



Configuring the Access Point for the First Time

This chapter describes how to configure basic settings on the wireless device for the first time. The contents of this chapter are similar to the instructions in the quick start guide that shipped with the wireless device. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the wireless device's web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

- [Before You Start, page 4-2](#)
- [Obtaining and Assigning an IP Address, page 4-4](#)
- [Connecting to the 350 Series Access Point Locally, page 4-5](#)
- [Connecting to the 1100 Series Access Point Locally, page 4-5](#)
- [Connecting to the 1130AG Series Access Point Locally, page 4-6](#)
- [Connecting to the 1200 and 1230AG Series Access Points Locally, page 4-7](#)
- [Connecting to the 1240AG Series Access Point Locally, page 4-7](#)
- [Connecting to the 1300 Series Access Point/Bridge Locally, page 4-8](#)
- [Assigning Basic Settings, page 4-8](#)
- [Configuring Basic Security Settings, page 4-14](#)
- [Configuring System Power Settings for 1130AG and 1240AG Access Points, page 4-24](#)
- [Using the IP Setup Utility, page 4-25](#)
- [Assigning an IP Address Using the CLI, page 4-26](#)
- [Using a Telnet Session to Access the CLI, page 4-27](#)
- [Configuring the 802.1X Supplicant, page 4-27](#)



Note

In this release, the access point radio interfaces are disabled by default.

Before You Start

Before you install the wireless device, make sure you are using a computer connected to the same network as the wireless device, and obtain the following information from your network administrator:

- The login and password for the access point. The default login is Cisco and the default password is Cisco (both case sensitive)
- A system name for the wireless device
- The case-sensitive wireless service set identifier (SSID) for your radio network
- If not connected to a DHCP server, a unique IP address for the wireless device (such as 172.17.255.115)
- If the wireless device is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- If you use IPSU to find the wireless device IP address, the access point MAC address. The MAC address can be found on the label on the bottom of the access point (such as 00164625854c).

Resetting the Device to Default Settings

If you need to start over during the initial setup process, you can reset the access point to factory default settings.

Resetting to Default Settings Using the MODE Button

Follow these steps to reset the access point to factory default settings using the access point MODE button:

-
- Step 1** Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.
 - Step 2** Press and hold the MODE button while you reconnect power to the access point.
 - Step 3** Hold the MODE button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button. All access point settings return to factory defaults.
-

**Note**

You cannot use the MODE button to reset 350 series access points to default settings. Use the web-browser interface to reset a 350 series access point to default settings, or follow the instructions in the [“Using the CLI” on page 22-17](#).

Resetting to Default Settings Using the GUI

Follow these steps to return to default settings using the access point GUI:

-
- Step 1** Open your Internet browser. The web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.
 - Step 2** Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password window appears.
 - Step 3** Enter your username in the User Name field. The default username is **Cisco**.
 - Step 4** Enter the wireless device password in the Password field and press **Enter**. The default password is **Cisco**. The Summary Status page appears.
 - Step 5** Click **System Software** and the System Software screen appears.
 - Step 6** Click **System Configuration** and the System Configuration screen appears.
 - Step 7** Click the **Reset to Defaults** button to reset all settings, including the IP address, to factory defaults. To reset all settings except the IP address to defaults, click the **Reset to Defaults (Except IP)** button.
-

Resetting to Default Settings Using the CLI



Caution

You should never delete any of the system files prior to resetting defaults or reloading software.

If you want to reset the access point to its default settings and a static IP address, use the *write erase* or *erase /all nvram* command. If you want to erase everything including the static IP address, in addition to the above commands, use the *erase* and *erase boot static-ipaddr static-ipmask* command.

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values using the CLI by following these steps:

-
- Step 1** Enter **erase nvram:** to erase all NVRAM files including the startup configuration.



Note The **erase nvram** command does not erase a static IP address.

-
- Step 2** Follow the step below to erase a static IP address and subnet mask. Otherwise, go to step 3.
 - a. Enter **erase boot static ip-address static-ipmask**.
 - Step 3** Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*.
 - Step 4** Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.

Step 5 Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm]*.



Caution

Do not interrupt the boot process to avoid damaging the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up*.

Step 6 After the access point/bridge reboots, you can reconfigure the access point by using the Web-browser interface if you previously assigned a static IP address, or the CLI if you did not.

The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). To obtain the access point/bridge's new IP address, you can use the *show interface bvi1* CLI command.

Obtaining and Assigning an IP Address

To browse to the wireless device's Express Setup page, you must either obtain or assign the wireless device's IP address using one of the following methods:

- If you have a 350, 1130AG, 1200, or 1240 series access point, connect to the access point console port and assign a static IP address. Follow the steps in the appropriate section to connect to the device's console port:
 - [Connecting to the 350 Series Access Point Locally, page 4-5](#)
 - [Connecting to the 1100 Series Access Point Locally, page 4-5](#)
 - [Connecting to the 1130AG Series Access Point Locally, page 4-6](#)
 - [Connecting to the 1200 and 1230AG Series Access Points Locally, page 4-7](#)
 - [Connecting to the 1240AG Series Access Point Locally, page 4-7](#)
 - [Connecting to the 1300 Series Access Point/Bridge Locally, page 4-8](#)
- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address using one of the following methods:
 - If you have a 350 or a 1200 series access point, connect to the wireless device console port and use the **show ip interface brief** command to display the IP address. Follow the steps in the [“Connecting to the 350 Series Access Point Locally”](#) section on page 4-5 or in the [“Connecting to the 1200 and 1230AG Series Access Points Locally”](#) section on page 4-7 to connect to the console port.
 - Provide your network administrator with the wireless device's Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The access point's MAC address is on label attached to the bottom of the access point.
 - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

You can download IPSU from the Software Center on Cisco.com. Click this link to browse to the Software Center:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

Default IP Address Behavior

When you connect a 350, 1130AG, 1200, 1240AG access point, or 1300 series access point/bridge with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

The 1300 series access point/bridge assumes a radio network role of a root access point. To configure it as a bridge, you must manually place it in install mode in order to align the antennas and establish a link. To establish the link you must have two access point/bridges configured in the install mode. In the install mode, one access point/bridge must be configured as a root bridge and the other a non-root bridge. To facilitate the configuration, an automatic option is available when the access point/bridge is in the install mode. After the wireless link is established and the bridge antennas are aligned, you take both access point/bridges out of install mode and place them on your LAN as root and non-root bridges.

Connecting to the 350 Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its RS-232 console port using a nine-pin, male-to-female, straight-through serial cable. Follow these steps to open the CLI by connecting to the access point console port:

-
- Step 1** Connect a nine-pin, male-to-female, straight-through DB-9 serial cable to the RS-232 serial port on the access point and to the COM port on a computer.
- Step 2** Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and Xon/Xoff flow control.-



Note If xon/xoff flow control does not work, use no flow control.

Connecting to the 1100 Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its Ethernet port using a Category 5 Ethernet cable. You can use a local connection to the Ethernet port much as you would use a serial port connection.



Note You do not need a special crossover cable to connect your PC to the access point; you can use either a straight-through cable or a crossover cable.

If the access point is configured with default values and it does not receive an IP address from the DHCP server, it defaults to IP address 10.0.0.1 for five minutes. During that five minutes, you can browse to that IP address to configure the unit. If after five minutes the unit has not been reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

Follow these steps to connect to the access point locally:

-
- Step 1** Make sure that the PC you intend to use to configure the access point is configured with an IP address from 10.0.0.2 to 10.0.0.10.
 - Step 2** Connect your PC to the access point using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.
 - Step 3** Power up the access point.
 - Step 4** Follow the steps in the “[Assigning Basic Settings](#)” section on page 4-8. If you make a mistake and need to start over, follow the steps in the “[Resetting the Device to Default Settings](#)” section on page 4-2.
 - Step 5** After configuring the access point, remove the Ethernet cable from your PC and connect the access point to your wired LAN.

**Note**

When you connect your PC to the access point or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Connecting to the 1130AG Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the access point console port:

-
- Step 1** Open the access point cover.
 - Step 2** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer. The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.
 - Step 3** Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

**Note**

If no flow control does not work, use xon/xoff flow control.

Connecting to the 1200 and 1230AG Series Access Points Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the access point console port:

-
- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.

- Step 2** Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.



Note If no flow control does not work, use xon/xoff flow control.



Note When your configuration changes are completed, you must remove the serial cable from the access point.

Connecting to the 1240AG Series Access Point Locally

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the access point console port:

-
- Step 1** Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.



Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to <http://www.cisco.com/go/marketplace> to order a serial cable.

- Step 2** Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.



Note If no flow control does not work, use xon/xoff flow control.

Connecting to the 1300 Series Access Point/Bridge Locally

If you need to configure the access point/bridge locally (without connecting the access point/bridge to a wired LAN), you can connect a PC to the Ethernet port on the long-reach power injector using a Category 5 Ethernet cable. You can use a local connection to the power injector's Ethernet port much as you would use a serial port connection.


Note

You do not need a special crossover cable to connect your PC to the power injector; you can use either a straight-through cable or a crossover cable.

Follow these steps to connect to the bridge locally:

Step 1 Make sure that the PC you intend to use is configured to obtain an IP address automatically, or manually assign it an IP address within the same subnet as the access point/bridge IP address. For example, if you assigned the access point/bridge an IP address of 10.0.0.1, assign the PC an IP address of 10.0.0.20.

Step 2 With the power cable disconnected from the power injector, connect your PC to the power injector using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.


Note

Communication takes place between the power injector and the access point/bridge using Ethernet Port 0. Do not attempt to change any of the Ethernet Port 0 settings.

Step 3 Connect the power injector to the access point/bridge using dual coaxial cables.

Step 4 Connect the power injector power cable and power up the access point/bridge.

Step 5 Follow the steps in the [“Assigning Basic Settings” section on page 4-8](#). If you make a mistake and need to start over, follow the steps in the [“Resetting the Device to Default Settings” procedure on page 4-2](#).

Step 6 After configuring the access point/bridge, remove the Ethernet cable from your PC and connect the power injector to your wired LAN.


Note

When you connect your PC to the access point/bridge or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering `ipconfig /release` and `ipconfig /renew` commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Assigning Basic Settings

After you determine or assign the wireless device's IP address, you can browse to the wireless device's Express Setup page and perform an initial configuration:

Step 1 Open your Internet browser. The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

- Step 2** Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.
- Step 3** Press **Tab** to bypass the Username field and advance to the Password field.
- Step 4** Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears, as shown in [Figure 4-1](#).

Figure 4-1 Summary Status Page

Cisco 1200 Access Point

Hostname **ap** ap uptime is 1 day, 1 hour, 36 minutes

Home: Summary Status

Association

Clients: [0](#) Repeaters: [0](#)

Network Identity

IP Address: 10.91.104.91
 MAC Address: 0005.9a38.42c0

Network Interfaces

Interface	MAC Address	Transmission Rate
↑ FastEthernet	0005.9a38.42c0	100Mb/s
↑ Radio0-802.11B	0001.6445.b9e6	11.0Mb/s
↑ Radio1-802.11A	0005.9a39.2451	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 00:00:58.231	◆ Notification	Line protocol on Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.250	◆ Error	Interface Dot11Radio0, changed state to up
Mar 1 00:00:57.231	◆ Information	Interface Dot11Radio0, frequency 2447 selected
Mar 1 00:00:57.231	◆ Information	Interface Dot11Radio0, frequency 2457 is in use
Mar 1 00:00:57.231	◆ Information	Interface Dot11Radio0, frequency 2437 is in use
Mar 1 00:00:57.231	◆ Information	Interface Dot11Radio0, frequency 2427 is in use
Mar 1 00:00:57.230	◆ Information	Interface Dot11Radio0, frequency 2422 is in use
Mar 1 00:00:57.230	◆ Information	Interface Dot11Radio0, frequency 2417 is in use
Mar 1 00:00:57.230	◆ Information	Interface Dot11Radio0, frequency 2412 is in use
Mar 1 00:00:55.232	◆ Notification	Line protocol on Interface Dot11Radio1, changed state to up

Refresh

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc. 111869

- Step 5** Click **Express Setup**. The Express Setup screen appears. [Figure 4-2](#) and [Figure 4-3](#) shows the Express Setup page for the 1100 and 1130AG access points.

Figure 4-2 Express Setup Page for 1100 and 1130AG Series Access Points

HOME | EXPRESS SET-UP | EXPRESS SECURITY | NETWORK MAP + | ASSOCIATION + | NETWORK INTERFACES + | SECURITY + | SERVICES + | WIRELESS SERVICES + | SYSTEM SOFTWARE + | EVENT LOG +

Hostname AP1100 15:03:21 Mon May 16 2005

Express Set-Up

Host Name:

MAC Address: 0005.9a39.2110

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0-802.11B

Role in Radio Network: Access Point Repeater
 Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Custom

Aironet Extensions: Enable Disable

Apply Cancel 135519

Figure 4-3 Express Setup Page for 1200 and 1240AG Series Access Points

HOME | EXPRESS SET-UP | EXPRESS SECURITY | NETWORK MAP + | ASSOCIATION + | NETWORK INTERFACES + | SECURITY + | SERVICES + | WIRELESS SERVICES + | SYSTEM SOFTWARE + | EVENT LOG +

Hostname AP1242AG AP1242AG uptime is 1 week, 2 days, 17 hours, 0 minutes

Express Set-Up

Host Name:

MAC Address: 000b.fcff.b04e

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0-802.11G

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

Radio1-802.11A

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

Apply Cancel 230144

Figure 4-4 shows the Express Setup page for the 1300 series access point/bridge.

Figure 4-4 Express Setup Page for the 1300 Series Access Point/Bridge

The screenshot displays the 'Express Set-Up' configuration page for a BR1310G access point. The page is titled 'Express Set-Up' and shows the following configuration details:

- Host Name:** BR1310G
- MAC Address:** 000b.fc8.adce
- Configuration Server Protocol:** DHCP Static IP
- IP Address:** 10.91.107.17
- IP Subnet Mask:** 255.255.255.192
- Default Gateway:** 10.91.107.1
- SNMP Community:** defaultCommunity
 - Read-Only
 - Read-Write

Below the main configuration section, there is a section for 'Radio0-802.11G' with the following options:

- Role in Radio Network:**
 - Access Point
 - Repeater
 - Root Bridge
 - Non-Root Bridge
 - Install-Mode
 - Workgroup Bridge
 - Scanner
- Optimize Radio Network for:**
 - Throughput
 - Range
 - Default
 - Custom
- Aironet Extensions:**
 - Enable
 - Disable

The page includes a navigation menu on the left with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. At the bottom right, there are 'Apply' and 'Cancel' buttons. The page number '146689' is visible in the bottom right corner.

Step 6 Enter the configuration settings you obtained from your system administrator. The configurable settings include:

- **Host Name**—The host name, while not an essential setting, helps identify the wireless device on your network. The host name appears in the titles of the management system pages.



Note You can enter up to 32 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between wireless devices, make sure a unique portion of the system name appears in the first 15 characters.



Note When you change the system name, the wireless device resets the radios, causing associated client devices to disassociate and quickly reassociate.

- **Configuration Server Protocol**—Click on the button that matches the network’s method of IP address assignment.
 - **DHCP**—IP addresses are automatically assigned by your network’s DHCP server.
 - **Static IP**—The wireless device uses a static IP address that you enter in the IP address field.

- **IP Address**—Use this setting to assign or change the wireless device’s IP address. If DHCP is enabled for your network, leave this field blank.

**Note**

If the wireless device’s IP address changes while you are configuring the wireless device using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the wireless device. If you lose your connection, reconnect to the wireless device using its new IP address. Follow the steps in the [“Resetting the Device to Default Settings”](#) section on page 4-2 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **Role in Radio Network**—Click on the button that describes the role of the wireless device on your network. Select **Access Point (Root)** if the wireless device is connected to the wired LAN. Select **Repeater (Non-Root)** if it is not connected to the wired LAN.
 - **Access Point**—A root device; accepts associations from clients and bridges wireless traffic from the clients to the wireless LAN. This setting can be applied to any access point.
 - **Repeater**—A non-root device; accepts associations from clients and bridges wireless traffic from the clients to root access point connected to the wireless LAN. This setting can be applied to any access point.
 - **Root Bridge**—Establishes a link with a non-root bridge. In this mode, the device also accepts associations from clients. This setting is available only for the 1200 and 1240AG series access points.
 - **Non-Root Bridge**—In this mode, the device establishes a link with a root bridge. This setting is available only for the 1200 and 1240AG series access points.
 - **Install Mode**—Places the 1300 series access point/bridge in auto installation mode so you can align and adjust a bridge link for optimum efficiency.
 - **Workgroup Bridge**—Emulates a Cisco Aironet 350 Series Workgroup Bridge. In the Workgroup bridge mode, the access point functions as a client device that associates with a Cisco Aironet access point or bridge. A workgroup bridge can have a maximum of 254 clients, presuming that no other wireless clients are associated to the root bridge or access point. This setting is available for the 1100, 1200, and 1300 series access points.
 - **Scanner**—Functions as a network monitoring device. In the Scanner mode, the access point does not accept associations from clients. It continuously scans and reports wireless traffic it detects from other wireless devices on the wireless LAN. All access points can be configured as a scanner.
- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the wireless device radio or customized settings for the wireless device radio.
 - **Throughput**—Maximizes the data volume handled by the wireless device, but might reduce its range.
 - **Range**—Maximizes the wireless device’s range but might reduce throughput.
 - **Custom**—The wireless device uses the settings you enter on the Network Interfaces: Radio-802.11b Settings page. Clicking **Custom** takes you to the Network Interfaces: Radio-802.11b Settings page.

- **Aironet Extensions**—Enable this setting if there are only Cisco Aironet devices on your wireless LAN.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).

Step 7 Click **Apply** to save your settings.

Step 8 Click **Network Interfaces** to browse to the Network Interfaces Summary page.

Step 9 Click the radio interface to browse to the Network Interfaces: Radio Status page.

Step 10 Click the **Settings** tab to browse to the Settings page for the radio interface.

Step 11 Click **Enable** to enable the radio.

Step 12 Click **Apply**.

Your wireless device is now running but probably requires additional configuring to conform to your network's operational and security requirements. Consult the chapters in this manual for the information you need to complete the configuration.



Note You can restore 1100 and 1200 series access points to factory defaults by unplugging the power jack and plugging it back in while holding down the Mode button for a few seconds, or until the Status LED turns amber.

Default Settings on the Express Setup Page

Table 4-1 lists the default settings for the settings on the Express Setup page.

Table 4-1 Default Settings on the Express Setup Page

Setting	Default
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; see the “Default IP Address Behavior” section on page 4-5 for a description of default IP address behavior on the access point
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, the default setting is 0.0.0.0
Role in Radio Network	Access point
Optimize Radio Network for	Throughput
Aironet Extensions	Enable
SNMP Community	defaultCommunity

Configuring Basic Security Settings

After you assign basic settings to the wireless device, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the wireless device can communicate beyond the physical boundaries of your worksite.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them. Figure 4-5 shows the Express Security page.

Figure 4-5 Express Security Page

Hostname AP1242AG AP1242AG uptime is 1 week, 3 days, 12 hours, 51 minutes

Express Security Set-Up

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN

No VLAN Enable VLAN ID: (1-4095) Native VLAN

3. Security

No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID

Close Window Copyright (c) 1992-2005 by Cisco Systems, Inc. 230143

The Express Security page helps you configure basic security settings. You can use the web-browser interface's main Security pages to configure more advanced security settings.

Understanding Express Security Settings

The SSIDs that you create using the Express security page appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the wireless device. On dual-radio wireless devices, the SSIDs that you create are enabled on both radio interfaces.



Note In Cisco IOS Release 12.3(8)JA, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

The SSID can consist of up to 32 alphanumeric, case-sensitive, characters.

The first character can not contain the following characters:

- Exclamation point (!)
- Pound sign (#)
- Semicolon (;)

The following characters are invalid and cannot be used in an SSID:

- Plus sign (+)
- Right bracket (])
- Front slash (/)
- Quotation mark (")
- Tab
- Trailing spaces

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because on the Express Security page encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Express Security Types

Table 4-2 describes the four security types that you can assign to an SSID.

Table 4-2 Security Types on Express Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the wireless device based on MAC address (see the “Using MAC Address ACLs to Block or Allow Client Association to the Access Point” on page 16-6) or, if your network does not have a RADIUS server, consider using an access point as a local authentication server (see Chapter 9, “Configuring an Access Point as a Local Authenticator”).	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the wireless device’s key.

Table 4-2 Security Types on Express Security Setup Page (continued)

Security Type	Description	Security Features Enabled
EAP Authentication	<p>This option enables 802.1X authentication (such as LEAP, PEAP, EAP-TLS, EAP-FAST, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1X/EAP based products)</p> <p>This setting uses mandatory encryption, WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645.</p> <p>You are required to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1X authentication provides dynamic encryption keys, you do not need to enter a WEP key.</p>	<p>Mandatory 802.1X authentication. Client devices that associate using this SSID must perform 802.1X authentication.</p> <p>If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you don't configure open authentication with EAP, the following GUI warning message appears:</p> <p>WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.</p> <p>If you are using the CLI, this warning message appears:</p> <p>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.</p>
WPA	<p>Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP.</p> <p>This setting uses encryption ciphers, TKIP, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645.</p> <p>As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).</p>	<p>Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable.</p> <p>If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you don't configure open authentication with EAP, the following GUI warning message appears:</p> <p>WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.</p> <p>If you are using the CLI, this warning message appears:</p> <p>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.</p>

Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the wireless device's security capabilities. Keep these limitations in mind when using the Express Security page:

- If the **No VLAN** option is selected, the static WEP key can be configured once. If you select **Enable VLAN**, the static WEP key should be disabled.
- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the wireless device. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

-
- Step 1** Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.
- Step 2** To broadcast the SSID in the wireless device beacon, check the Broadcast SSID in Beacon check box. When you broadcast the SSID, devices that do not specify an SSID can associate to the wireless device. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the wireless device unless their SSID matches this SSID. Only one SSID can be included in the wireless device beacon.
- Step 3** (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.
- Step 4** (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.
- Step 5** Select the security setting for the SSID. The settings are listed in order of robustness, from No Security to WPA, which is the most secure setting. If you select EAP Authentication or WPA, enter the IP address and shared secret for the authentication server on your network.



Note If you do not use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. See the [“Using VLANs”](#) section on page 4-15 for details.

- Step 6** Click **Apply**. The SSID appears in the SSID table at the bottom of the page.
-

CLI Configuration Examples

The examples in this section show the CLI commands that are equivalent to creating SSIDs using each security type on the Express Security page. This section contains these example configurations:

- [Example: No Security, page 4-19](#)
- [Example: Static WEP, page 4-20](#)
- [Example: EAP Authentication, page 4-21](#)
- [Example: WPA, page 4-22](#)

Example: No Security

This example shows part of the configuration that results from using the Express Security page to create an SSID called *no_security_ssid*, including the SSID in the beacon, assigning it to VLAN 10, and selecting VLAN 10 as the native VLAN:

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid no_security_ssid
  vlan 10
  authentication open
  guest-mode
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
 !
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
 !
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid no_security_ssid
  vlan 10
  authentication open
  guest-mode
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 !
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
```

Example: Static WEP

This example shows part of the configuration that results from using the Express Security page to create an SSID called *static_wep_ssid*, excluding the SSID from the beacon, assigning the SSID to VLAN 20, selecting 3 as the key slot, and entering a 128-bit key:

```
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 FFD518A21653687A4251AEE1230C transmit-key
encryption vlan 20 mode wep mandatory
!
ssid static_wep_ssid
vlan 20
authentication open
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
bridge-group 20 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 741F07447BA1D4382450CB68F37A transmit-key
encryption vlan 20 mode wep mandatory
!
ssid static_wep_ssid
vlan 20
authentication open
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1.20
```

```

encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
bridge-group 20 spanning-disabled

```

Example: EAP Authentication

This example shows part of the configuration that results from using the Express Security page to create an SSID called *eap_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 30:



Note

The following warning message appears if your radio clients are using EAP-FAST and you don't include open authentication with EAP as part of the configuration:

SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

```

interface Dot11Radio0/1
no ip address
no ip route-cache
!
encryption vlan 30 mode wep mandatory
!
ssid eap_ssid
vlan 30
authentication open eap eap_methods
authentication network-eap eap_methods
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0/1.30
encapsulation dot1Q 30
no ip route-cache
bridge-group 30
bridge-group 30 subscriber-loop-control
bridge-group 30 block-unknown-source
no bridge-group 30 source-learning
no bridge-group 30 unicast-flooding
bridge-group 30 spanning-disabled
!
interface Dot11Radio0/1
no ip address
no ip route-cache
!
encryption vlan 30 mode wep mandatory
!
ssid eap_ssid
vlan 30
authentication open eap eap_methods

```

```

        authentication network-eap eap_methods
    !
    speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
    rts threshold 2312
    station-role root
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
    bridge-group 1 spanning-disabled
    !
interface Dot11Radio0/1.30
    encapsulation dot1Q 30
    no ip route-cache
    bridge-group 30
    bridge-group 30 subscriber-loop-control
    bridge-group 30 block-unknown-source
    no bridge-group 30 source-learning
    no bridge-group 30 unicast-flooding
    bridge-group 30 spanning-disabled
    !
interface FastEthernet0
    mtu 1500
    no ip address
    ip mtu 1564
    no ip route-cache
    duplex auto
    speed auto
    bridge-group 1
    no bridge-group 1 source-learning
    bridge-group 1 spanning-disabled
    !
interface FastEthernet0.30
    mtu 1500
    encapsulation dot1Q 30
    no ip route-cache
    bridge-group 30
    no bridge-group 30 source-learning
    bridge-group 30 spanning-disabled
    !
interface BVI1
    ip address 10.91.104.91 255.255.255.192
    no ip route-cache
    !
    ip http server
    ip http help-path
    http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
    ip radius source-interface BVI1
    radius-server attribute 32 include-in-access-req format %h
    radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 091D1C5A4D5041
    radius-server authorization permit missing Service-Type
    radius-server vsa send accounting
    bridge 1 route ip

```

Example: WPA

This example shows part of the configuration that results from using the Express Security page to create an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```

aaa new-model
!

```

```
!
aaa group server radius rad_eap
  server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0/1
  no ip address
  no ip route-cache
  !
  encryption vlan 40 mode ciphers tkip
  !
  ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
  !
  speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
  rts threshold 2312
  station-role root
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
  bridge-group 1 spanning-disabled
!
interface Dot11Radio0/1.40
  encapsulation dot1Q 40
  no ip route-cache
  bridge-group 40
  bridge-group 40 subscriber-loop-control
  bridge-group 40 block-unknown-source
  no bridge-group 40 source-learning
  no bridge-group 40 unicast-flooding
  bridge-group 40 spanning-disabled
!
interface FastEthernet0
  no ip address
  no ip route-cache
  duplex auto
  speed auto
```

```

bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.40
encapsulation dot1Q 40
no ip route-cache
bridge-group 40
no bridge-group 40 source-learning
bridge-group 40 spanning-disabled

```

Configuring System Power Settings for 1130AG and 1240AG Access Points

The 1130AG and 1240AG access points disable the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. Figure 4-6 shows the System Power Settings section of the System Configuration page.

Figure 4-6 Power Options on the System Software: System Configuration Page

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

Using the AC Power Adapter

If you use the AC power adapter to provide power to the 1130AG or 1240AG access point, you do not need to adjust the access point configuration.

Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG or 1240AG access point, and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG access point, and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

Using a Power Injector

If you use a power injector to provide power to the 1130AG or 1240AG access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

Using the IP Setup Utility

IPSU enables you to find a wireless device's IP address when it has been assigned by a DHCP server. This section explains how to install the utility and how to use it to find the wireless device's IP address.

**Note**

IPSU discovers the access point's IP address only if the unit receives an address from the DHCP server or if you set the IP address manually. By default, access points that have a console port send DHCP requests to the DHCP server indefinitely. IPSU cannot report the IP address until the access point receives one.

**Note**

IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP.

**Tip**

Another simple way to find the wireless device's IP address is to look on the Status screen in the Aironet Client Utility on a client device associated to the wireless device.

Obtaining IPSU

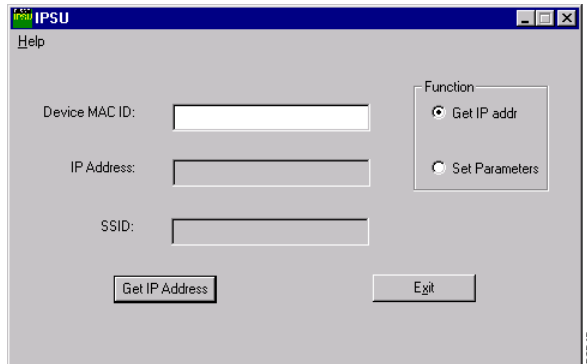
IPSU is available on the Cisco web site. Click this link to browse to the Software Center on Cisco.com:
<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>

Using IPSU to Find the Access Point's IP Address

If the wireless device receives an IP address from a DHCP server, you can use IPSU to find its IP address. Because IPSU sends a reverse-ARP request based on the wireless device MAC address, you must run IPSU from a computer on the same subnet as the wireless device. Follow these steps to find the wireless device's IP address:

- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see [Figure 4-7](#)).

Figure 4-7 IPSU Get IP Address Screen



Step 2 When the utility window opens, make sure the *Get IP addr* radio button in the Function box is selected.

Step 3 Enter the wireless device's MAC address in the Device MAC ID field. The wireless device's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your wireless device's MAC address might look like the following example:

000BFCFFB24E



Note The MAC address field is not case-sensitive.

Step 4 Click **Get IP Address**.

Step 5 When the wireless device's IP address appears in the IP Address field, write it down.

Assigning an IP Address Using the CLI

When you connect the wireless device to the wired LAN, the wireless device links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the wireless device's Ethernet and radio ports, the network uses the BVI.

When you assign an IP address to the wireless device using the CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the wireless device's BVI:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface bvi1	Enter interface configuration mode for the BVI.
Step 3	ip address address mask	Assign an IP address and address mask to the BVI.
		<p>Note If you are connected to the wireless device using a Telnet session, you lose your connection to the wireless device when you assign a new IP address to the BVI. If you need to continue configuring the wireless device using Telnet, use the new IP address to open another Telnet session to the wireless device.</p>

Using a Telnet Session to Access the CLI

Follow these steps to access the CLI by using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.



Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the wireless device's IP address.

Step 3 In the Host Name field, type the wireless device's IP address and click **Connect**.

Configuring the 802.1X Supplicant

Traditionally, the dot1x authenticator/client relationship has always been a network device and a PC client respectively, as it was the PC user that had to authenticate to gain access to the network. However, wireless networks introduce unique challenges to the traditional authenticator/client relationship. First, access points can be placed in public places, inviting the possibility that they could be unplugged and their network connection used by an outsider. Second, when a repeater access point is incorporated into a wireless network, the repeater access point must authenticate to the root access point in the same way as a client does.



Note

The 802.1X supplicant is available on 1130AG, 1240AG, and 1300 series access points. It is not available on 1100 and 1200 series access points.

The supplicant is configured in two phases:

- Create and configure a credentials profile
- Apply the credentials to an interface or SSID

You can complete the phases in any order, but they must be completed before the supplicant becomes operational.

Creating a Credentials Profile

Beginning in privileged EXEC mode, follow these steps to create an 802.1X credentials profile:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x credentials <i>profile</i>	Creates a dot1x credentials profile and enters the dot1x credentials configuration submenu.
Step 3	anonymous-id <i>description</i>	(Optional)—Enter the anonymous identity to be used.
Step 4	description <i>description</i>	(Optional)—Enter a description for the credentials profile
Step 5	username <i>username</i>	Enter the authentication user id.
Step 6	password { 0 7 LINE }	Enter an unencrypted password for the credentials. 0 —An unencrypted password will follow. 7 —A hidden password will follow. Hidden passwords are used when applying a previously saved configuration. LINE —An unencrypted (clear text) password. Note Unencrypted and clear text are the same. You can enter a 0 followed by the clear text password, or omit the 0 and enter the clear text password.
Step 7	pki-trustpoint <i>pki-trustpoint</i>	(Optional and only used for EAP-TLS)—Enter the default pki-trustpoint.
Step 8	end	Return to the privileged EXEC mode.
Step 9	copy running config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the **dot1x credentials** command to negate a parameter.

The following example creates a credentials profile named *test* with the username *Cisco* and a the unencrypted password *Cisco*:

```
ap1240AG>enable
Password:xxxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG(config)# dot1x credentials test
ap1240AG(config-dot1x-creden)#username Cisco
ap1240AG(config-dot1x-creden)#password Cisco
ap1240AG(config-dot1x-creden)#exit
ap1240AG(config)#
```

Applying the Credentials to an Interface or SSID

Credential profiles are applied to an interface or an SSID in the same way.

Applying the Credentials Profile to the Wired Port

Beginning in the privileged EXEC mode, follow these steps to apply the credentials to the access point's wired port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface fastethernet 0	Enter the interface configuration mode for the access point's Fast Ethernet port. Note You can also use interface fa0 to enter the fast Ethernet configuration mode.
Step 3	dot1x credentials <i>profile name</i>]	Enter the name of a previously created credentials profile.
Step 4	end	Return to the privileged EXEC mode
Step 5	copy running config startup-config	(Optional) Save your entries in the configuration file.

The following example applies the credentials profile *test* to the access point's Fast Ethernet port:

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG (config)#interface fa0
ap1240AG (config-if)#dot1x credentials test
ap1240AG (config-if)#end
ap1240AG#
```

Applying the Credentials Profile to an SSID Used For the Uplink

If you have a repeater access point in your wireless network and are using the 802.1X supplicant on the root access point, you must apply the 802.1X supplicant credentials to the SSID the repeater uses to associate with and authenticate to the root access point.

Beginning in the privileged EXEC mode, follow these steps to apply the credentials to an SSID used for the uplink:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 ssid <i>ssid</i>	Enter the 802.11 SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Note The first character cannot contain the !, #, or ; character. +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.
Step 3	dot1x credentials <i>profile</i>	Enter the name of a preconfigured credentials profile.
Step 4	end	Exits the dot1x credentials configuration submode
Step 5	copy running config startup-config	(Optional) Save your entries in the configuration file.

The following example applies the credentials profile *test* to the ssid *testap1* on a repeater access point.

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
repeater-ap(config-if)#dot1x ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

Creating and Applying EAP Method Profiles

You can optionally configure an EAP method list to enable the supplicant to recognize a particular EAP method. See [“Creating and Applying EAP Method Profiles for the 802.1X Supplicant” on page 11-17](#).