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:

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
- An 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" section on page 22-13.

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.

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 2-4
  - Connecting to the 1100 Series Access Point Locally, page 2-5
  - Connecting to the 1130AG Series Access Point Locally, page 2-5
  - Connecting to the 1200 Series Access Points Locally, page 2-6.

  - Connecting to the 1240AG Series Access Point Locally, page 2-6

- 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 2-4 or in the "Connecting to the 1200 Series Access Points Locally" section on page 2-6 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/cisco/software/navigator.html

Default IP Address Behavior

When you connect a 350, 1130AG, 1200, or 1240AG series access point 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.

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, try 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 is configured with 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 2-7. If you make a mistake and need to start over, follow the steps in the "Resetting the Device 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 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 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 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, try Xon/Xoff flow control.

Connecting to the 1200 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, try Xon/Xoff flow control.

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, try Xon/Xoff flow control.

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:

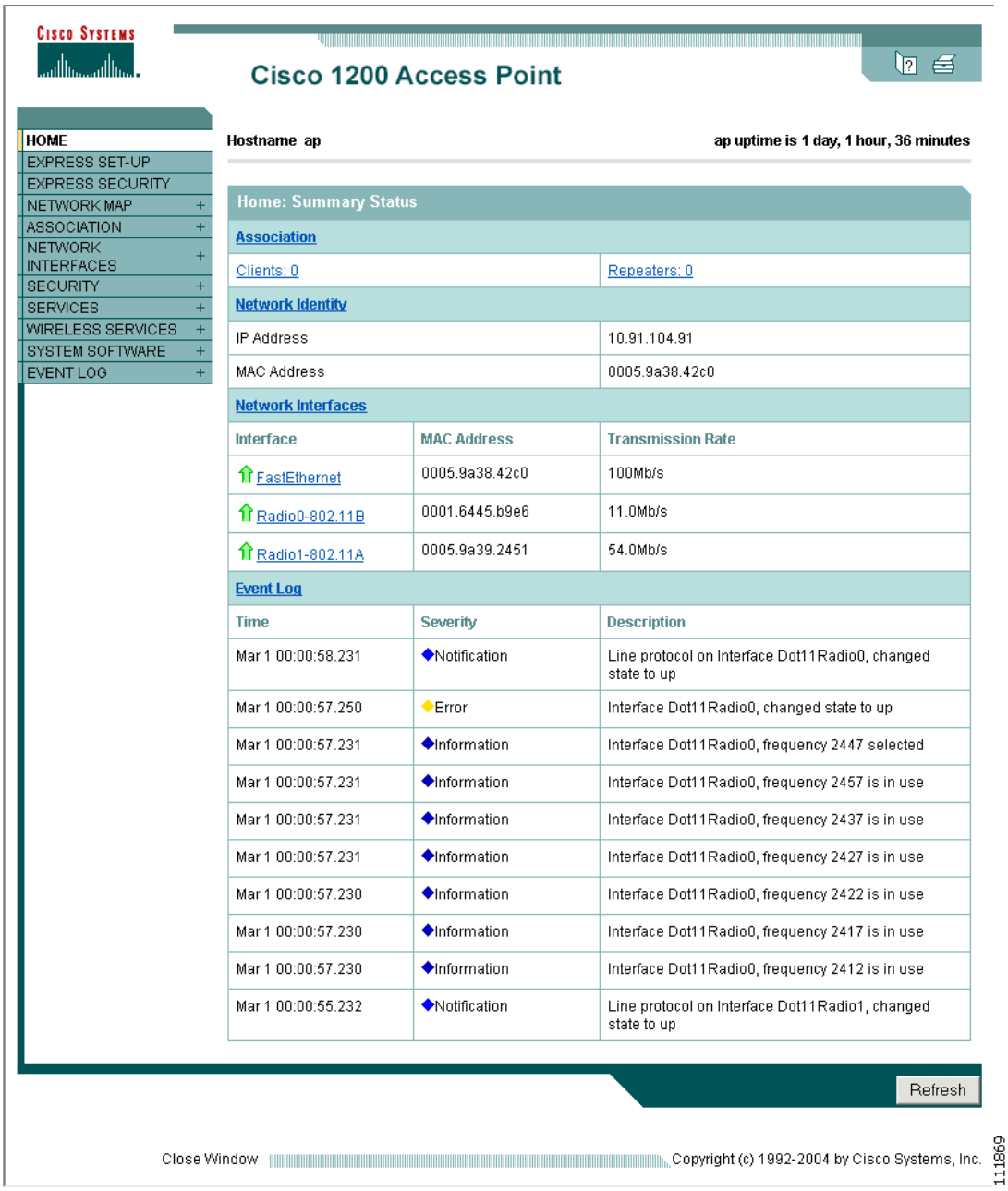
Step 1 Open your Internet browser. The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.

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 2-1.

Figure 2-1 Summary Status Page



Step 5 Click **Express Setup**. The Express Setup screen appears. Figure 2-2 shows the Express Setup page for the 1100 and 1130AG access points.

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

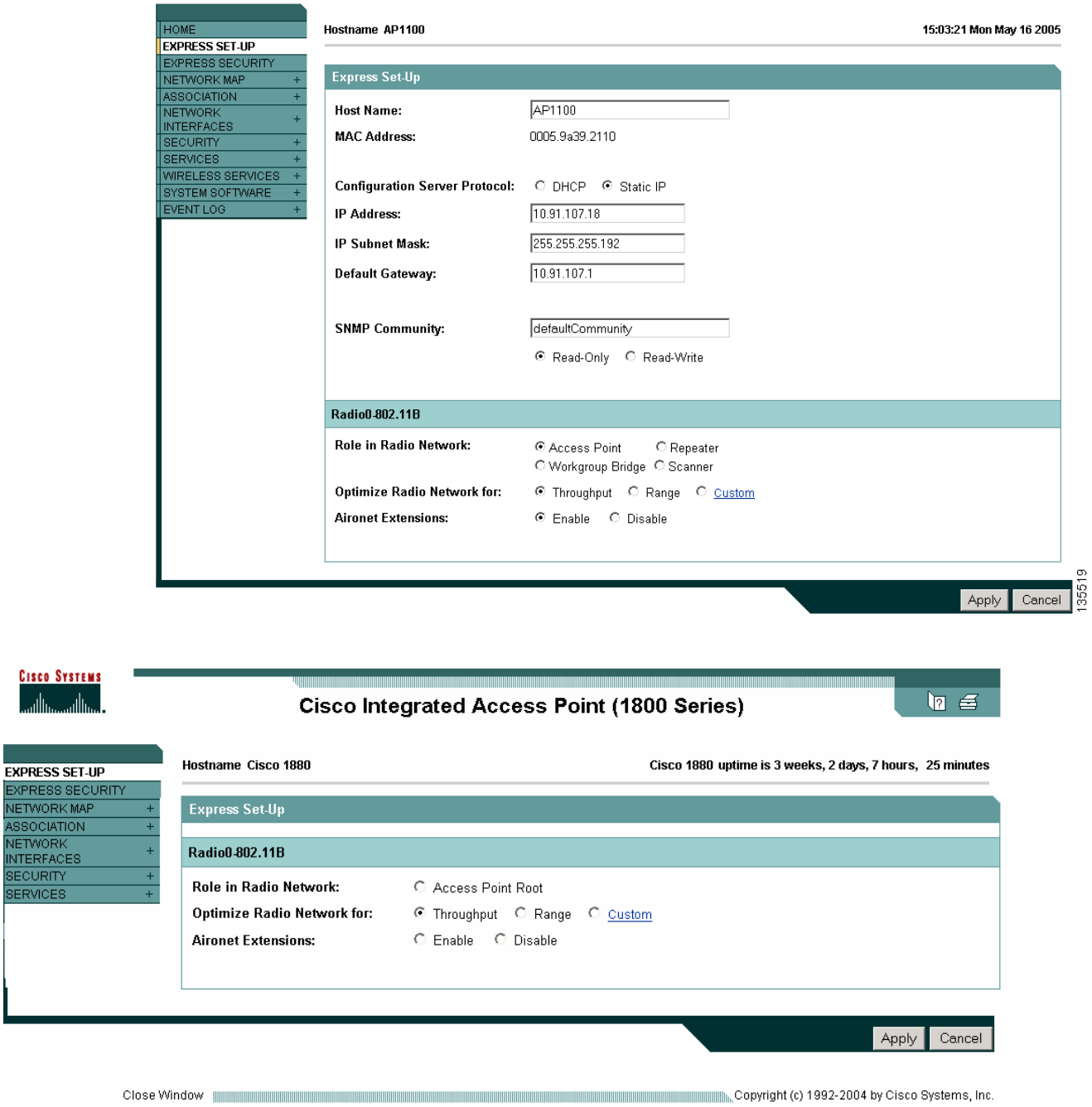
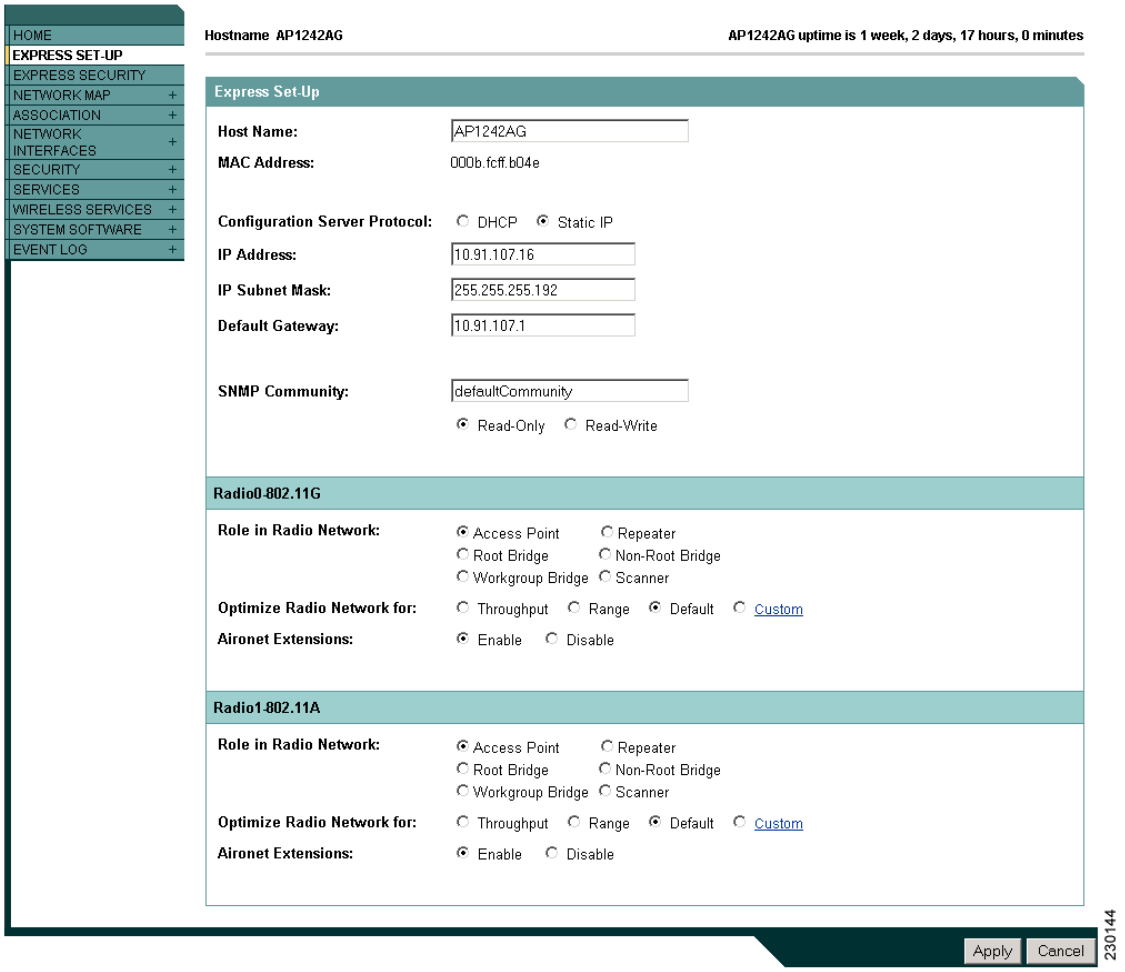


Figure 2-3 Express Setup Page for 1200 and 1240AG Series Access Points



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 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 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.The only role supported on the Airlink is root.
  - **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.
  - **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. This setting is available for the 1100, 1130AG, 1200, and 1240AG 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 Aironetwireless 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 2-1 lists the default settings for the settings on the Express Setup page.

Table 2-1 Default Settings on the Express Setup Page

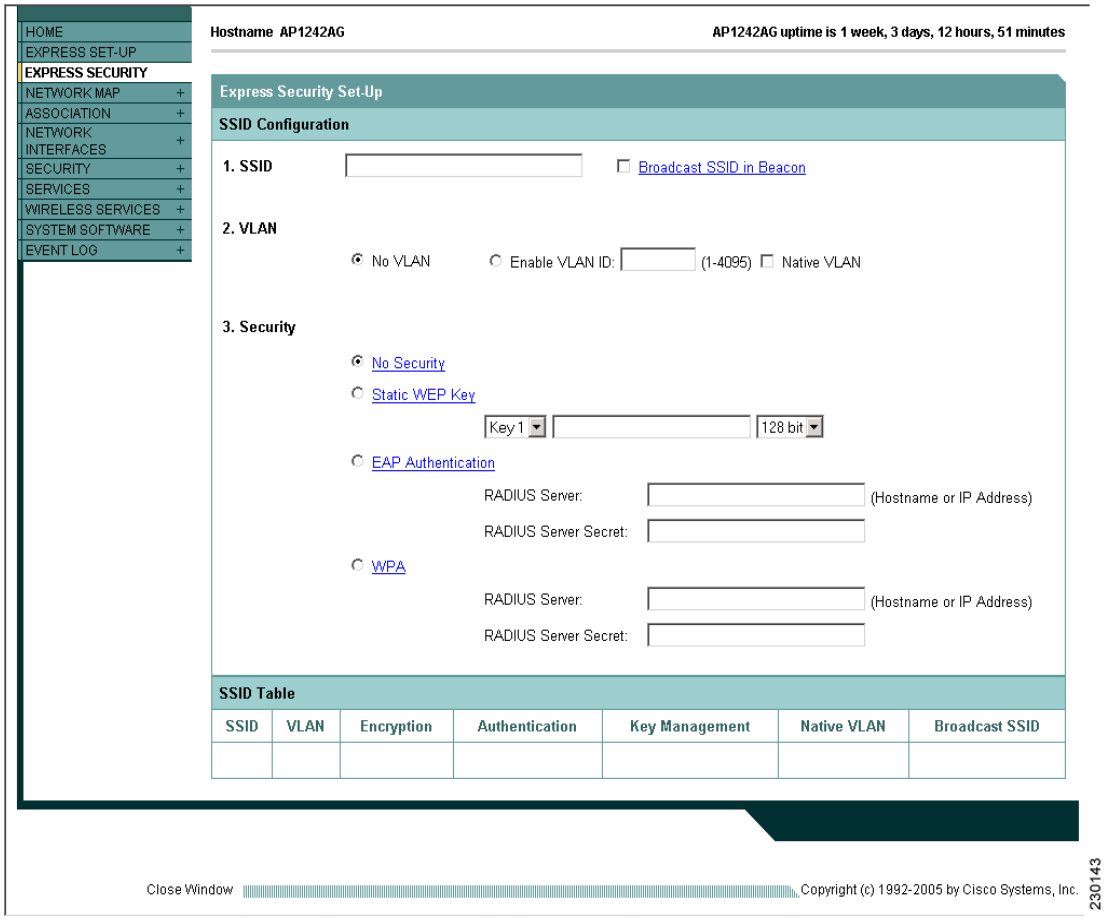
Setting	Default
Host Name	ap
Optimize Radio Network for	Throughput
Aironet Extensions	Enable

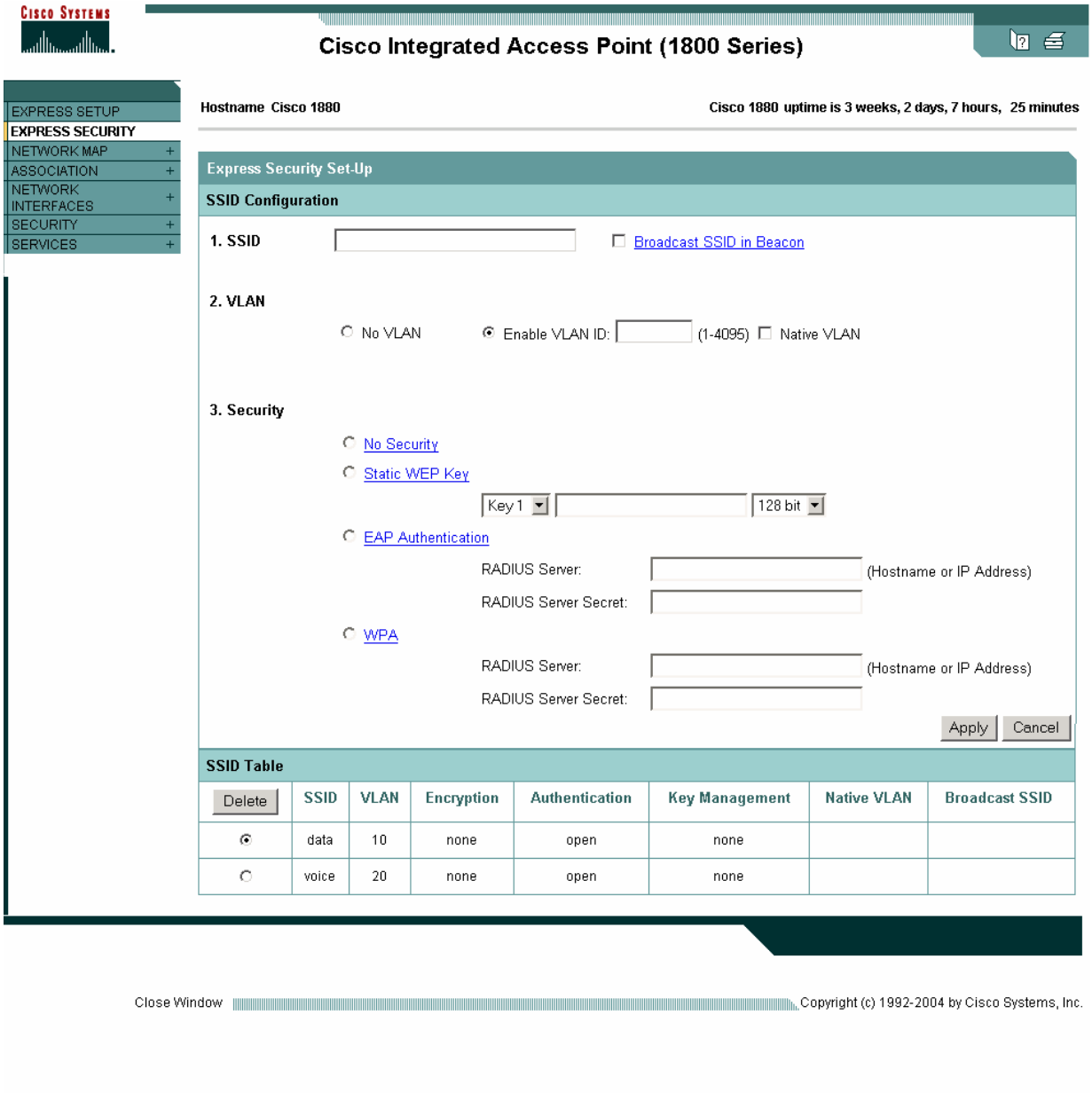
Configuring Basic Security Settings

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 2-4 shows the Express Security page.

Figure 2-4 Express Security Page





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(7)JA, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

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 wireless device based on MAC address.	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the wireless device 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 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 2-15 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

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 Dot11Radio0/1
 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 Dot11Radio0/1.10
 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 Dot11Radio1/1
 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 Dot11Radio1/1.10
 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 Dot11Radio0/1
 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 Dot11Radio0/1.20
 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 Dot11Radio1/1
 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 Dot11Radio1/1.20
 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 Dot11Radio0/1
 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 2-5 shows the System Power Settings section of the System Configuration page.

Figure 2-5 Power Options on the System Software: System Configuration Page

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:

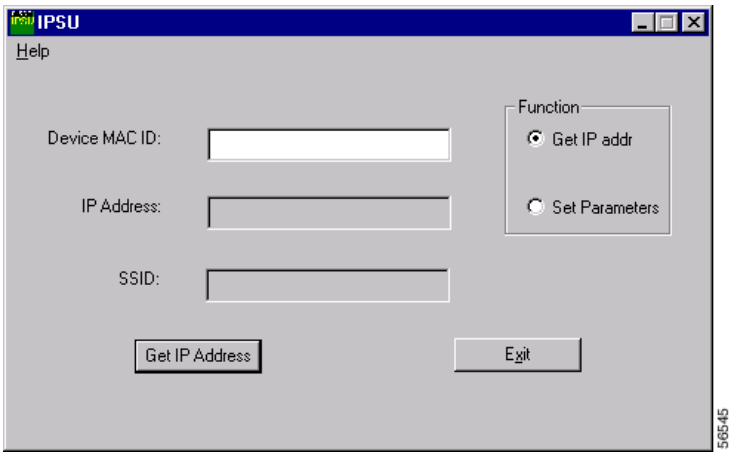
http://www.cisco.com/cisco/software/navigator.html

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 2-6).

Figure 2-6 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. **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.

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**.