



Configuring the Access Point for the First Time

This chapter describes how to configure basic settings on your access point for the first time. The contents of this chapter are similar to the instructions in the quick start guide that shipped with your access point. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the access point'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 2-2](#)
- [Obtaining and Assigning an IP Address, page 2-3](#)
- [Connecting to the 350 Series Access Point Locally, page 2-4](#)
- [Connecting to the 1100 Series Access Point Locally, page 2-5](#)
- [Connecting to the 1200 Series Access Point Locally, page 2-6](#)
- [Assigning Basic Settings, page 2-6](#)
- [Configuring Basic Security Settings, page 2-11](#)
- [Using the IP Setup Utility, page 2-19](#)
- [Assigning an IP Address Using the CLI, page 2-22](#)
- [Using a Telnet Session to Access the CLI, page 2-22](#)

Before You Start

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

- A system name for the access point
- The case-sensitive wireless service set identifier (SSID) for your radio network
- If not connected to a DHCP server, a unique IP address for your access point (such as 172.17.255.115)
- If the access point 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 or assign the access point IP address, the MAC address from the label on the bottom of the access point (such as 00164625854c)

Resetting the Access Point to Default Settings

If you need to start over during the initial setup process, 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” section on page 22-7](#).

Follow these steps to return to default settings using the web-browser interface:

-
- Step 1** Open your Internet browser. The access point 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 access point’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 access point 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.

**Note**

If the access point is configured with a static IP address, the IP address does not change. If the access point is not configured with a static IP address, the access point requests a DHCP address. If it does not receive an address from a DHCP server, its IP address is 10.0.0.1.

Obtaining and Assigning an IP Address

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

- Use default address 10.0.0.1 when you connect to the access point locally. For detailed instructions, see the [“Connecting to the 1100 Series Access Point Locally”](#) section on page 2-5.
- If you have a 350 or a 1200 series access point, connect to the access point console port and assign a static IP address. Follow the steps in the [“Connecting to the 350 Series Access Point Locally”](#) section on page 2-4 or in the [“Connecting to the 1200 Series Access Point Locally”](#) section on page 2-6 to connect to the console port.
- 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 access point 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 2-4 or in the [“Connecting to the 1200 Series Access Point Locally”](#) section on page 2-6 to connect to the console port.
 - Provide your organization's network administrator with your access point'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. You can also use IPSU to assign an IP address to the access point if it did not receive an IP address from the DHCP server. 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>

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. [Figure 2-3](#) shows the serial port connection.

Figure 2-1 Connecting the Serial Cable (Access Point with Plastic Case)

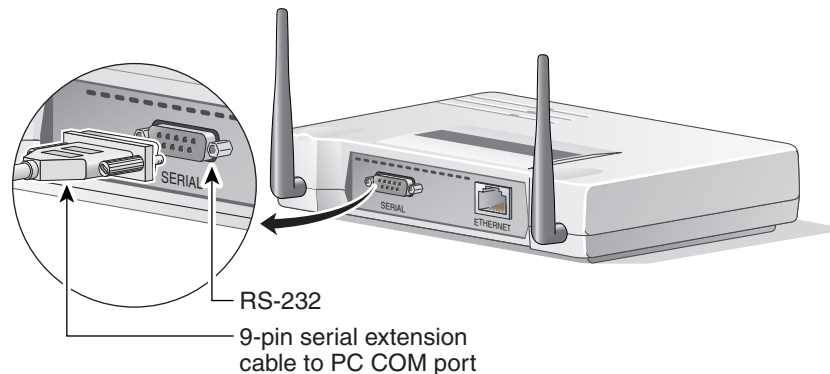
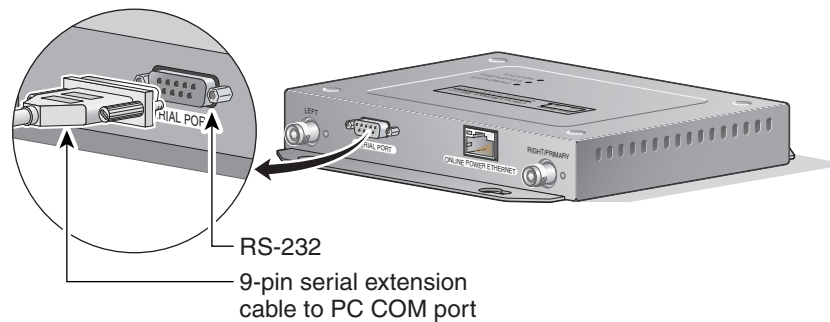


Figure 2-2 Connecting the Serial Cable (Access Point with Metal Case)



- 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.

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 not connected to a DHCP server or cannot obtain an IP address, it defaults to IP address 10.0.0.1 and becomes a mini-DHCP server. In that capacity, the access point provides up to twenty IP addresses between 10.0.0.11 and 10.0.0.30 to the following devices:

- An Ethernet-capable PC connected to its Ethernet port
- Wireless client devices configured to use either no SSID or *tsunami* as the SSID, and with all security settings disabled

The mini-DHCP server feature is disabled automatically when you assign a static IP address to the access point.



Caution

When an access point with default settings is connected on a wired LAN and does not receive an IP address from a DHCP server, the access point provides an IP address to any DHCP requests it receives.

Follow these steps to connect to the access point 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 from 10.0.0.2 to 10.0.0.10. 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 2** Power up the access point.
- Step 3** Follow the steps in the [“Assigning Basic Settings” section on page 2-6](#). If you make a mistake and need to start over, follow the steps in the [“Resetting the Access Point to Default Settings” section on page 2-2](#).
- Step 4** After configuring the access point, remove the Ethernet cable from your PC and connect the access point to your wired LAN.



Note

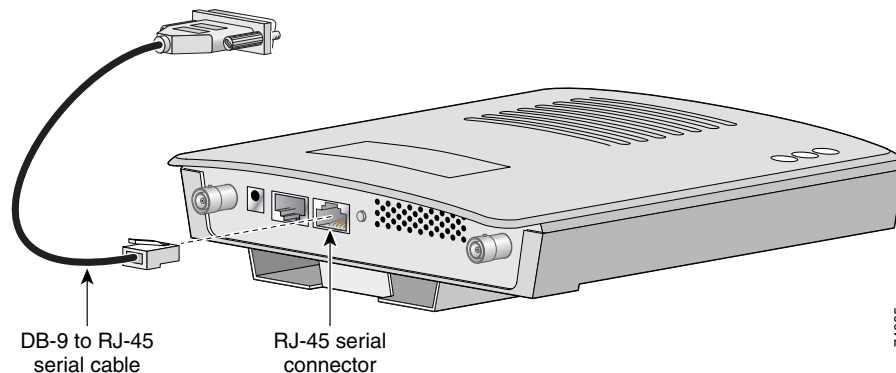
When you connect your PC to the access point or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering `ipconfig /release` and `ipconfig /renew` commands in a command prompt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

Connecting to the 1200 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. [Figure 2-3](#) shows the serial port connection.

Figure 2-3 Connecting the Serial Cable



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.
-

Assigning Basic Settings

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

-
- Step 1** Open your Internet browser. The access point 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 access point'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. [Figure 2-4](#) shows the Summary Status page.

Figure 2-4 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 2-5](#) shows the Express Setup page.

Figure 2-5 Express Setup Page

HOME Hostname ap ap uptime is 2 days, 23 hours, 31 minutes

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Express Set-Up

System Name:

MAC Address: 0005.9a38.42c0

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 Root Repeater Non-Root

Optimize Radio Network for: Throughput Range [Custom](#)

Aironet Extensions: Enable Disable

Radio1-802.11A

Role in Radio Network: Access Point Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Default [Custom](#)

Aironet Extensions: Enable Disable

Apply Cancel

111857

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

- **System Name**— The system name, while not an essential setting, helps identify the access point on your network. The system 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 access point 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 access points, make sure a unique portion of the system name appears in the first 15 characters.

**Note**

When you change the system name, the access point 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 access point uses a static IP address that you enter in the IP address field.
- **IP Address**—Use this setting to assign or change the access point’s IP address. If DHCP is enabled for your network, leave this field blank.



Note If the access point’s IP address changes while you are configuring the access point using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the access point. If you lose your connection, reconnect to the access point using its new IP address. Follow the steps in the [“Resetting the Access Point to Default Settings”](#) section on page 2-2 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 access point on your network. Select **Access Point (Root)** if your access point is connected to the wired LAN. Select **Repeater (Non-Root)** if it is not connected to the wired LAN.
- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the access point radio or customized settings for the access point radio.
 - **Throughput**—Maximizes the data volume handled by the access point but might reduce its range.
 - **Range**—Maximizes the access point’s range but might reduce throughput.
 - **Custom**—The access point uses 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. If you changed the IP address, you lose your connection to the access point. Browse to the new IP address to reconnect to the access point.

Your access point 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 2-1 lists the default settings for the settings on the Express Setup page.

Table 2-1 *Default Settings on the Express Setup Page*

Setting	Default
System Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; if DHCP is disabled, the default setting is 10.0.0.1
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 (root)
Optimize Radio Network for	Throughput
Aironet Extensions	Enable
SNMP Community	defaultCommunity

Configuring Basic Security Settings

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point 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 2-6 shows the Express Security page.

Figure 2-6 Express Security Page

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:

Apply Cancel

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	tsunami	none	none	open	none		<input checked="" type="checkbox"/>

111856

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

When the access point configuration is at factory defaults, the first SSID that you create using the Express security page overwrites the default SSID, *tsunami*, which has no security settings. The SSIDs that you create appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the access point. On dual-radio access points, the SSIDs that you create are enabled on both radio interfaces.

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

Table 2-2 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 access point based on MAC address (see the “Using MAC Address ACLs to Block or Allow Client Association to the Access Point” section on page 16-5) or, if your network does not have a RADIUS server, consider using an access point as a local authentication server (see Chapter 8, “Configuring an Access Point as a Local Authenticator”).	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the access point’s key.

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

Security Type	Description	Security Features Enabled
EAP Authentication	This option enables 802.1x authentication (such as LEAP, PEAP, EAP-TLS, EAP-GTC, EAP-SIM, and others) and requires you 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.	Mandatory 802.1x authentication. Client devices that associate using this SSID must perform 802.1x authentication.
WPA	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. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable.

Express Security Limitations

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

- 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 access point. 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 access point 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 access point. 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 access point unless their SSID matches this SSID. Only one SSID can be included in the access point 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 2-12 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 2-14](#)
- [Example: Static WEP, page 2-15](#)
- [Example: EAP Authentication, page 2-16](#)
- [Example: WPA, page 2-18](#)

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:

```

interface Dot11Radio0
 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 Dot11Radio0.30
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 Dot11Radio1
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 Dot11Radio1.30
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
 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 Dot11Radio0.40
    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
```

Using the IP Setup Utility

IPSU enables you to find the access point's IP address when it has been assigned by a DHCP server. You can also use IPSU to set the access point's IP address and SSID if they have not been changed from the default settings. This section explains how to install the utility, how to use it to find the access point's IP address, and how to use it to set the IP address and the SSID.



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 access point's IP address is to look on the Status screen in the Aironet Client Utility on a client device associated to the access point.

Obtaining IPSU

IPSU is available on the Cisco web site. Click this link to browse to the Software Center on Cisco.com:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

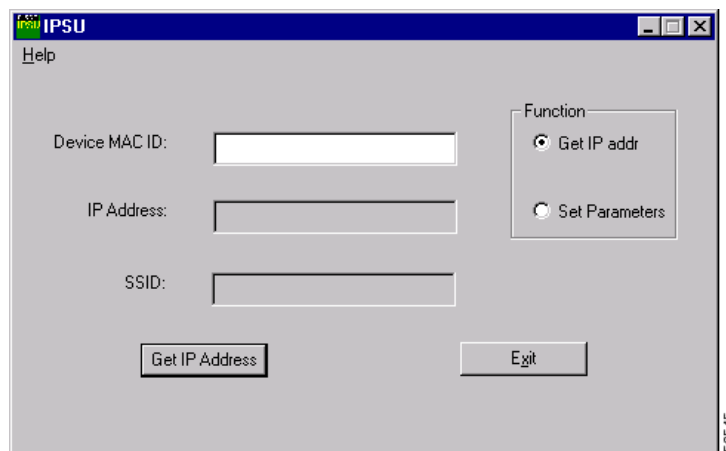
You can find IPSU in the Software Display Tables for access points that run Cisco IOS software.

Using IPSU to Find the Access Point's IP Address

If your access point 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 access point MAC address, you must run IPSU from a computer on the same subnet as the access point. Follow these steps to find the access point's IP address:

- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see [Figure 2-7](#)).

Figure 2-7 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 access point's MAC address in the Device MAC ID field. The access point's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point's MAC address might look like the following example:

000164xxxxxx



Note The MAC address field is not case-sensitive.

- Step 4** Click **Get IP Address**.
- Step 5** When the access point's IP address appears in the IP Address field, write it down.

If IPSU reports that the IP address is 10.0.0.1, the default IP address, then the access point did not receive a DHCP-assigned IP address. To change the access point IP address from the default value using IPSU, refer to the “Using IPSU to Set the Access Point’s IP Address and SSID” section on page 2-21.

Using IPSU to Set the Access Point’s IP Address and SSID

If you want to change the default IP address (10.0.0.1) of the access point, you can use IPSU. You can also set the access point’s SSID at the same time.



Note

IPSU can change the access point’s IP address and SSID only from their default settings. After the IP address and SSID have been changed, IPSU cannot change them again.



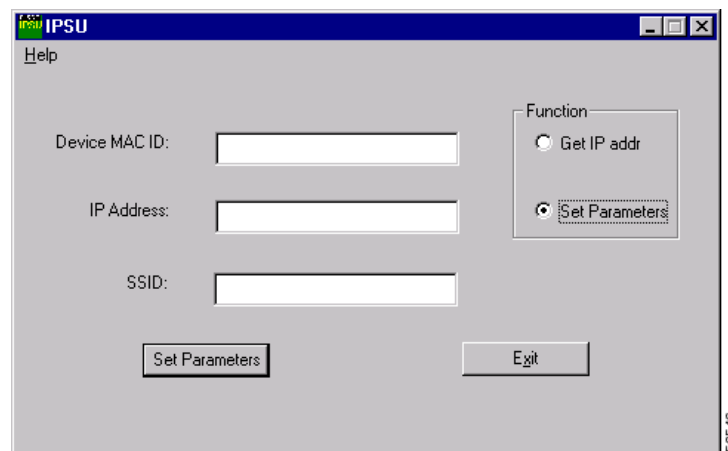
Note

The computer you use to assign an IP address to the access point must have an IP address in the same subnet as the access point (10.0.0.x).

Follow these steps to assign an IP address and an SSID to the access point:

- Step 1** Double-click the **IPSU** icon on your computer desktop to start the utility.
- Step 2** Click the **Set Parameters** radio button in the Function box (see [Figure 2-8](#)).

Figure 2-8 IPSU Set Parameters Screen



- Step 3** Enter the access point’s MAC address in the Device MAC ID field. The access point’s MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your access point’s MAC address might look like this example:

004096xxxxxx



Note

The MAC address field is not case-sensitive.

Step 4 Enter the IP address you want to assign to the access point in the IP Address field.

Step 5 Enter the SSID you want to assign to the access point in the SSID field.



Note You cannot set the SSID without also setting the IP address. However, you can set the IP address without setting the SSID.

Step 6 Click **Set Parameters** to change the access point's IP address and SSID settings.

Step 7 Click **Exit** to exit IPSU.

Assigning an IP Address Using the CLI

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

When you assign an IP address to the access point 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 access point'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 <i>address</i> <i>mask</i>	Assign an IP address and address mask to the BVI. Note If you are connected to the access point using a Telnet session, you lose your connection to the access point when you assign a new IP address to the BVI. If you need to continue configuring the access point using Telnet, use the new IP address to open another Telnet session to the access point.

Using a Telnet Session to Access the CLI

Follow these steps to browse to access the CLI 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 access point's IP address.

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