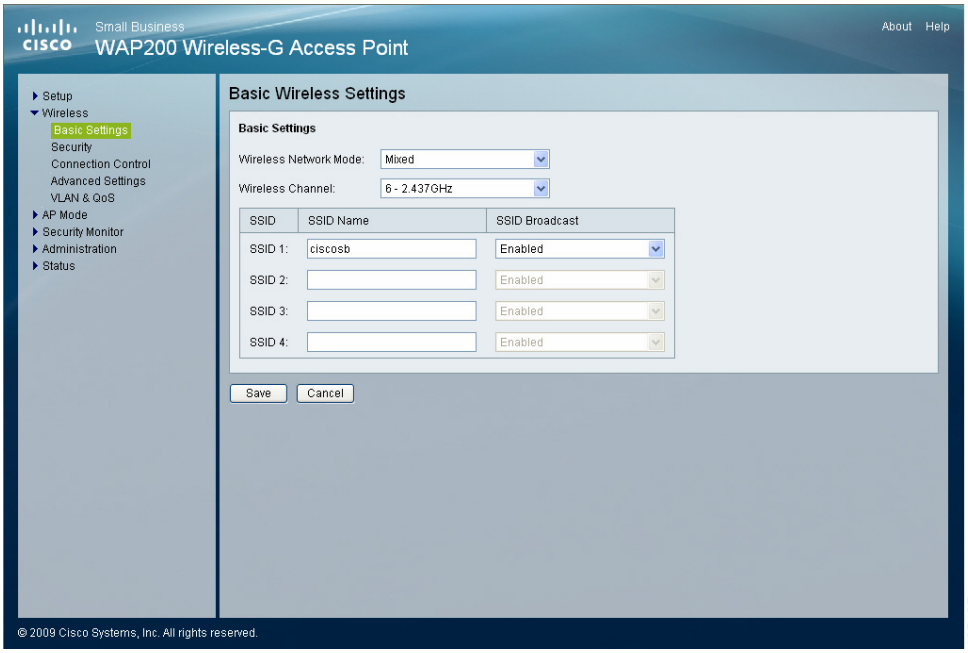
STEP 4 Click **Save**.

Configuring Wireless Settings

This section describes how to configure the wireless settings of the access point:

Configuring Basic Settings

The Wireless > Basic Settings window displays the basic wireless network settings of the access point. The access point can connect to up to four wireless networks (SSIDs) at the same time, so this window offers settings for up to four different SSIDs. Each SSID has its own MAC address on this access point.



To configure the Wireless Network basic attributes for the entire system and for each SSID, follow these steps:

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 From the **Wireless Network Mode** drop-down menu, select one of the following modes. The default is **Mixed**.

- **Disable**—Disables wireless connectivity completely. This mode can be useful during system maintenance.
- **B-Only**—Connects all the wireless client devices to the access point at Wireless-B data rates with maximum speed at 11 Mbps.

- **G-Only**—Connects Wireless-G client devices at Wireless-G data rates with maximum speed at 54 Mbps. Wireless-B clients cannot be connected in this mode.
- **Mixed**—Connects both Wireless-B and Wireless-G client devices at their respective data rates. Wireless-G devices can be connected at Wireless-G data rates.

STEP 3 From the **Wireless Channel** drop-down menu, select the appropriate channel to be used by your access point and your client devices.

Select **Auto** to have your access point select the channel with the lowest amount of wireless interference while the system is powering up. Auto channel selection starts when you click the **Save** button; it takes several seconds to scan through all the channels to find the best channel. The default setting is **Channel 6**.

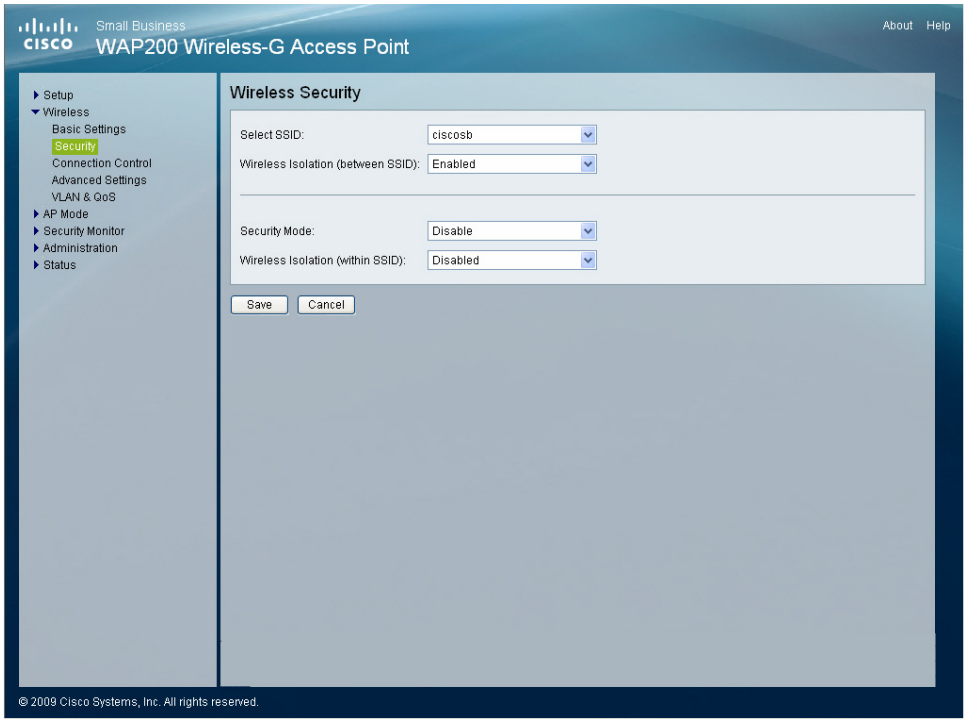
STEP 4 In the **SSID Name** and **SSID Broadcast** fields, enter the SSID, and select whether you want your access point to broadcast it, respectively.

- **SSID Name**—This field specifies the unique name to be 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 name is used for all devices in your wireless network. The default SSID name is **ciscosb**.
- **SSID Broadcast**—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. Select **Enabled** to broadcast the SSID to all wireless devices in range. Select **Disabled** to increase network security by preventing the SSID from being seen on networked computers. The default is **Enabled**.

STEP 5 Click **Save**.

Configuring Security

The Wireless > Security window displays the wireless security settings of the access point, including Wi-Fi Protected Access (WPA) and Remote Authentication Dial-In User Service (RADIUS). WPA is a stronger security standard than Wired Equivalent Privacy (WEP) encryption, and is forward-compatible with IEEE 802.11i. Enterprise modes use a RADIUS server for authentication.



To configure the wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security.**

STEP 2 Configure wireless isolation between SSIDs:

a. From the Select SSID drop-down menu, select any of the SSID names configured previously on the Basic Wireless Settings window.

b. To isolate wireless clients from each other, from the Wireless Isolation (between SSID) drop-down menu, select **Enabled**. Otherwise, select **Disabled**.

Wireless isolation between SSIDs prevents eavesdropping on the network. When it is enabled, wireless frames received on this access point are not forwarded to other wireless networks (SSIDs).

This feature is very useful when setting up a wireless hotspot location, for example, to keep its wireless network (SSID) isolated from your other wireless networks (SSIDs). This is a global option applying to all SSIDs. The default is **Enabled**.

STEP 3 To disable wireless security completely, from the Security Mode drop-down menu, select **Disabled**.

STEP 4 To enable wireless security, from the Security Mode drop-down menu, select one of the following security modes, and enter the information needed for that particular mode, as described in one of the following sections:

- **Configuring WPA-Personal, page 29**
- **Configuring WPA2-Personal, page 30**
- **Configuring WPA2-Personal Mixed, page 31**
- **Configuring WPA-Enterprise, page 33**
- **Configuring WPA2-Enterprise, page 35**
- **Configuring WPA2-Enterprise Mixed, page 37**
- **Configuring RADIUS, page 39**
- **Configuring WEP, page 41**

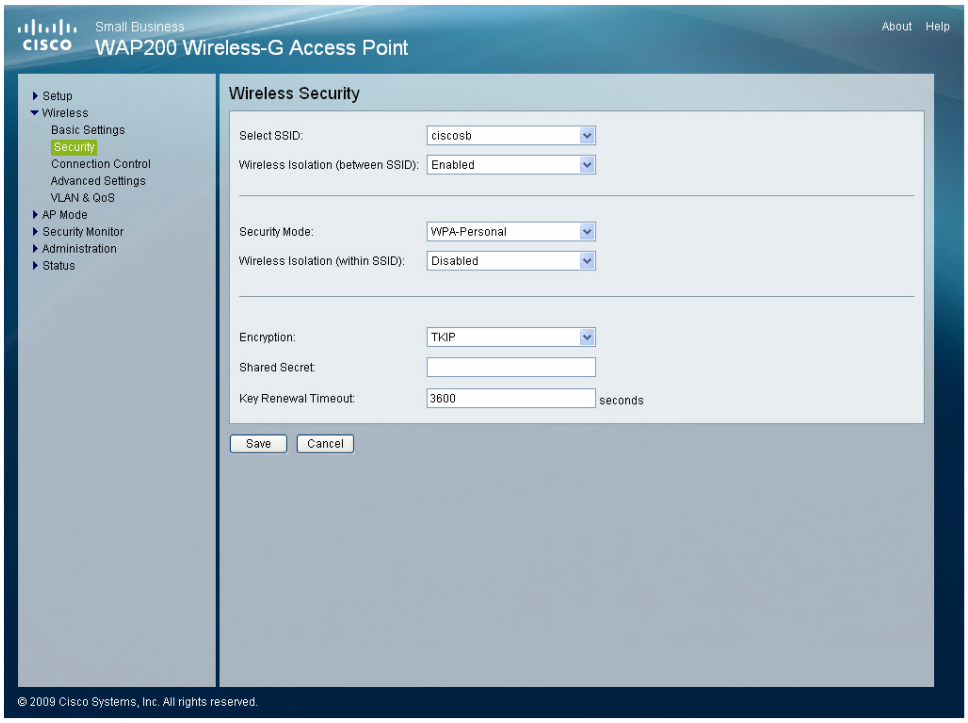
STEP 5 To prevent wireless computers associated to the same SSID from seeing each other and transferring files between each other, from the **Wireless Isolation (within SSID)** drop-down menu, select **Enabled**.

The default is **Disabled** which allows visibility and the exchanging of files between wireless computers associated with the same SSID.

STEP 6 Click **Save**.

Configuring WPA-Personal

WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11i.



To configure the WPA-Personal (also known as WPA-PSK) wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security.**

STEP 2 From the Security Mode drop-down menu, select **WPA-Personal.**

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled.**

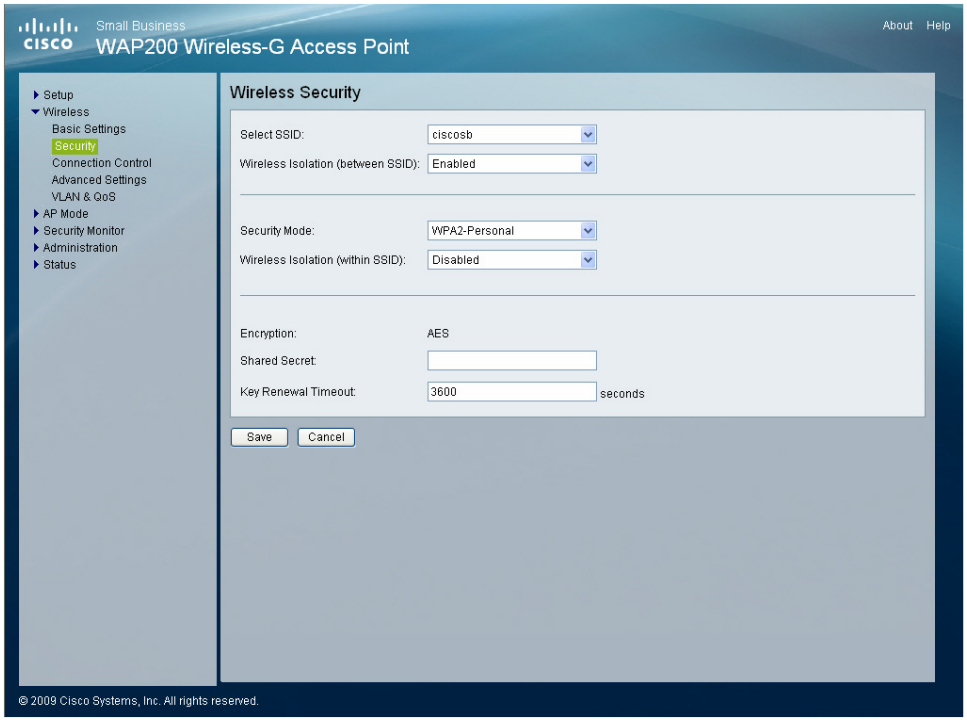
STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled.**

STEP 5 Provide the following information:

- **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.

STEP 6 Click **Save**.

Configuring WPA2-Personal



To configure the WPA2-Personal wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **WPA2-Personal**.

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

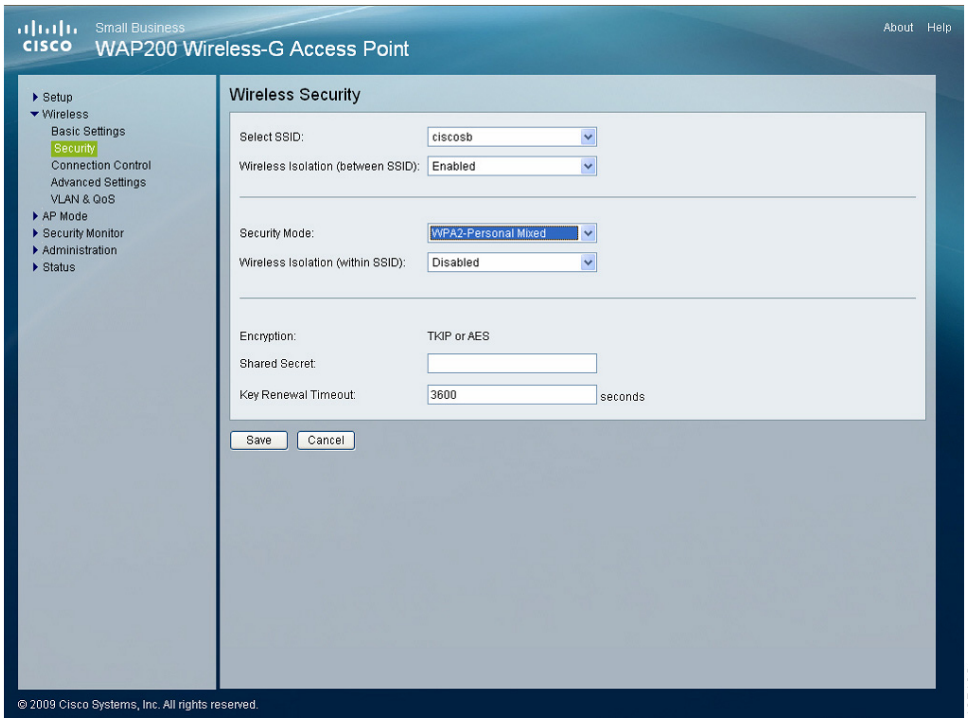
STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 5 Provide the following information:

- **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.

STEP 6 Click **Save**.

Configuring 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 automatically chooses the encryption algorithm used by each client device.

To configure the WPA2-Personal Mixed wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **WPA2-Personal Mixed**.

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 5 Provide the following information:

- **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.

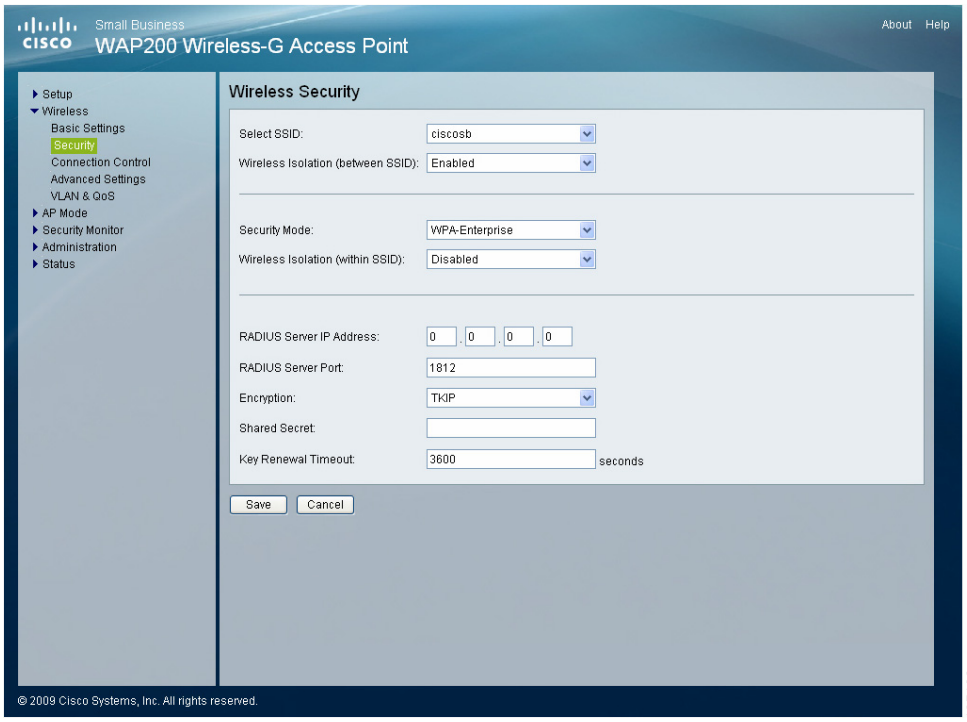
STEP 6 Click **Save**.

Configuring WPA-Enterprise

This option features WPA used in coordination with a Remote Authentication Dial-In User Service (RADIUS) server for client authentication.

Enterprise modes use a RADIUS server for authentication.

NOTE Use WPA-Enterprise only when a RADIUS server is connected to the access point.



To configure the WPA-Enterprise wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **WPA-Enterprise**.

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 5 Provide the following information:

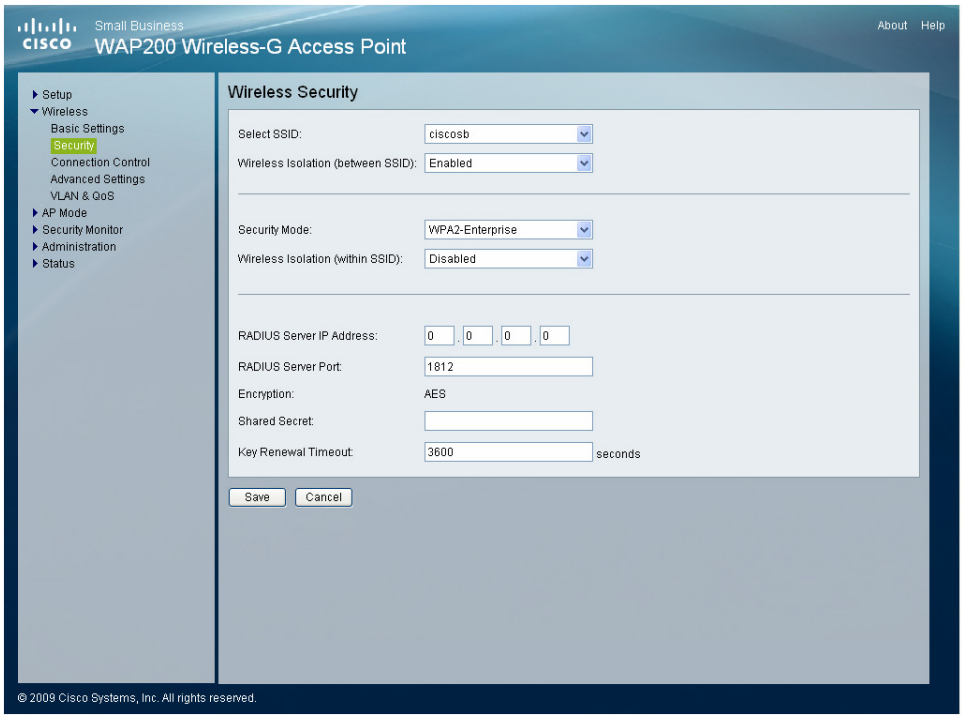
- **RADIUS Server IP Address**—Enter the RADIUS server's IP address.
- **RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is **1812**.
- **Encryption**—WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **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.

STEP 6 Click **Save**.

Configuring WPA2-Enterprise

This option features WPA2 used in coordination with a RADIUS server for client authentication.

NOTE Use WPA2-Enterprise only when a RADIUS server is connected to the access point.



To configure the WPA2-Enterprise wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **WPA2-Enterprise**.

STEP 3 To enable wireless isolation **across SSIDs** select **Enabled** from the drop-down menu. Otherwise select **Disabled**.

STEP 4 To enable wireless isolation **within SSID**, select **Enabled** from the drop-down menu. Otherwise select **Disabled**.

STEP 5 Provide the following information:

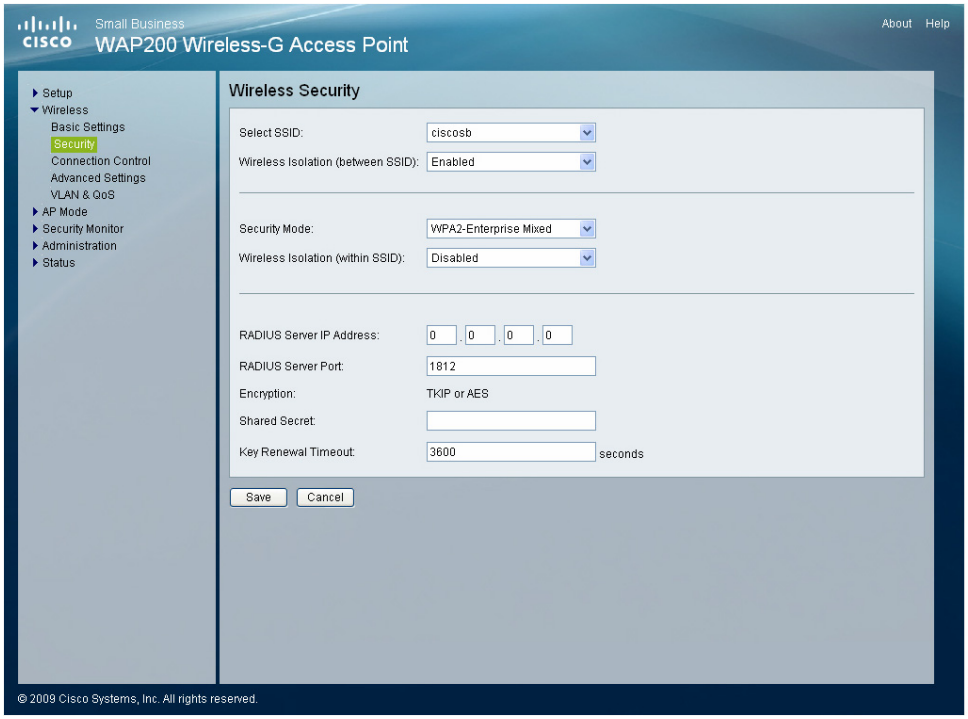
- **RADIUS Server IP Address**—Enter the RADIUS server's IP address.
- **RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is **1812**.
- **Encryption**—WPA2 always uses **AES** for data encryption.
- **Shared Secret**—Enter the shared secret key used by the access point 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.

STEP 6 Click **Save**.

Configuring 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 automatically chooses the encryption algorithm used by each client device.



To configure the WPA2-Enterprise Mixed wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **WPA2-Enterprise Mixed**.

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 5 Provide the following information:

- **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.

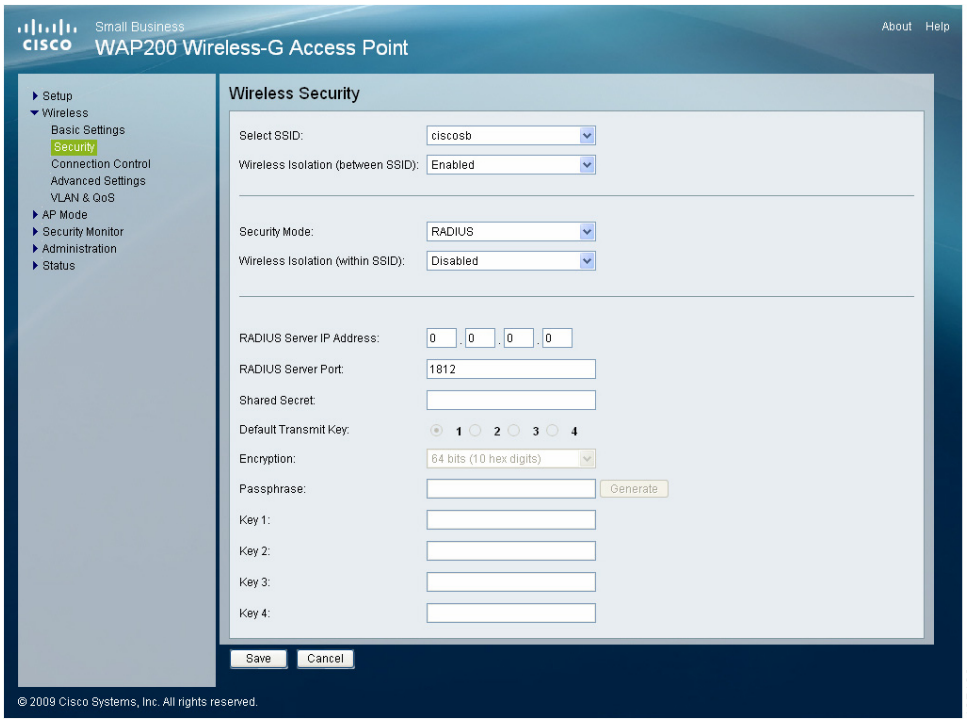
STEP 6 Click **Save**.

Configuring 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.

NOTE Manual WEP key is no longer supported to ensure compatibility with Microsoft's Windows implementation.



To configure the RADIUS wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security**.

STEP 2 From the Security Mode drop-down menu, select **RADIUS**.

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled**.

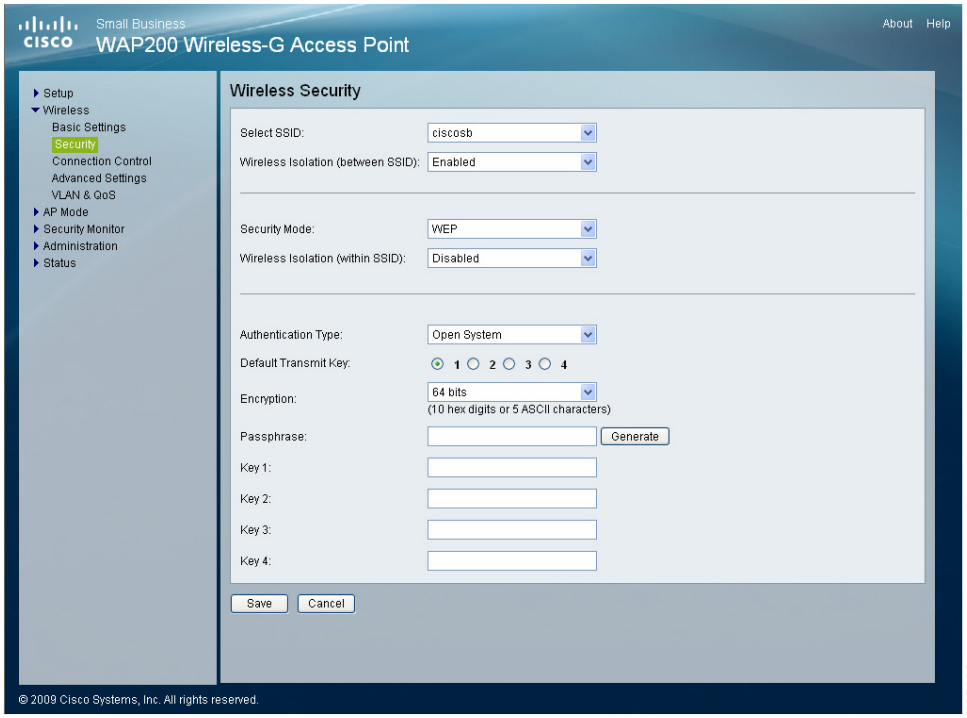
STEP 5 Provide the following information:

- **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.

STEP 6 Click **Save**.

Configuring WEP

CAUTION For improved security, migrate to WPA or WPA2. The Wired Equivalent Privacy (WEP) security mode is not recommended any more, due to its weak security protection. It was defined in the original IEEE 802.11.



To configure the WEP wireless security settings for the access point, follow these steps:

STEP 1 Click **Wireless > Security.**

STEP 2 From the Security Mode drop-down menu, select **WEP.**

STEP 3 To enable wireless isolation across SSIDs, select **Enabled** from the drop-down menu. Otherwise, select **Disabled.**

STEP 4 To enable wireless isolation within SSID, select **Enabled** from the drop-down menu. Otherwise, select **Disabled.**

STEP 5 Provide the following information:

- **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 **Generate**. The 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." A WEP key should be 10 characters long for 64-bit encryption or 26 characters long for 128-bit encryption.

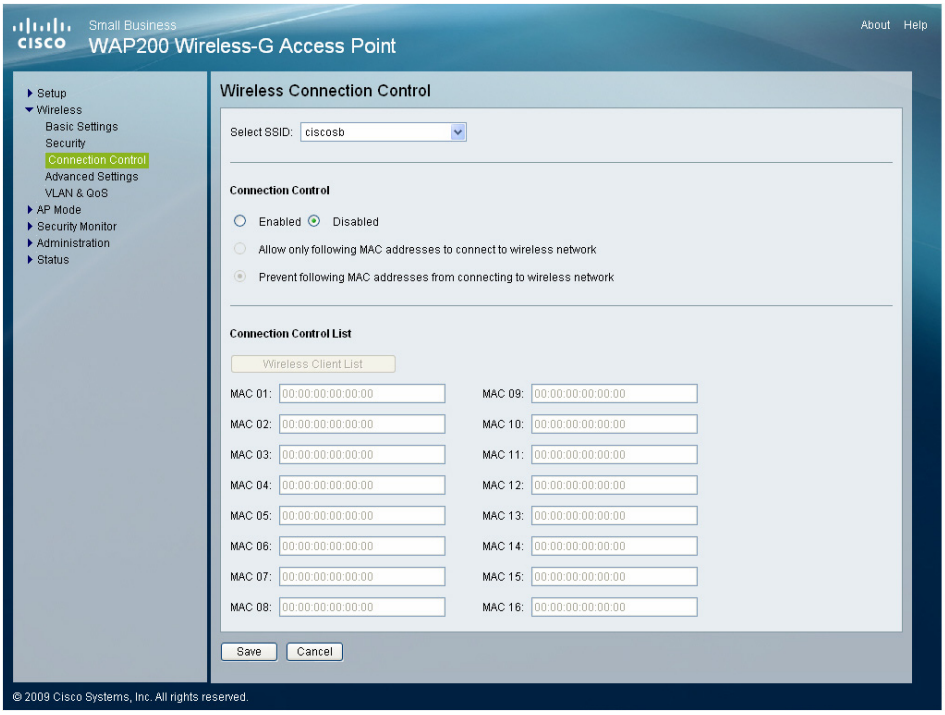
STEP 6 Click **Save**.

Configuring Connection Control

The Wireless > Connection Control window displays the wireless connection settings, and allows you to configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the access point.

Disabling Wireless Connection Control

You can use the Wireless Connection Control window to disable wireless connection control.



To disable wireless connection control for your access point, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 From the Select SSID drop-down menu, select the SSID of the wireless network that you want to disable.

STEP 3 In the connection control section, click **Disabled** (default).

STEP 4 Click **Save**.

Allowing Specified MAC Addresses to Connect to the Wireless Network

To allow only specific MAC addresses to connect to the wireless network, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 In the **Select SSID** drop-down menu, select the SSID of the wireless network on which you want to allow the specified MAC addresses.

STEP 3 In the connection control section, click **Enabled** (default).

STEP 4 Click **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.

STEP 5 To automatically capture the MAC addresses of each client to allow, click **Wireless Client List**.

A window appears to let you select each MAC address from the table. The selected MAC address is copied into the Connection Control List.

Alternatively, manually enter the MAC addresses of the wireless client devices you want to allow, in the text boxes labeled MAC 01–16.

STEP 6 Click **Save**.

Preventing MAC Addresses from Connecting to the Wireless Network

To allow only specific MAC addresses to connect to the wireless network, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 In the **Select SSID** drop-down menu, select the SSID of the wireless network on which you want to block the specified MAC addresses.

STEP 3 In the connection control section, click **Enabled** (default).

STEP 4 Click **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 is not allowed to connect to the access point.

STEP 5 To automatically capture the MAC addresses of each client to block, click **Wireless Client List**.

A window appears to let you select each MAC address from the table. The selected MAC address is copied into the Connection Control List.

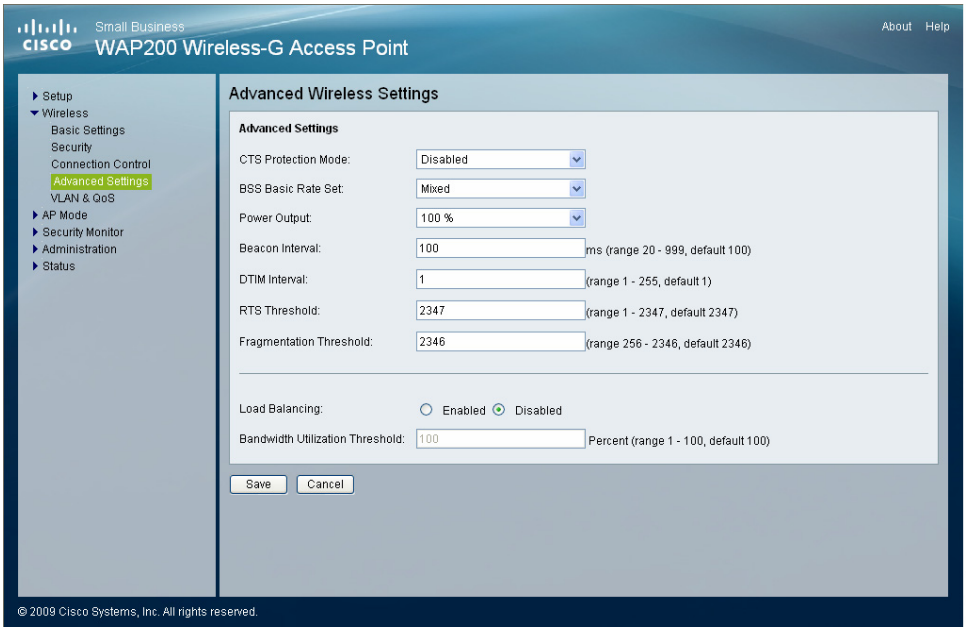
Alternatively, manually enter the MAC addresses of the wireless client devices you want to disallow, in the text boxes labeled MAC 01-16.

STEP 6 Click **Save**.

Configuring Advanced Settings

This Wireless > Advanced Settings window allows you to configure the advanced settings for the access point.

We recommend to let your access point automatically adjust the parameters for maximum data throughput.



To configure the wireless advanced settings for the access point, follow these steps:

STEP 1 Click **Wireless > Advanced Settings**.

STEP 2 In the Advanced Settings section, configure the following advanced parameters:

- **CTS Protection Mode**—The Clear-To-Send (CTS) Protection Mode function boosts the access point's ability to catch all wireless transmissions but severely reduces 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** to permanently disable this mode.

- **BSSBasicRateSet**—This setting provides 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 setting (**Mixed mode**) 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, configure the transmission rate through the Tx Rate Limiting field in the **Wireless > VLAN & QoS** window.

- **Power Output**—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 about 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 information regarding 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 computer from dropping into

power-saving sleep mode. Higher settings allow your computer to enter sleep mode, thus saving power, but interferes with wireless transmissions. The default is **1 ms**.

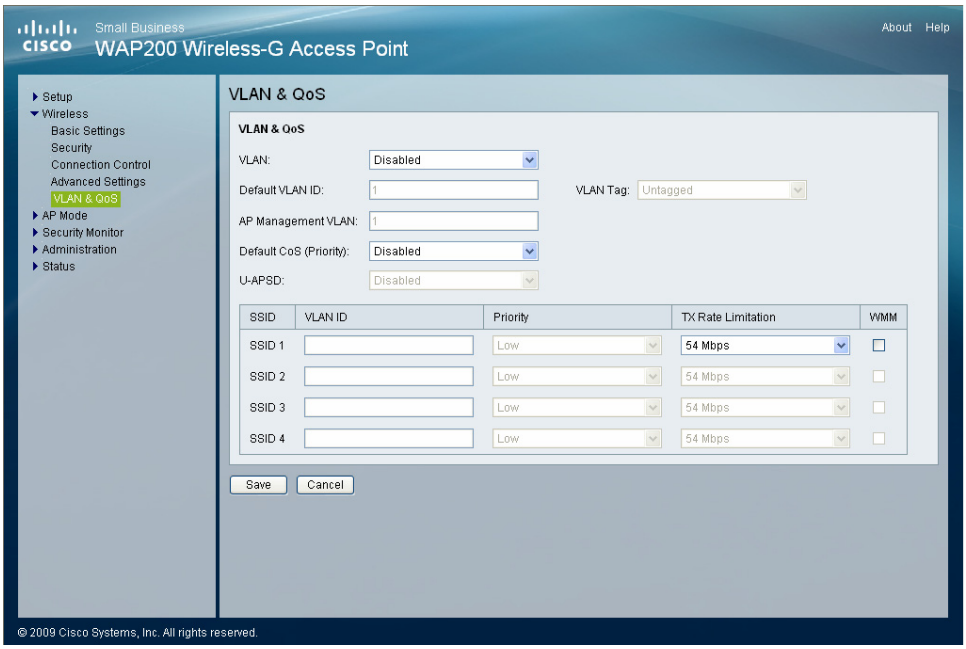
- **RTS Threshold**—This setting determines how large a packet can be before the access point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.
- **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 creates more packets for each transmission. If you experience high packet error rates, you can decrease this value, but it likely decreases overall network performance. Only minor modifications of this value are recommended.

STEP 3 Click **Save**.

Configuring VLAN & QoS

The Wireless > VLAN & QoS window allows you to configure the VLAN and QoS related settings for the access point.



To configure the wireless VLAN and QoS settings of the access point, follow these steps:

STEP 1 Click **Wireless > VLAN & QoS**.

STEP 2 Configure VLAN settings by providing the following information for the global VLAN settings for the access point:

- **VLAN**—Select **Enabled** to pass 802.1q VLAN tagged traffic between the wired LAN and wireless LAN. Your access point maps the VLAN tag (wired side) to different SSIDs (wireless side) according to your specified settings. Select **Disabled** and your access point drops 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 Cisco SRW2024 switch has the Trunk port mode, which sets the default VLAN (PVID) to 1 untagged, while the 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 the web-based utility. To access the web-based utility from the wireless side, the SSID needs to map to the same VLAN ID. Remember to enable wireless web access in the Administration > Management window.
- **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 does not carry VLAN information. Multiple SSIDs can map to the same VLAN on the wired side.

NOTE To use wireless security which requires RADIUS server (802.1X) authentication, make the VLAN ID the same as the AP management VLAN ID. This restriction in will be removed in a future releases.

STEP 3 Configure QoS settings by providing the following information for the VLAN global settings for the access point:

- **Default CoS (Priority)**—Select **Enabled** 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**—This option is only available when Wi-Fi Multimedia (WMM) is enabled on any of the SSIDs. Select **Enabled** to have client devices with Unscheduled Automatic Power Save Delivery (U-APSD) capability take advantage of the power save mode. The default is **Disabled**.
- **SSID Name**—Displays the SSIDs defined in the Basic Wireless Settings window (Wireless > Basic Settings). If an SSID has been disabled, the options cannot be configured.
- **VLAN ID**—Select a VLAN ID (**1–4094**) for the SSID for where you want to map the traffic to, on the wired side. The wireless traffic does not carry VLAN information. Multiple SSIDs can map to the same VLAN on the wired side.
- **Priority**—To assign the default priority (802.1p CoS bits) for packets coming in from each wireless network, select a value from the drop-down menu. The default is **Low**.

- **Tx Rate Limitation**—Limits 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 the Mixed or G-Only wireless mode and **11 Mbps** for the 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).

STEP 4 Click **Save**.

Configuring the Access Point's Modes of Operation

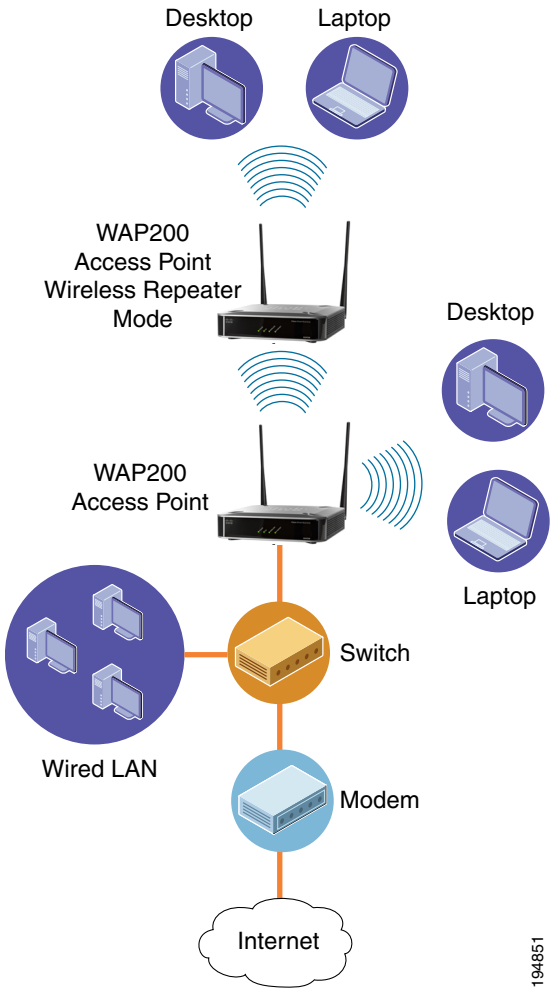
The AP Mode > AP Mode window displays the access point mode settings for the access point.

The access point offers three mutually exclusive modes of operation:

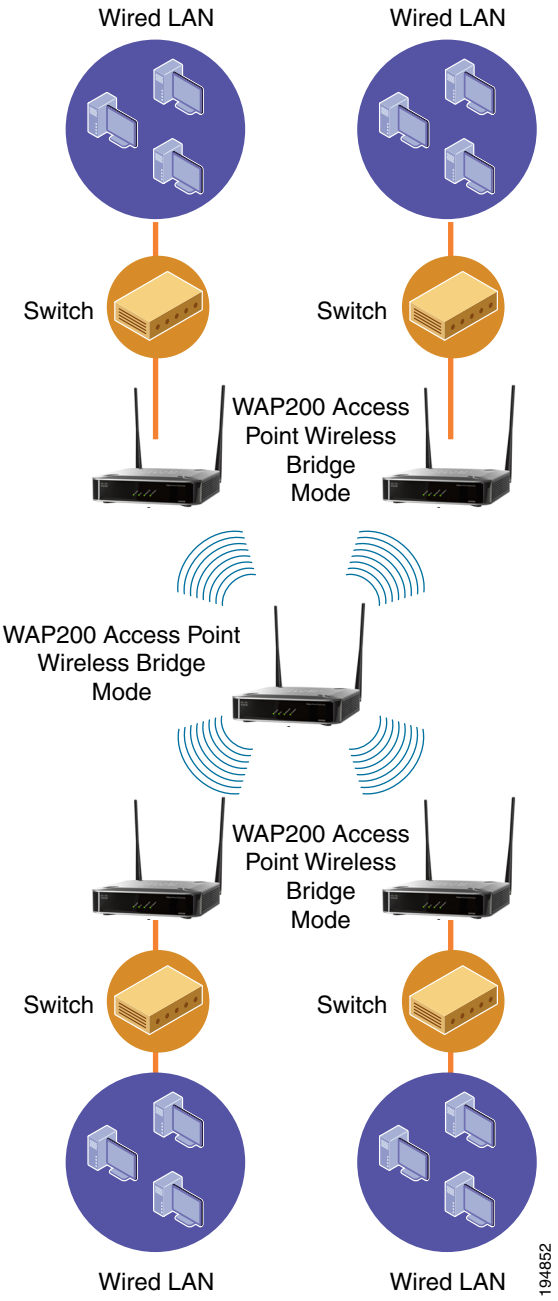
- Access Point (default)—Connects your wireless computers to a wired network. In most cases, no change is necessary when choosing this mode.
- Wireless Repeater—Allows you to communicate with, and re-transmit the signal of another remote wireless access point device if this access point is within its range.
- Wireless Bridge—Wirelessly connects your wired network to other physically separate wired networks having their own access points similarly configured as wireless bridges. Wireless clients cannot connect to the access point in this mode.

The access point's mode is set to **Access Point** by default. This connects your wireless devices to a wired network. In most cases, no change is necessary.

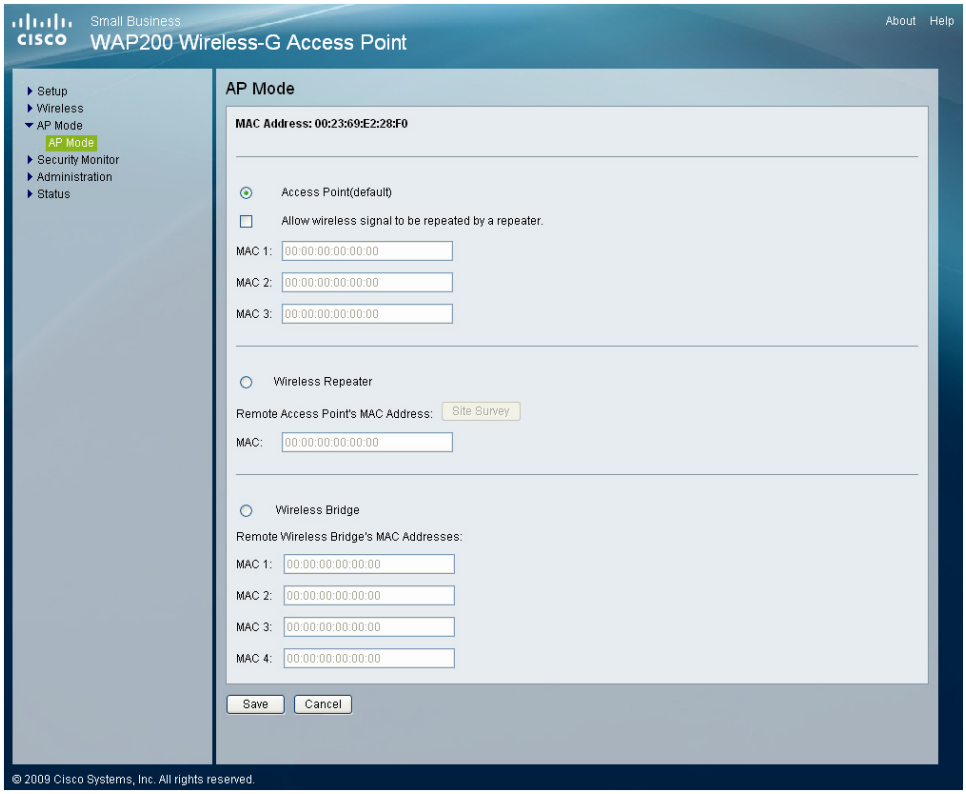
You may wish to change the access point's mode of operation if you want to use the access point as a wireless repeater to extend the range of your wireless network. When set to the **Wireless Repeater** mode, the wireless repeater is able to talk to a remote access point within its range and retransmit its signal.



You may alternately 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 the **Wireless Bridge** mode to connect two wired networks that are in two different buildings.



For the Wireless Repeater and Wireless Bridge modes, the Wireless Network mode, Channel, and Security settings must be the same for other remote wireless access points and devices.



To configure the access point mode settings of the access point, follow these steps:

STEP 1 Click **AP Mode > AP Mode**.

The MAC address of the access point is displayed below the window's title.

STEP 2 To configure the access point for operation as an access point, click **Access Point** (default), if it is not already selected. This connects your wireless computers to a wired network. In most cases, no change is necessary. Provide the following information:

- **Allow wireless signal to be repeated by a repeater**—Check this option to use another wireless device to repeat the signal of this access point.
- **MAC1** to **MAC3**—Enter the MAC addresses of up to three wireless devices that should act as the repeaters. You can use up to 3 repeaters.

STEP 3 To configure the access point for operation as a wireless repeater, click **Wireless Repeater** and fill in the following information:

- **Remote Access Point's MAC Address**—Click **Site Survey** to select the access point that has its signal repeated by this access point or enter the MAC address of the access points manually in the MAC field.

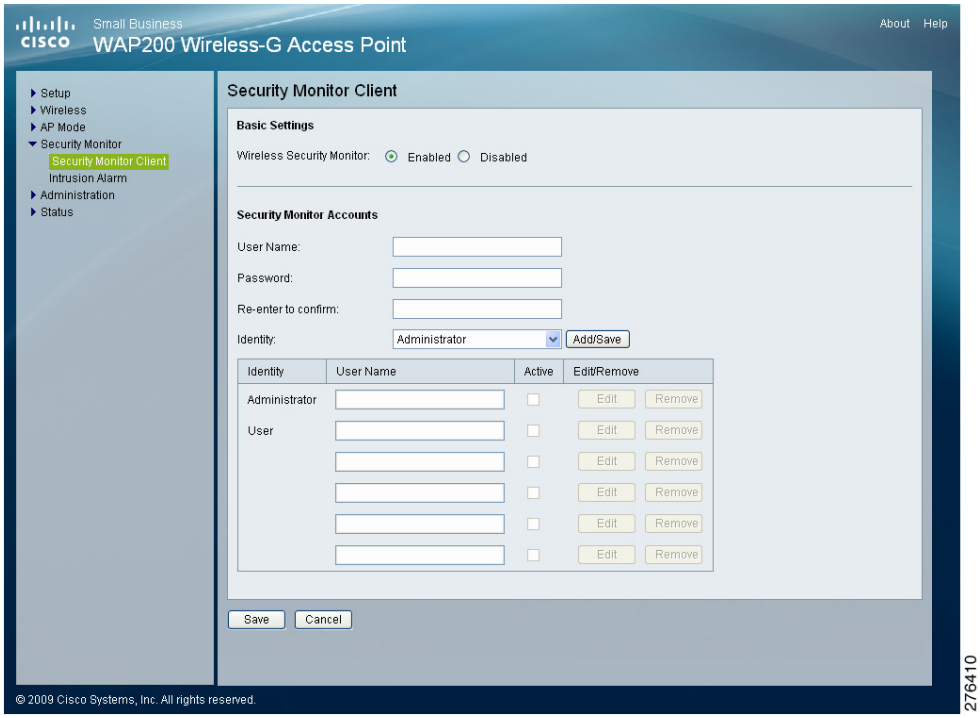
STEP 4 To configure the access point for operation as a wireless bridge, click **Wireless Bridge** and fill in the following information:

- **Remote Wireless Bridge's MAC Addresses**—Enter the MAC addresses of the access points that bridge to this access point in the fields below.

STEP 5 Click **Save**.

Configuring Security Monitor Settings

This section describes how to configure the security monitor settings of the access point:



Configuring the Security Monitor Client Settings

The Security Monitor > Security Monitor Client window displays the access point's security monitor client account settings.

Disabling the Wireless Security Monitor

You can use the Security Monitor Client Settings window to disable the wireless security monitor. If you do not plan to use client utility to actively monitor your network, disable the wireless security monitor feature to improve your wireless network performance. The default is **Disabled**.

To disable the wireless security monitor for your access point, follow these steps:

STEP 1 Click **Security Monitor > Security Monitor Client**.

STEP 2 In the Basic Settings section, click **Disabled** (default) if it is not already disabled.

STEP 3 Click **Save**.

Creating Security Monitor Accounts

The Security Monitor Accounts section of the Security Monitor Client window allows you to create accounts to monitor wireless security. You can create one account at a time. The administrator then uses his client utility to log in and be authenticated by the system, after user accounts are created.

To create security accounts to monitor wireless security for the access point, follow these steps:

STEP 1 Click **Security Monitor > Security Monitor Client**.

STEP 2 In the Basic Settings section, click **Enabled**.

STEP 3 Create one Administrator security account and up to five User security accounts by providing the following information for each:

- Enter the user name and password for this account
- Re-enter the password to re-confirm.
- Select the Identity for this account from the drop-down menu.

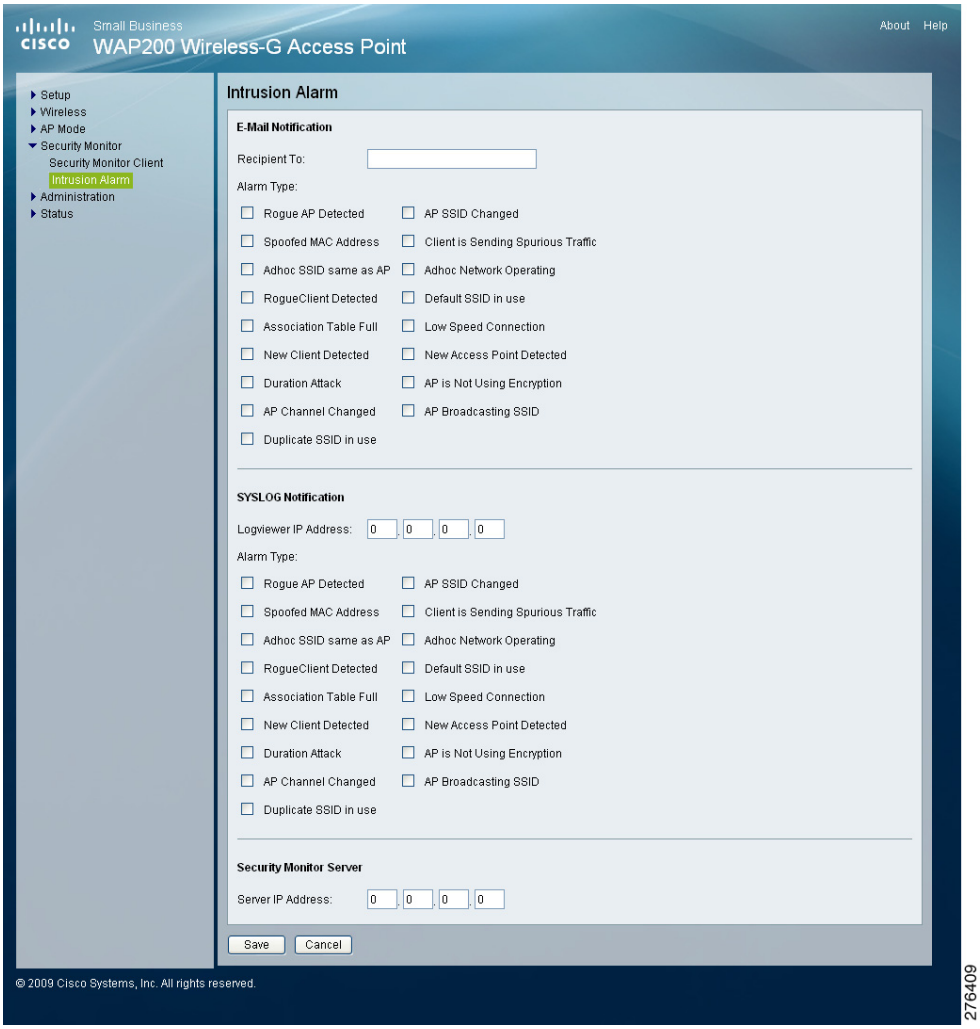
STEP 4 Click **Add/Save** to save the account created. The account created is added to the table.

STEP 5 Correct any errors in the accounts created, by clicking the **Edit** or **Remove** button as appropriate, in the table.

STEP 6 Click **Save**.

Configuring Intrusion Alarm Event Log Settings

The Security Monitor > Intrusion Alarm window displays the access point's security monitor intrusion alarm event logging / notification settings for E-mail Notification and SYSLOG Notification.



Configuring E-mail Notification Settings

To configure e-mail notification settings for the access point, follow these steps:

STEP 1 Click **Security Monitor > Intrusion Alarm**.

STEP 2 Enter the e-mail address of Recipient to whom the alarm notifications are sent.

STEP 3 Select the types of intrusion that will be notified in the e-mail:

- **Rogue AP Detected**— A rogue access point has been detected.
- **AP SSID Changed**—The Access Point (AP) SSID has been changed.
- **Spoofed MAC Address**—Another device is using the AP MAC address to send out packets.
- **Client is Sending Spurious Traffic**—An unassociated client is sending out frames to the AP.
- **Adhoc SSID same as AP**—An Adhoc network uses the same SSID as the AP.
- **Adhoc Network Operating**—An STA is advertising a peer-to-peer (Adhoc) network.
- **Rogue Client Detected**—An STA is conducting an illegal transaction with an AP.
- **Default SSID in use**—Default SSID is in use on an AP.
- **Association Table Full**—An AP refused a new STA association due to resource unavailability.
- **Low Speed Connection**—An STA is transmitting data at a much slower rate set by AP.
- **New Client Detected**—A new STA is associated with an AP.
- **New Access Point Detected**—A new AP has been detected joining the network.
- **Duration Attack**—A STA packet contains an abnormally large duration value in the 802.11 header.
- **AP is Not Using Encryption**—An AP has wireless security disabled.
- **AP Channel Changed**—An AP has changed its wireless channel.
- **AP Broadcasting SSID**—SSID broadcasting is left enabled on an AP.
- **Duplicate SSID in use**—An unauthorized AP has the same SSID value as an authorized AP.

STEP 4 Click **Save**.

Configuring SYSLOG Notification Settings

To configure SYSLOG Notification settings for the access point, follow these steps:

STEP 1 Click **Security Monitor > Intrusion Alarm**.

STEP 2 Enter the IP address of the system that will store the system log (Logviewer).

STEP 3 Select the e-mail notification alarm type to respond to intrusions. For a list of e-mail alarm types, see **Step 3 on page 58**.

STEP 4 In the Security Monitor Server section, enter the IP address for the Security Monitor Server, a special Syslog server that can record all security monitor events instead of only selected events.

STEP 5 Click **Save**.

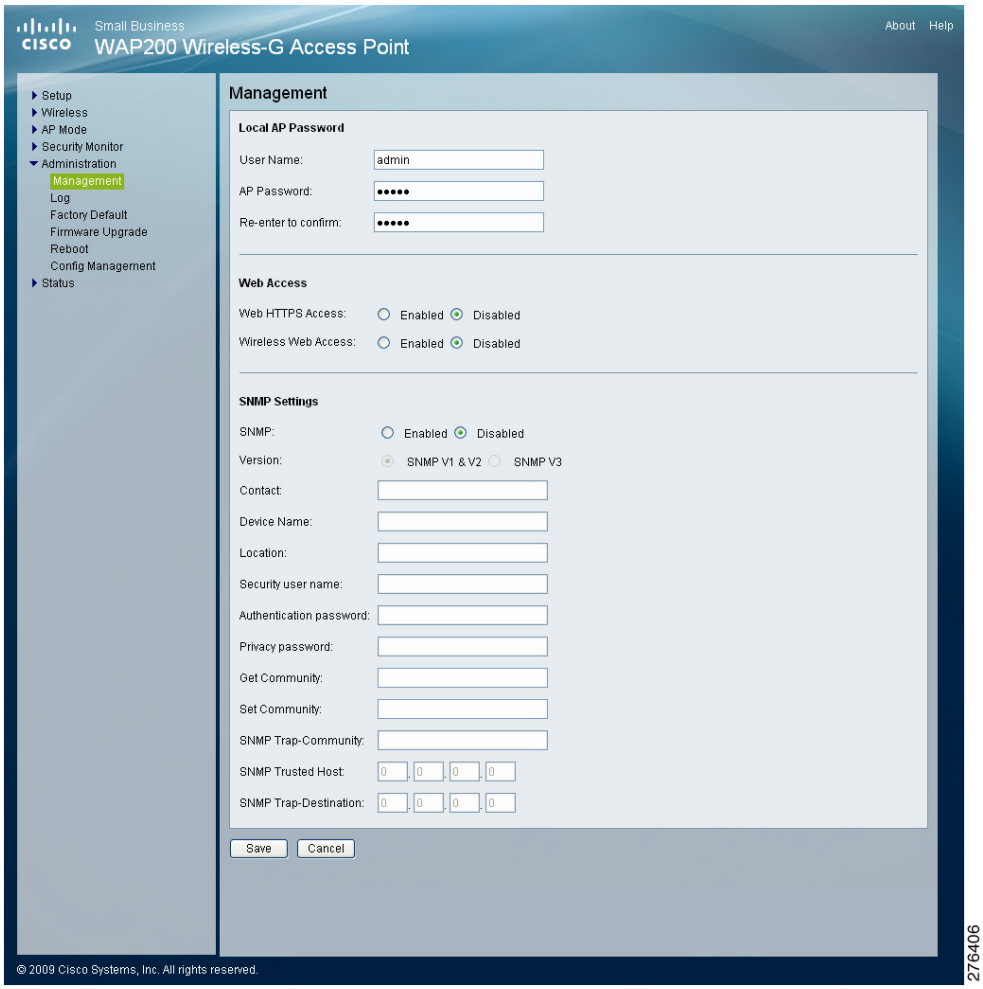
Configuring Administration Settings

This section describes how to configure the administration settings of the access point:

Configuring Management Settings

The Administration > Management window allows you to configure the password, web access, and Simple Network Management Protocol (SNMP) settings.

You should frequently change the username/password that controls access to the access point's web-based utility to prevent unauthorized access.



To change the management settings of the access point, follow these steps:

STEP 1 Click **Administration > Management**.

STEP 2 Configure the management settings:

- 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**—Confirm the new password by entering it again in this field.
- **Web Access**—Enable HTTPS to increase the security on accessing the web-based utility. Once enabled, users must use https:// when accessing the web-based utility.
  - **Web HTTPS Access**—Use secured HTTP session to access the web-based configuration utility. The default is **Disabled**.
  - **Wireless Web Access**—Allow or deny wireless clients access to the web-based configuration utility. The default is **Disabled**.
- SNMP settings
  - **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.

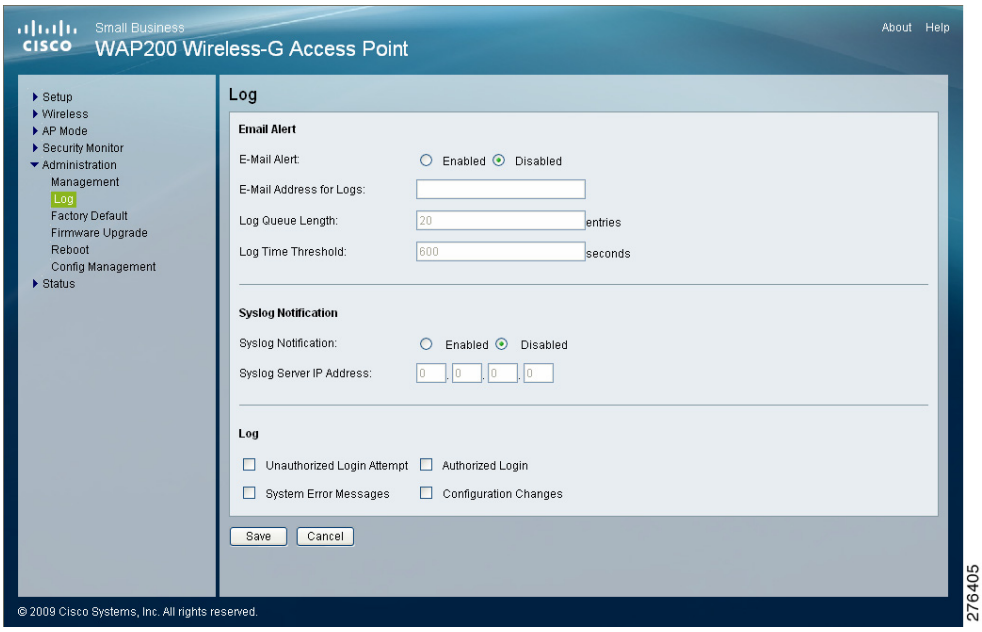
    To enable the SNMP support feature, click **Enabled**, and **SNMP V1 & V2** or **SNMP V3**, selecting the SNMP version. Otherwise, click **Disabled**. The default is **Disabled**.
  - **Contact**—Enter the name of the contact person for the access point.
  - **Device Name**—Enter the name you wish to give to the access point.
  - **Location**—Enter the location of the access point.
  - **(SNMP v3 only) Security User Name**—Enter the name you wish to give an administrator account to access and manage SNMP MIB objects.
  - **(SNMP v3 only) Authentication Password**—Enter the authentication password for the administrator account. Minimum password length is 8 characters.

- **(SNMP v3 only) Privacy Password**—Enter the privacy password for data encryption to monitor administrator traffic. Minimum password length is 8 characters.
- **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 receives trap messages or notices sent by the access point.
- **SNMP Trusted Host**—Enter the IP address of the host trusted with accessing the access point's SNMP information. If this field is set to 0.0.0.0, then access point will response to SNMP message from every host within the LAN.
- **SNMP Trap-Destination**—Enter the IP address of the remote host computer that receives the trap messages.

STEP 3 Click **Save**.

Configuring the Administration Log

The Administration > Log window configures the log settings and provides alerts for particular events.



To configure the log settings of the access point, follow these steps:

STEP 1 Click **Administration > Log**.

STEP 2 Configure the log settings:

- 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 receives logs.
  - **Log Queue Length**—Enter the length of the log that is e-mailed to you. The default is **20** entries.
  - **Log Time Threshold**—Specify how often the log is emailed to you. The default is **600** seconds (10 minutes).

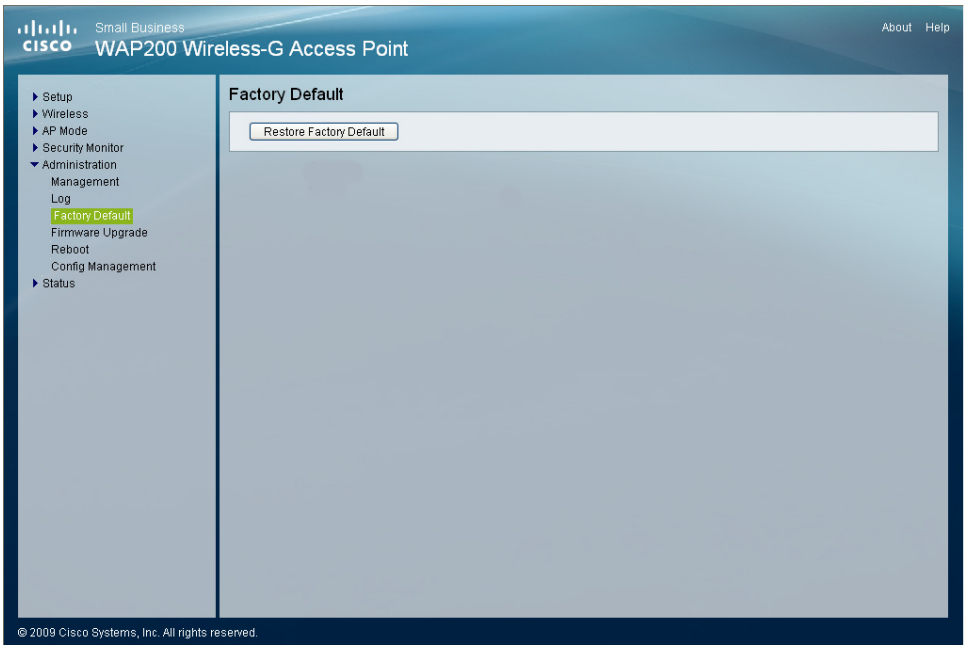
- Syslog Notification
  - **Syslog Notification**—Syslog is a standard protocol used to capture information about network activity. The access point supports this protocol and sends its activity logs to an external server. To enable Syslog, select **Enabled**. The default is **Disabled**.
  - **Syslog 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 log.
  - **Unauthorized Login Attempt**—If you want to receive alert logs about any unauthorized login attempts, click this check box.
  - **Authorized Login**—If you want to log authorized logins, click this check box.
  - **System Error Messages**—If you want to log system error messages, click this check box.
  - **Configuration Changes**—If you want to log any configuration changes, click this check box.

STEP 3 Click **Save**.

Restoring Factory Default Settings

The Administration > Factory Default window allows you to restore the access point's factory default settings.



CAUTION Restoring the factory default settings deletes all your custom settings. To preserve your custom settings, save them to disk before restoring the factory default settings, as described in **"Managing the Access Point's Configuration" on page 68**.

To restore the factory default settings of the access point, follow these steps:

STEP 1 Click **Administration > Factory Default**.

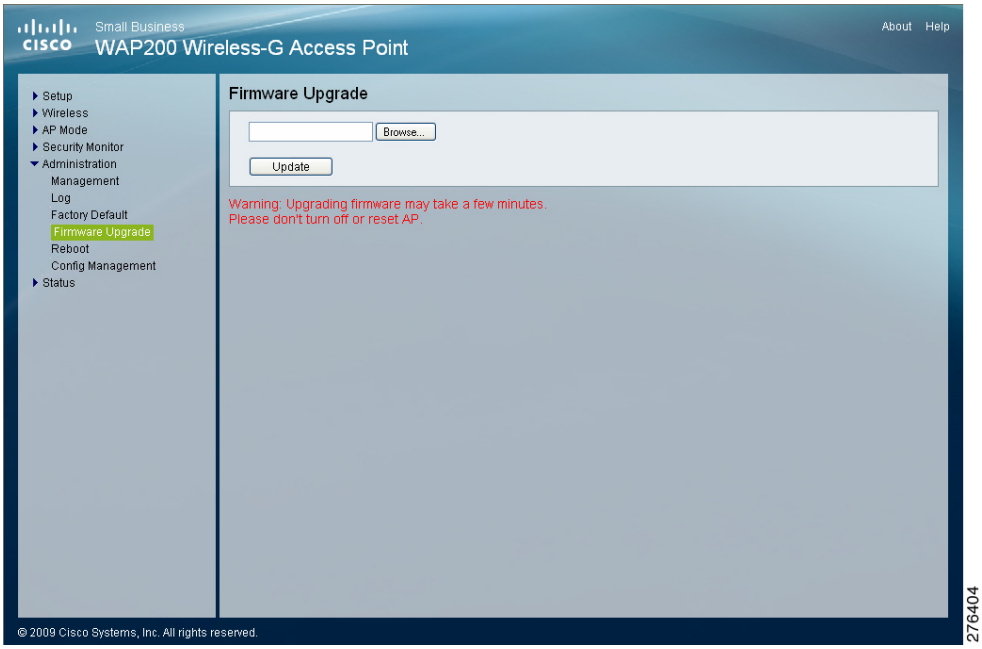
STEP 2 Click **Restore Factory Default**.

Your access point reboots and comes back up with the factory default settings in a few seconds.

Upgrading the Firmware

The Administration > Firmware Upgrade window allows you to upgrade the access point's firmware.

CAUTION Do not upgrade the firmware unless you are experiencing problems with the access point or the new firmware has a feature you want to use. Upgrading the firmware deletes all custom settings. To preserve your custom settings, save them to disk before upgrading the firmware, as described in **"Managing the Access Point's Configuration," on page 68**.



To upgrade the firmware of the access point, follow these steps:

STEP 1 Upgrade the firmware of the access point.

a. Download the firmware upgrade file from www.cisco.com/en/US/products/ps10048/index.html.

b. Extract the firmware upgrade file and save it on your computer.

c. Click **Administration > Firmware Upgrade**.

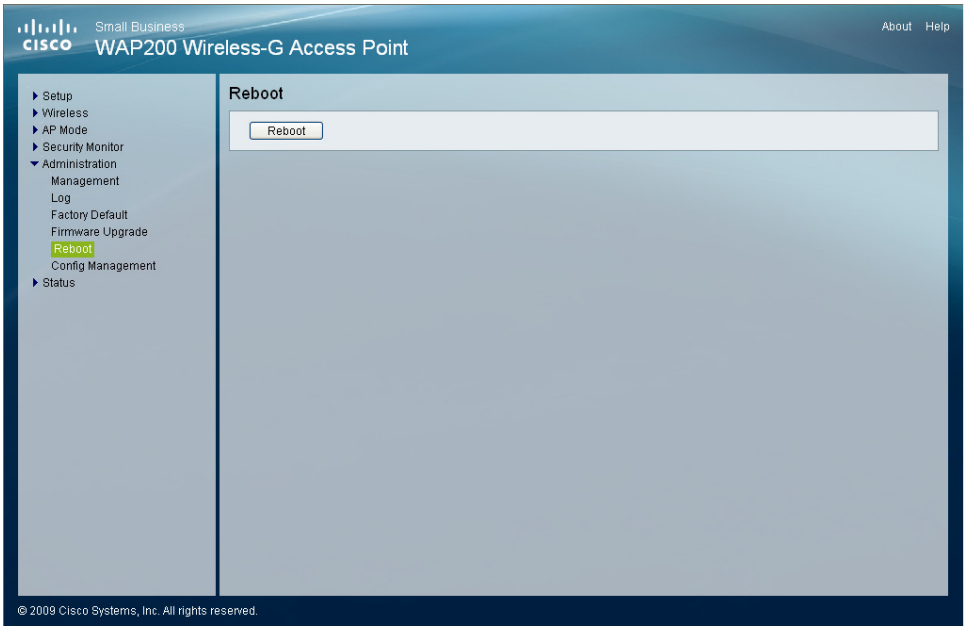
d. Enter the location of the firmware upgrade file in the field provided or click **Browse** to locate the file.

e. Click **Upgrade** and follow the on-screen instructions.

STEP 2 Restore your custom settings as described in **"Managing the Access Point's Configuration," on page 68**.

Rebooting the Access Point

The Administration > Reboot window allows you to reboot the access point.



To reboot the access point, follow these steps:

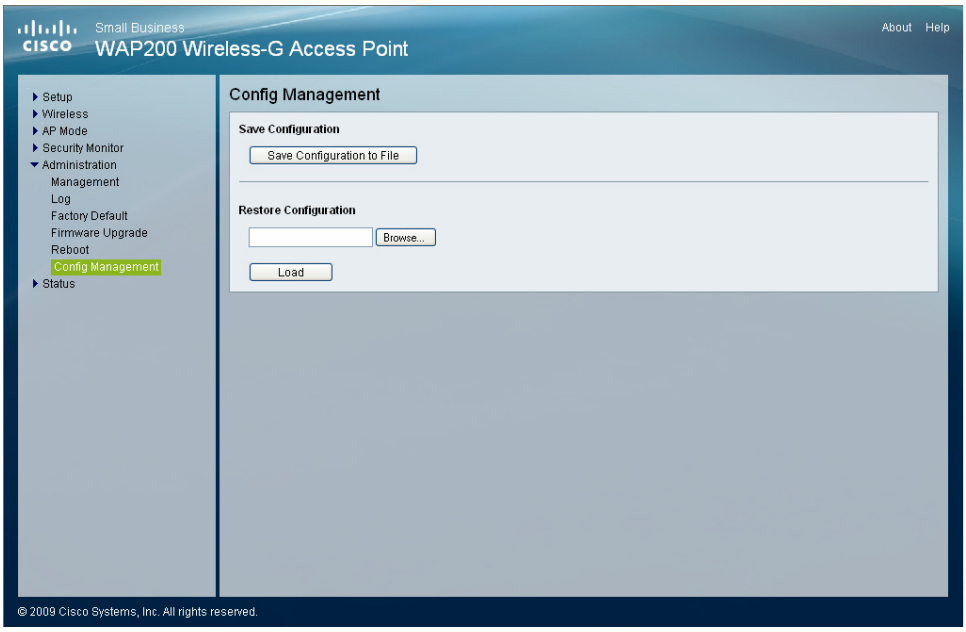
STEP 1 Click **Administration > Reboot**.

This feature is useful when you need to remotely reboot the access point.

STEP 2 Click **Reboot**.

Managing the Access Point's Configuration

The Administration > Config Management window allows you to create a backup configuration file or upload a configuration file to the access point.



To manage the configuration for the access point, follow these steps:

STEP 1 Click **Administration > Config Management**.

STEP 2 To create a backup configuration file, click **Save Configuration to File** and follow the on-screen instructions.

STEP 3 To restore (upload) the access point's configuration settings:

a. Enter the location of the configuration file or click **Browse** button to locate the file.

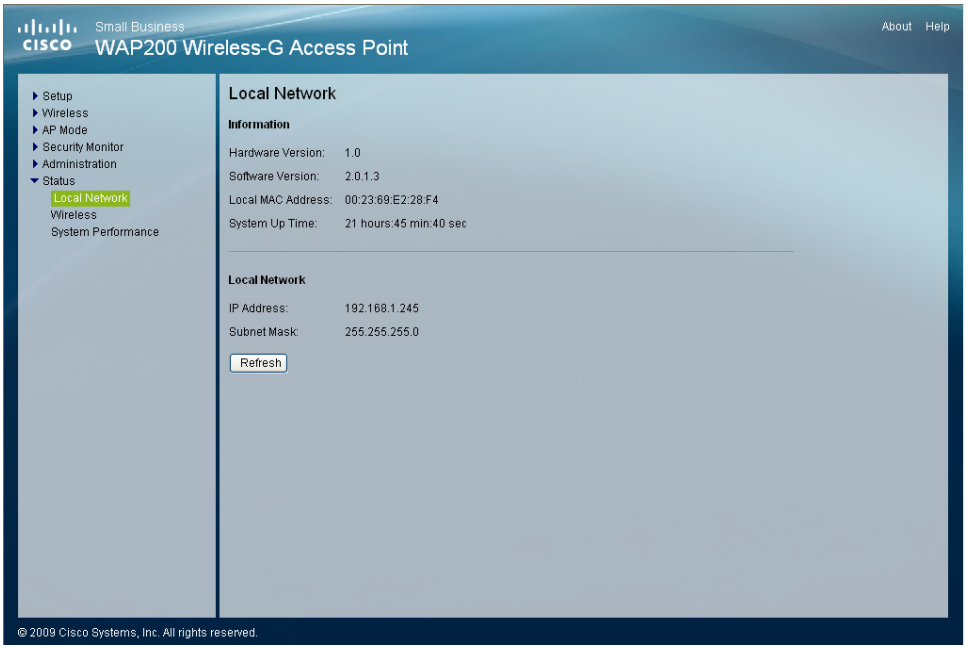
b. Click **Load**.

Verifying Access Point Status

This section describes how to check the status of the access point:

Checking Local Network Status

The Status > Local Network window displays the access point's current status information for the local network.



To check local network status, follow these steps:

STEP 1 Click **Status > Local Network**.

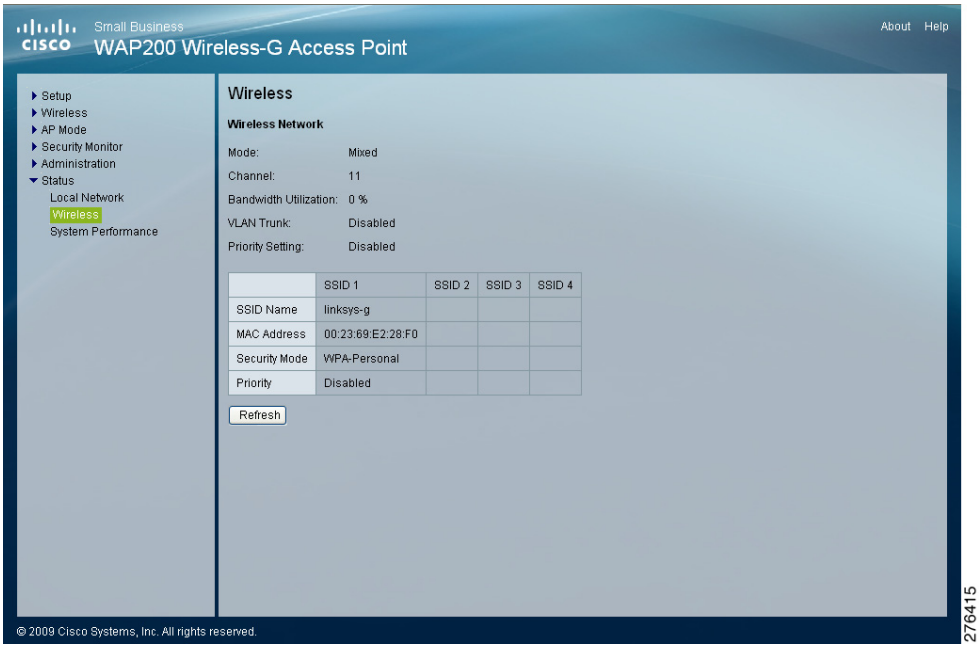
The Status > Local Network window displays the status information of the access point.

- Information
  - **Hardware Version**—Version of the access point's current hardware.
  - **Software Version**—Version of the access point's current software.
  - **Local MAC Address**—MAC address of the access point's LAN interface.
  - **System Up Time**—Length of time the access point has been running.
- Local Network
  - **IP Address**—Access point's IP address, as it appears on your local network.
  - **Subnet Mask**—Access point's subnet mask.

STEP 2 To update the status information, click **Refresh**.

Checking Wireless Status

The Status > Wireless window displays the access point's current status information for the wireless networks.



To check the wireless network status of the access point, follow these steps:

STEP 1 Click **Status > Wireless**.

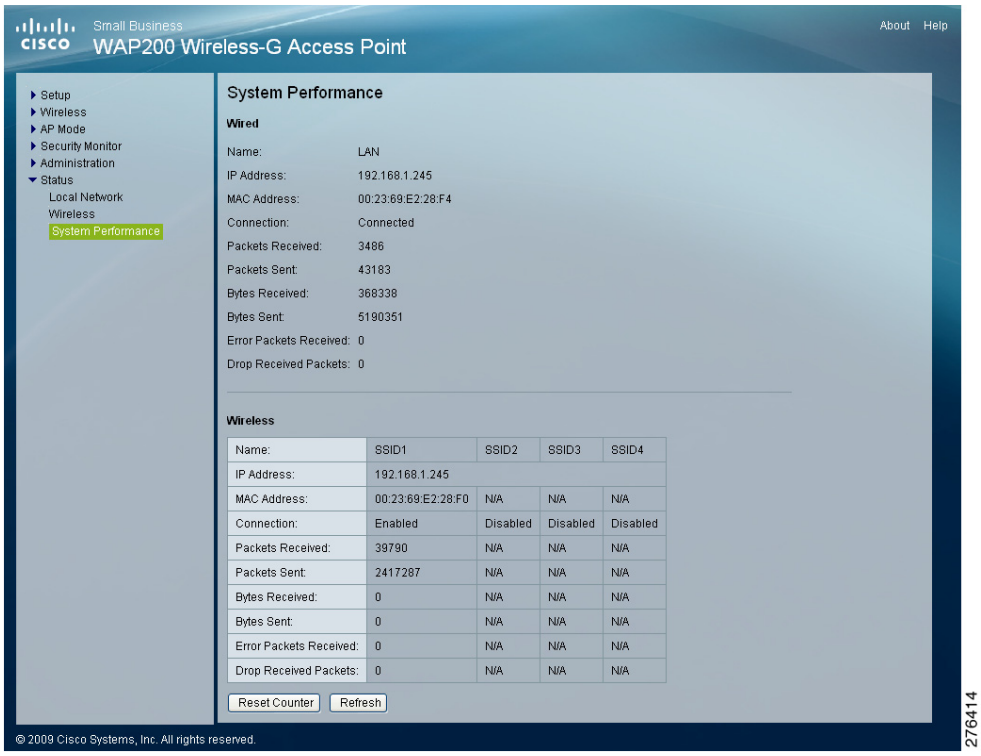
This page displays the status of the wireless network:

- **Mode**—Access point's wireless network mode.
- **Channel**—Access point's channel setting for the SSID.
- **Bandwidth Utilization**—Percentage of the bandwidth being used.
- **VLAN Trunk**—VLAN Trunk status.
- **Priority Setting**—Priority setting status.
- **SSID 1–4**—Information about the access point's SSIDs that have been configured.

STEP 2 To update the status information, click **Refresh**.

Checking System Performance

The Status > System Performance window displays the access point's status information for its current settings and data transmissions.



To check system performance of the access point, follow these steps:

STEP 1 Click **Status > Systems Performance**.

This page displays the access point's system performance values:

- Wired

  The statistics for the wired network, the LAN.

  - **Name**—Network to which the statistics refer, i.e. the LAN.
  - **IP Address**—Access point's local IP address.
  - **MAC Address**—MAC Address of the access point's wired interface.
  - **Connection**—Status of the access point's connection for the wired network.

- **Packets Received**—Number of packets received.
- **Packets Sent**—Number of packets sent.
- **Bytes Received**—Number of bytes received.
- **Bytes Sent**—Number of bytes sent.
- **Error Packets Received**—Number of error packets received.
- **Drop Received Packets**—Number of packets being dropped after they were received.

▪ Wireless

The statistics for the wireless network.

- **Name**—Wireless network/SSID to which the statistics refer.
- **IP Address**—Access point's local IP address.
- **MAC Address**—MAC Address of the access point's wireless interface.
- **Connection**—This shows the status of the access point's wireless networks.
- **Packets Received**—Number of packets received for each wireless network.
- **Packets Sent**—Number of packets sent for each wireless network.
- **Bytes Received**—Number of bytes received for each wireless network.
- **Bytes Sent**—Number of bytes sent for each wireless network.
- **Error Packets Received**—Number of error packets received for each wireless network.
- **Drop Received Packets**—Number of packets being dropped after they were received.
- **Reset Counter**—Click to reset packet statistic counters to zeros.

STEP 2 To update the status information, click **Refresh**.

STEP 3 To reset the counter, click **Reset Counter**.

Using Windows Help Menus

This wireless product requires Microsoft Windows. Product features can be accessed through Windows Help and are described in the following sections:

- TCP/IP, page 74
- Shared Resources, page 74
- Network Neighborhood/My Network Places, page 74

TCP/IP

Before a computer can communicate with the access point, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all computers follow to communicate over a network. This is true for wireless networks as well. Your computers will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other computers on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding computers to your network.

A

Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster.

If you can't find an answer here, check the Cisco website at www.cisco.com.

Can the WAP200 access point act as my DHCP Server?

No. The WAP200 access point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Can I run an application from a remote computer over the wireless network?

This depends on whether the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?

Yes, as long as the game supports multiple players over a local area network (LAN). Refer to the game's documentation for more information.

What is the IEEE 802.11b standard?

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard.

The 802.11b standard states a maximum data transfer rate of 11 Mbps and an operating frequency of 2.4 GHz.

What is the IEEE 802.11g standard?

It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard.

The 802.11g standard states a maximum data transfer rate of 54 Mbps and an operating frequency of 2.4 GHz.

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11 functions:

- CSMA/CA
- Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS
- Fragmentation
- Power Management

What IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

- CSMA/CA
- Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS
- Fragmentation
- Power Management

What is Ad-hoc?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is set to the same channel number as the access point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data.

Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system.

First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the Industrial, Scientific, and Medical (ISM) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security.

In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast.

If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

FHSS uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered.

Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with DSSS technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers a variety of wireless security methods to enhance security and access control. Users can set it up depending upon their needs.

Can Cisco wireless products support file and printer sharing?

Cisco wireless products perform the same function as LAN products. Therefore, Cisco wireless products can work with NetWare, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I avoid interference?

Using multiple access points on the same channel and in close proximity to one another will generate interference. When employing multiple access points, make sure to operate each one on a different channel (frequency).

How do I reset the access point?

Press the Reset button on the back of the access point for about ten seconds. This will reset the unit to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an access point and wireless computer will create signal loss. Leaded glass, metal, concrete floors, water, and walls will inhibit the signal and reduce range. Start with your access point and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, open the access point's web-based utility, click Wireless > Advanced, and make sure the output power is set to 100%.

Does the access point function as a firewall?

No. The access point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but cannot see my network.

Wireless security, such as WEP or WPA, is probably enabled on the access point, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices in your wireless network.

What is the maximum number of users the access point can handle?

No more than 65, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.

B

Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace.

Wireless networking operates by sending information over radio waves. As a result, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted.

Because you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

Security Checklist

The following is a complete list of security precautions to take (you should follow at least steps 1 through 6):

1. Change the default SSID. (See **Change the Default Wireless Network Name or SSID, page 81**.)
2. Disable SSID Broadcast. (See **Disable SSID Broadcast, page 81**.)
3. Change the default password for the Administrator account. (See **Change the Default Password, page 81**.)
4. Change the password for the Administrator account regularly. (See **Change the Administrator's Password Regularly, page 81**.)
5. Enable MAC Address Filtering. (See **Enable MAC Address Filtering, page 82**.)
6. Change the SSID periodically. (See **Change the SSID Periodically, page 82**.)
7. Use the highest encryption algorithm possible. (See **Enable Encryption, page 82**.)

Change the Default Wireless Network Name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Cisco wireless products use “ciscosb” as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

Disable SSID Broadcast

Most wireless networking devices give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don’t broadcast the SSID.

Change the Default Password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Cisco default password is admin. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device’s password so it will be hard to guess.

Change the Administrator’s Password Regularly

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings.

If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.

Enable MAC Address Filtering

Cisco routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

Change the SSID Periodically

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

Enable Encryption

Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

CAUTION Always remember that each device in your wireless network *must* use the same encryption method and encryption key or your wireless network will not function properly.

There are several ways that WEP can be maximized:

- Use the highest level of encryption possible.
- Change your WEP key regularly.

The WAP200 access point supports the following encryption algorithms.

- WPA—Wi-Fi Protected Access (WPA) is the replacement standard for WEP in Wi-Fi security. Two modes are available: Personal, and Enterprise. Both give you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. Enterprise utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

- WPA Personal—If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the AP or other device how often it should change the encryption keys.
- WPA Enterprise—WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the AP or other device.) First, select the type of WPA algorithm, TKIP or AES. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server.

- WPA2—Wi-Fi Protected Access 2 (WPA2) is the latest security standard in Wi-Fi security. Two modes are available: Personal and Enterprise. WPA2 always uses AES (Advanced Encryption System) for stronger data encryption.
  - WPA2 Personal—If you do not have a RADIUS server, enter a password in the Pre-Shared key field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the AP or other device how often it should change the encryption keys.
  - WPA2 Enterprise—WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the AP or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.
- WPA2 Mixed—WPA2 Mixed modes provide users an upgrade path from WPA to WPA2. You can have client devices running both WPA and WPA2 and the access point will automatically select the security method used by the client.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, you should enable encryption to protect your data.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password-protect all computers on the network and individually password-protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from computers walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

C

Specifications

This appendix lists the specifications of the Cisco WAP200 Wireless-G Access Point with Power Over Ethernet and Rangebooster.

Specifications

Model	WAP200
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power Over Ethernet),802.1p (QoS priority), 802.1q (VLAN), 802.1X (Security Authentication), 802.11i - Ready (Security WPA2), 802.11e - Ready (Wireless QoS), 802.11F (Wireless Roaming)
Ports	10/100 Base-T Ethernet, 12 VDC Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, POE, Wireless, Ethernet
Operating System	Linux

Setup/Configuration

Web UI	Built-in web user interface (UI) for easy browser-based configuration (HTTP/HTTPS)

Management

SNMP Version	SNMP Version 1, 2c, and 3
Event Logging	E-mail notification
	Remote Syslog
Web F/W upgrade	Firmware upgradeable through web-browser
Diags: Flash, etc.	Flash, RAM, LAN, WLAN
DHCP	DHCP Client

Operating Modes

Access Point	Access Point Mode, point-to-point Bridge Mode, point-to-multipoint Bridge Mode, Repeater Mode

Wireless

Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 11g/OFDM
Channels	Operating Channels: 11 North America
	13 Most of Europe (ETSI and Japan)
# of Internal Ant.	None
# of External Ant.	2 (Omni-Directional) SMA detachable
Transmit Power dBm	Transmit Power (Adjustable) @ Normal Temp Range: 11b - 18 dBm
	11g - 14 dBm

Antenna Gain in dBi	2
Receiver Sensitivity	11.g: 54Mbps@ -72dBm 11.b: 11Mbps@ -85dBM

Security

WEP/WPA/WPA2	WEP 64bit/128bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT
Access Control	Wireless Connection Control: MAC-Based
SSID Broadcast	SSID Broadcast Enable/Disable
802.1X	IEEE 802.1X support

Wireless Security

Monitor	Scans and Classifies wireless devices in the network. Reports new clients and access points joining the network, and suspicious network events. (Working together with 200 Business series client cards.)

Quality of Service

QoS	4 queues WMM wireless priority

General

	Wireless roaming based on IAPP Auto-channel selection

Environmental

Device Dimensions (W x D x H)	6.69 in. x 8.07 in. x 7.68 in. 170 mm x 205 mm x 195 mm
Weight	0.88 lb (0.4 kg)
Power	12V 1A DC input, and IEEE802.3af Compliant PoE
Certification	FCC, ICES-003, CE
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5% to 90% Noncondensing

D

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco WAP200 Wireless-G Access Point.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
Cisco WAP200 Access Point	www.cisco.com/en/US/products/ps10048/index.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace