
# 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 web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

**Note** 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:

- 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

**Note** Using the MODE button for resetting to default settings applies only to autonomous mode access points and not to lightweight mode access points.

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.

## Resetting to Default Settings Using the GUI

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

**Step 1** Open your Internet browser.
The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 9.0 and Mozilla Firefox version 17.

**Step 2** Enter the wireless device 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 **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 **write default-config**.

**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 protocal 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), from privileged EXEC mode. To obtain the new IP address for an access point/bridge, you can use the *show interface bvi1* CLI command.

# Logging into the Access Point

A user can login to the access point using one of the following methods:

- graphical user interface (GUI)
- Telnet (if the AP is configured with an IP address)
- console port

**Note** Not all models of Cisco Aironet Access Points have the console port. If the access point does not have a console port, use either the GUI or the Telnet for access.

For information on logging into the AP through the GUI, refer to Using the Web-Browser Interface for the First Time, page 2-2.

For information on logging into the AP through the CLI refer to Accessing the CLI, page 3-9.

For information on logging into the AP through a console port refer to Connecting to an Access Point Locally, page 4-5.

# Obtaining and Assigning an IP Address

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

- 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 console port:
  - Connecting to an Access Point Locally, page 4-5.
  - Connecting to the 1550 Series Access Point Locally, page 4-5

**Note** In some terminal emulator applications you may need to set the Flow control parameter to Xon/Xoff. If you are not able to console into the device with the flow control value set to none, try changing the flow control value to Xon/Xoff.

- 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:
  - 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 an Access Point Locally" section on page 4-5 to connect to the console port.
  - Provide your network administrator with the wireless device 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 MAC address is on label attached to the bottom of the access point.

## Default IP Address Behavior

When you connect a 1040, 1140, 1260, 2600 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.

# Connecting to an Access Point Locally

**Note** The following applies to all APs except the 1550 series APs.

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

**Step 3** When connected, press **enter** or type **en** to access the command prompt. Pressing **enter** takes you to the user exec mode. Entering **en** prompts you for a password, then takes you to the privileged exec mode. The default password is *Cisco* and is case-sensitive.

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

# Connecting to the 1550 Series Access Point Locally

If you need to configure the access point locally (without connecting 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 Ethernet port the same 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 on the access point/bridge.

**Step 5** Follow the steps in the "Assigning Basic Settings" section on page 4-6. If you make a mistake and need to start over, follow the steps in the "Resetting the Device to Default Settings" procedure on page 4-1.

**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.

# Default Radio Settings

Beginning with Cisco IOS Release 12.3(8)JA, access point radios are disabled and no default SSID is assigned. This was done in order to prevent unauthorized users to access a customer wireless network through an access point having a default SSID and no security settings. You must create an SSID before you can enable the access point radio interfaces.

# Assigning Basic Settings

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

**Step 1** Open your Internet browser.

**Step 2** Enter the wireless device 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.

**Step 5** Click **Easy Setup**.
The Express Setup screen appears.

**Step 6** Click **Network Configuration**.

**Step 7** Enter the **Network Configuration** settings which 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 that 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.

- **Server Protocol**—Click the radio button that matches the network method of IP address assignment.
  - **DHCP**—IP addresses are automatically assigned by your network 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 IP address. If DHCP is enabled for your network, leave this field blank.

**Note** If the wireless device 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 4-1 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.
- **IPv6 ProtocolP**—Specify the protcols to be applied, by selecting the required check boxes. You can select:
  - DHCP
  - Autoconfig
  - Static IP
- **IPv6 Address**—Enter the IPv6 address
- **Username**—Enter the username required to access the network.
- **Password**—Enter the password corresponding to the username required to access the network.
- **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).
- **Current SSID List (Read Only)**

**Step 8** Enter the following **Radio Configuration** settings for the radio bands supported by the access point. Both the 2.4 GHz and 5 GHz radios have the following options:

- **SSID**—Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.
  - **Broadcast SSID in Beacon**—To allow devices without a specified SSID to associate with the access point, select this check box. If this check box is selected, the access point will respond to Broadcast SSID probe requests and also broadcast its own SSID with its Beacons. 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.
- **VLAN**—To enableVLAN for the radio, click the **Enable VLAN ID** radio button and then enter a VLAN identifier ranging from 1- 4095. To specify this as the native VLAN, check the **Native VLAN** check box. To disable VLAN, click the **No VLAN** radio button.
- **Security**—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 (the RADIUS Server IP address) and shared secret (RADIUS Server 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 4-11 for details.

  - **No Security**—This security setting does not use an encryption key or key management, and uses open authentication.
  - **WEP Key**—This security setting uses mandatory WEP encryption, no key management and open authentication. You can specify up to four WEP keys, i.e. Key 1, 2, 3, and 4. Enter each key value, and specify whether it is 128 bit or 40 bit.
  - **EAP Authentication**—The Extensible Authentication Protocols (EAP) Authentication permits wireless access to users authenticated against a database through the services of an authentication server then encrypts the authenticated and authorized traffic. Use this setting for LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1x/EAP based protocols. This setting uses mandatory encryption WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645. Specify the RADIUS Server and the RADIUS Server Secret.
  - **WPA**—The Wi-Fi Protected Access (WPA) security setting permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their authenticated and authorized IP traffic with stronger algorithms than those used in WEP. Make sure clients are WPA certified before selecting this option. This setting uses encryption ciphers tkip, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645. Specify the RADIUS Server and the RADIUS Server Secret.

**Note** To better understand the security settings used here, see "Understanding the Security Settings" section on page 4-11.

- **Role in Radio Network**—Click 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. For information on the roles supported by different APs in a radio network, see Configuring the Role in Radio Network, page 6-3. The following roles are available in a radio network:

  - **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.
  - **Non-Root Bridge**—In this mode, the device establishes a link with a root bridge.
  - **Install Mode**—Places the access point/bridge in auto installation mode so you can align and adjust a bridge link for optimum efficiency.
  - **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.
  - **Universal Workgroup Bridge**—Configures the access point as a workgroup bridge capable of associating with non-Cisco access points.
  - **Client MAC:**—The Ethernet MAC address of the client connected to the universal workgroup bridge. This field appears only in the universal workgroup bridge mode.
  - **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 range but might reduce throughput.
  - **Default**—Sets the default values for the access point.
  - **Custom**—The wireless device uses the settings you enter on the Network Interfaces. Clicking **Custom** takes you to the Network Interfaces.
- **Aironet Extensions**—Enable this setting if there are only Cisco Aironet wireless devices on your wireless LAN.
- **Channel**—The default channel setting for the wireless device radios is least congested; at startup, the wireless device scans for and selects the least-congested channel. For the most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point.
  - For the 2.4 GHz radio, the relevant options are Least-Congested, channel 1-2412, channel 2-2417, channel 3-2422, channel 4-2427, channel 5-2432, channel 6-2437, channel 7-2442, channel 8-2447, channel 9-2452, channel 10-2457, and channel 11-2462.
  - For the 5 GHz radio, the relevant options are Dynamic Frequency selection, channel 36-5180, channel 40-5200, channel 44-5220, channel 48-5240, channel 149-5745, channel 153-5765, channel 157-5785, channel 161-5805, and channel 165-5825.

- **Power**—Choose the power level from the **Power** drop-down list.
  - For the 2.4 GHz radio, the relevant options are Maximum, 22, 19, 16, 13, 10, 7, and 4.
  - For the 5 GHz radio, the relevant options are Maximum, 14, 11, 8, 5, and 2.

**Step 9** Click **Apply** to save your settings.

**Step 10** Click **Network Interfaces** to browse to the Network Interfaces Summary page.

**Step 11** Click the radio interface to browse to the Network Interfaces: Radio Status page.

**Step 12** Click the **Settings** tab to browse to the Settings page for the radio interface.

**Step 13** Click **Enable** to enable the radio.

**Step 14** Click **Apply**.

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

**Note** You can restore 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 Easy 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 4-4 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 |
| IPv6 Protocol | DHCP and Autoconfig |
| SNMP Community | defaultCommunity (Read-only) |
| VLAN | No VLAN |
| Security | No Security |
| Role in Radio Network (for each radio installed) | Access point |
| Optimize Radio Network for | Default |

*Table 4-1 Default Settings on the Express Setup Page (continued)*

| Setting | Default |
|---|---|
| Aironet Extensions | Enable |
| Channel | Least-Congested (for 2.4GHz) and Dynamic Frequency Selection (for 5GHz) |
| Power | Maximum |

# Understanding the Security Settings

You can configure basic security settings in the **Easy Setup > Radio Configuration** section. You can use the options given in this section to create unique SSIDs and assign one of four security types to them.

You can create up to 16 SSIDs on the wireless device. The created SSIDs appear in the **Current SSID List**. On dual-radio wireless devices, the SSIDs that you create are enabled by default on both radio interfaces.

**Note** In Cisco IOS Release 12.4(23c)JA and 12.xxx, 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.

## Security Types for an SSID

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 Chapter 16, "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" 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 key. |

*Table 4-2 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-FAST, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1X/EAP based products)<br><br>This setting uses mandatory encryption, WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645.<br><br>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. | Mandatory 802.1X authentication. Client devices that associate using this SSID must perform 802.1X authentication.<br><br>If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears:<br><br>WARNING:<br>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.<br><br>If you are using the CLI, this warning message appears:<br><br>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured. |
| 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.<br><br>This setting uses encryption ciphers, TKIP, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645.<br><br>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.<br><br>If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears:<br><br>WARNING:<br>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.<br><br>If you are using the CLI, this warning message appears:<br><br>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured. |

## Limitations of Security Settings

The security settings in the Easy Setup Radio Configuration section are designed for simple configuration of basic security. The options available are a subset of the wireless device 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 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.

# CLI Configuration Examples

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



### Example: No Security for Radio 2.4GHz

This example shows a part of the resulting configuration when an SSID called *no_security_ssid* is created, the SSID is included in the beacon, assigned to VLAN 10, and then VLAN 10 is selected as the native VLAN:

```
!
dot11 ssid no_security_ssid
   vlan 10
   authentication open
   guest-mode
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 ssid no_security_ssid
 !
 antenna gain 0
 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 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 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 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
!
```

### Example: Static WEP for Radio 2.4 GHz

This example shows a part of the configuration that results from creating 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:

```
!
dot11 ssid static_wep_ssid
   vlan 20
   authentication open
!
!
!
encryption vlan 20 key 3 size 128bit 7 76031220D71D63394A6BD63DE57F transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 E55F05382FE2064B7C377B164B73 transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio1.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio1.31
encapsulation dot1Q 31 native
```

```
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface GigabitEthernet0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
no bridge-group 20 source-learning
!
interface GigabitEthernet0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
```

#### Example: EAP Authentication

This example shows a part of the configuration that results from creating 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 do not 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.

```
dot11 ssid eap_ssid
   vlan 30
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
dot11 guest
!
username apuser password 7 096F471A1A0A
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
```

```
 !
 antenna gain 0
 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
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 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
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
```

```
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 00271A150754
!
bridge 1 route ip
```

### Example: WPA2 for Radio 2.4GHz

This example shows a part of the configuration that results from creating 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 name 10.10.11.100
!
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 accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
!
dot11 ssid wpa_ssid
   vlan 40
   authentication open eap eap_methods
   authentication network-eap eap_methods
    authentication key-management wpa version 2
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
encryption vlan 40 mode ciphers aes-ccm
 !
 ssid wpa_ssid
```

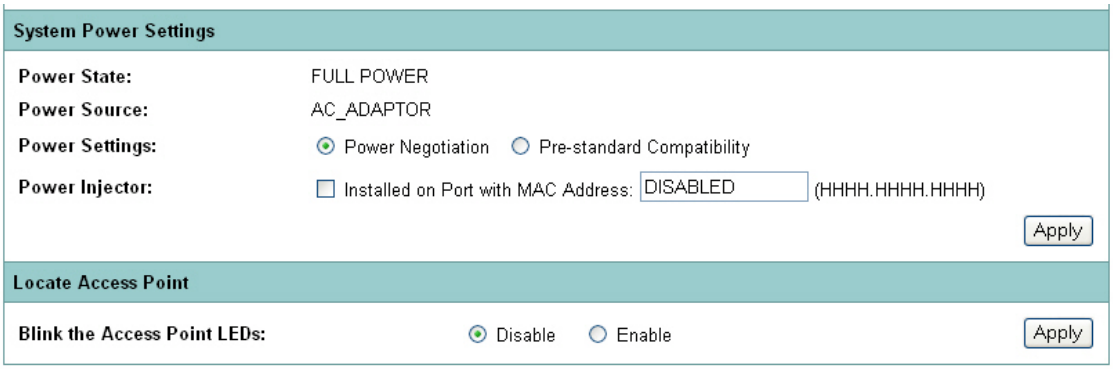
```
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 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
!
interface Dot11Radio1.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 spanning-disabled
 no bridge-group 40 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
```

```
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 0....F175804
!
```

# Configuring System Power Settings Access Points

The AP 1040, AP 802, AP 1140, AP 1550, AP 1600, AP 2600, AP 3500, AP 3600 and AP 1260 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. Choose the **Software > System Configuration** page on the web-browser interface, and then select a power option. Figure 4-1 shows the System Power Settings section of the System Configuration page.

***Figure 4-1 Power Options on the System Software: System Configuration Page***




## Using the AC Power Adapter

If you use the AC power adapter to provide power 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 1040, 1140, and 1260 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 1040, or 1140 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 1040, 1140, or 1260 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.

### dot11 extension power native Command

When enabled, the **dot11 extension power native** shifts the power tables the radio uses from the IEEE 802.11 tables to the native power tables. The radio derives the values for this table from the NativePowerTable and NativePowerSupportedTable of the CISCO-DOT11-1F-MIB. The Native Power tables were designed specifically to configure powers as low as -1dBm for Cisco Aironet radios that support these levels.

## Support for 802.11ac

802.11ac is the next generation wireless standard of 802.11. It is designed to provide high throughput and operate in the 5 GHz band. 802.11ac is supported on the 3700, 2700, and 1700 series access points. The 802.11ac radio depends on the 802.11n radio to be fully functional. Shutting down the 802.11n radio will affect the 802.11ac functionalities.

## Channel Widths for 802.11ac

802.11n and 802.11ac radios operate in the same band. However the channel widths can be independently configured with the restriction that it should be above the channel width configured on 802.11n. Please see Table 4-3 for more details on the supported channel width combinations.

*Table 4-3 Supported Channel Width Combinations*

| 802.11n Channel Bandwidth | 802.11ac Channel Bandwidth |
|---|---|
| 20 | 20 |
| 20 | 40 |
| 20 | 80 |
| 40 | 40 |
| 40 | 80 |

Off channel scanning or transmissions are not supported. The 802.11ac radio depends on 802.11n radios for the off channel scanning functionality.

For example, to configure 80 Mhz channel width:

```
ap# configure terminal
ap(config)# interface dot11Radio 1
```

```
ap(config-if)# channel width 80
ap(config-if)# end
```

# Power Management for 802.11ac

The 3700, 2700, and 1700 802.11ac series access points can be powered by a Power-over-Ethernet (PoE) sources, local power, or a power injector. If the AP is powered by PoE, based on the whether the source is PoE+ (802.3at) or PoE (802.3af), the AP will adjust certain radio configurations as it may require more power than provided by the inline power source.

For example, a 3700 series AP which is powered by PoE+ (802.3at) will provide 4x4:3 configuration on both radios, and when powered by PoE (802.3af) it will provide a 3x3:3 configuration on both radios. Please refer to the below table.

**Tip** Radio configurations such as 4x4:3 imply 4 transmitters and 4 receivers capable of 3 spatial streams

**Note** To determine whether the AP is running at high PoE power or reduced (15.4W) power, in the AP's GUI, got to the Home page. If the AP is running on reduced power, under **Home:Summary Status**, the following warning is displayed:

*Due to insufficient inline power. Upgrade inline power source or install power injector.*

All access points except outdoor mesh products can be powered over Ethernet. Access points with two radios powered over Ethernet are fully functional and support all the features. See Table 4-4 for the various power management options available.

***Table 4-4 Inline Power Options based on Power Sources***

| Power Draw | Description | AP Functionality | PoE Budget (Watts)[1] | 802.3af | E-PoE | 802.3at PoE+ PWRINJ4 |
|---|---|---|---|---|---|---|
| PoE + 802.3at | AP3700 Out of the box | 4x4:3 on 2.4/5 GHz | 16.1 | No | Yes | Yes |
| PoE 802.3af | AP3700 Out of the box | 3x3:3 on 2.4/5 GHz | 15.4 | Yes | N/A | N/A |
| PoE 802.3at | AP2700 Out of the Box | 3x4:3 on 2.4/5 GHz and Auxillary Ethernet Port Enabled | 16.8 | No | No | Yes |
| PoE 802.3af | AP2700 Out of the Box | 3x4:3 on 5 GHz and 2x2:2 on 2.4 GHz and Auxiliary Ethernet Port Enabled | 15.4 | Yes | Yes | N/A |

1. This is the power required at the PSE, which is either a switch or an injector.

802.11n and 802.11ac use the power levels configured on 802.11n. You cannot configure power levels independently for 802.11ac.

# 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 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 BVI:

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enters global configuration mode. |
| Step 2 | **interface bvi1** | Enters interface configuration mode for the BVI. |
| Step 3 | **ip address** *address mask* | Assigns an IP address and address mask to the BVI.<br>**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** Choose **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 lists. To start the Telnet session in Windows 2000, type **open** followed by the wireless device IP address.

**Step 3** In the Host Name field, type the wireless device 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.

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** *profile* | Creates a dot1x credentials profile and enters the dot1x credentials configuration submode. |
| **Step 3** | **anonymous-id** *description* | (Optional)—Enter the anonymous identity to be used. |
| **Step 4** | **description** *description* | (Optional)—Enter a description for the credentials profile |
| **Step 5** | **username** *username* | Enter the authentication user id. |
| **Step 6** | **password {0 \| 7 \| LINE}** | Enter an unencrypted password for the credentials.<br>**0**—An unencrypted password will follow.<br>**7**—A hidden password will follow. Hidden passwords are used when applying a previously saved configuration.<br>**LINE**—An unencrypted (clear text) password.<br>**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** *pki-trustpoint* | (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*:

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

```
ap(config-dot1x-creden)#exit
ap(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 wired port:

| | Command | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enter global configuration mode. |
| **Step 2** | **interface gigabitethernet 0** | Enter the interface configuration mode for the access point Gigabit Ethernet port.<br>**Note** You can also use **interface fa0** to enter the Gigabit Ethernet configuration mode. |
| **Step 3** | **dot1x credentials** *profile name* | 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 gigabit Ethernet port:

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap(config)#interface Gig0
ap(config-if)#dot1x credentials test
ap(config-if)#end
```

## 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** *ssid* | Enter the 802.11 SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.<br>**Note** The first character cannot contain the !, #, or; character.<br>+,], /, ", TAB, and trailing spaces are invalid characters for SSIDs. |
| **Step 3** | **dot1x credentials** *profile* | 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 applys 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)#dot11 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 the "Creating and Applying EAP Method Profiles for the 802.1X Supplicant" section on page 11-17.

# Configuring IPv6

IPv6 is the latest Internet protocol for IPv, developed to provide an extremely large number of addresses. It uses 128 bit addresses instead of the 32 bit addresses that are used in IPv4.

As deployments in wireless networks use greater number of IP wireless devices and smart phones, IPv6 with its 128-bit address format can support 3.4 x 1038 address space.

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x.

There are three types of IPv6 address types:

- Unicast

  The Cisco IOS software supports these IPv6 unicast address types:

  - Aggregatable Global Address

    Aggregatable global unicast addresses are globally routable and reachable on the IPv6 portion of the Internet. These global addresses are identified by the format prefix of 001.

  - Link-Local Address

Link-Local Addressses are automatically configured on interface using link-local prefix FE80::/10 (1111 1110 10). The interface identifier is in the modified EUI-64 format.

- Anycast can be used only by a router and not the host. Anycast addresses must not be used as the source address of an IPv6 packet.
- Multicast address is a logical identifier for a group of hosts that process frames intended to be multicast for a designated network service. Multicast addresses in IPv6 use a prefix of FF00::/8 (1111 1111)

  IPv6 configuration uses these multicast groups:

  - Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104
  - All-nodes link-local multicast group FF02::1
  - All-routers link-local multicast group FF02::2

Table 4-5 lists the IPv6 address types and formats.

***Table 4-5 IPv6 Address Formats***

| IPv6 Address Type | Preferred Format | Compressed Format |
|---|---|---|
| Unicast | 2001:0:0:0:DB8:800:200C:417A | 2001::DB8:800:200C:417A |
| Multicast | FF01:0:0:0:0:0:0:101 | FF01::101 |
| Loopback | 0:0:0:0:0:0:0:1 | ::1 |
| Unspecified | 0:0:0:0:0:0:0:0 | :: |

The following modes are supported

- Root
- Root bridge
- Non Root bridge
- Repeater
- WGB

The following modes are not supported

- Spectrum mode
- Monitor mode

Beginning in privileged EXEC mode, use these commands to enable tie ipv6 address

- ap(config)# **int bv1**
- ap(config-if)# **ipv6 address**

A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.

Beginning in privileged EXEC mode, use the following command to enable stateless autoconfiguration:

ap(config-if)# **ipv6 address autoconfig**

Beginning in privileged EXEC mode, use the following command to configure a link local addreess without assigning any other IPv6 addressesto the interface:

ap(config-if)# **ipv6 address ipv6-address link-local**

Beginning in privileged EXEC mode, use the following command to assign a site-local or global address to the interface:

ap(config-if)# **ipv6 address ipv6-address [eui-64]**

**Note** The optional eui-64 keyword is used to utilize the Modified EUI-64 interface ID in the low order 64 bits of the address.

# Configuring DHCPv6 address

DHCPv6 is a network protocol that is used for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration required to operate on an IPv6 network. The DHCPv6 client obtains configuration parameters from a server either through a rapid two-message exchange (solicit, reply), or through a normal four-message exchange (solicit, advertise, request, reply). By default, the four-message exchange is used. When the rapid-commit option is enabled by both client and server, the two-message exchange is used.

Beginning in privileged EXEC mode, use these commands to enable the DHCPv6 client in an Access Point:

- ap# c**onf t**
- ap(config)**# int bv1**
- ap(config)**# ipv6 address dhcp rapid-commit(optional)**

Autonomous AP supports both DHCPv6 stateful and stateless addressing.

### Stateful addressing

Stateful addressing uses a DHCP server. DHCP clients use stateful DHCPv6 addressing to obtain an IP address.

Beginning in privileged EXEC mode, use this command to configure stateful addressing:

ap(config)**# ipv6 address dhcp**

### Stateless addressing

Stateless addressing does not use a DHCP server to obtain IP addresses. The DHCP clients autoconfigure their own IP addresses based on router advertisments.

Beginning in privileged EXEC mode, use this command to configure stateless addressing:

ap(config)# **ipv6 address autoconfig**

# IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network.

Beginning in privileged EXEC mode, use these commands to configure IPv6 neighbor discovery:

| Command | Purpose |
|---|---|
| **ipv6 nd ?** | Configures neighbor discovery protocol. |
| **ipv6 nd ns-interval** *value* | This command is available only on bridge group virtual interface (BVI).<br>Sets the interval between IPv6 neighbor solicitation retransmissions on an interface. |
| **ipv6 nd reachable-time** *value* | Sets the amount of time that a remote IPv6 node is reachable. |
| **ipv6 nd dad attempts** *value* | This command is available only on bridge group virtual interface (BVI).<br>Configures the number of consecutive neighbor solicitation messages sent when duplicate address detection is performed on the unicast IPv6 addresses. |
| **ipv6 nd dad time** *value* | Configures the interval between IPv6 neighbor solicit transmissions for duplicate address detection. |
| **ipv6 nd autoconfig default-router** | This command is available only on bridge group virtual interface (BVI).<br>Configures a default route to the Neighbor Discovery-derived default router. |
| **ipv6 nd autoconfig prefix** | This command is available only on bridge group virtual interface (BVI).<br>Configures router solicitation message to solicit a router advertisement to eliminate any delay in waiting for the next periodic router advertisement. |
| **ipv6 nd cache expire** *expire-time-in-seconds* | Configures the length of time before the IPv6 neighbor discovery cache entry expires. |
| **ipv6 nd cache interface-limit size** [log rate] | Configures a neighbor discovery cache limit on a specified interface. |
| **ipv6 nd na glean** | This command is available only on bridge group virtual interface (BVI).<br>Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement. |
| **ipv6 nd nsf** {**convergence** *time-in-seconds*\| **dad** [**suppress**]\| **throttle** *resolutions*} | Configures IPv6 neighbor discovery non-stop forwarding. You can specify the covergence time in seconds (10 to 600 seconds), suppress duplicate address detection (DAD), or set the number of resolutions to use with non-stop forwarding (NSF). |
| **ipv6 nd nud limit** *limit* | Configures the number of neighbor unreachability detection (NUD) resends, and set a limit to the number of unresolved resends. |
| **ipv6 nd resolution data limit** *limit-in-packets* | Configures a limit to the number of data packets in queue awaiting neighbor discovery (ND) resolution. |
| **ipv6 nd route-owner** | Inserts Neighbor Discovery-learned routes into the routing table with "ND" status and enables ND autoconfiguration behavior. |

# Configuring IPv6 Access Lists

IPv6 access lists (ACL) are used to filter traffic and restrict access to the router. IPv6 prefix lists are used to filter routing protocol updates.

Beginning in privileged EXEC mode, use these commands to to configure the access list globally and assign it to interface:

- ap(config)# **ipv6 access-list** *acl-name*

Beginning in privileged EXEC mode, you can use the command given in Table 4-6 for IPv6 Access List configuration.

***Table 4-6 IPv6 Access List configuration commands***

| Command | Purpose |
|---|---|
| **default** | Set a command to its defaults. |
| **deny** | Specify packets to reject. |
| **evaluate** | Evaluate an access list. |
| **exit** | Exit from access-list configuration mode. |
| **no** | Negate a command or set its defaults. |
| **permit** | Specify packets to forward. |
| **remark** | Set an access list entry comment. |
| **sequence** | Set a sequence number for this entry. |

Beginning in privileged EXEC mode, use these commands to assign the globally configured ACL to the outbound and inbound traffic on layer3 interface:

- ap(config)# **interface** *interface*
- ap(config)# **ipv6 traffic-filter** *acl-name* **in/out**

# RADIUS Configuration

RADIUS server is a background process serving three functions:

- Authenticate users before granting them access to the network
- Authorize users for certain network services
- Account for the usage of certain network services

See Controlling Access Point Access with RADIUS, page 5-12.

# IPv6 WDS Support

The WDS and the infrastructure access points communicate over a multicast protocol called WLAN Context Control Protocol (WLCCP).

Cisco IOS Release 15.2(4)JA supports communication between the WDS and Access Point through IPv6 addresses. The WDS works on a Dual Stack; that is, it accepts both IPv4 and IPv6 registeration.

### IPv6 WDS AP registration

The first active IPv6 address is used to register the WDS. Table 4-7 shows different scenarios in the IPv6 WDS AP registration process.

*Table 4-7 IPv6 WDS–AP Registration*

| Scenario | WDS | | | AP | | | Mode of Communication |
|---|---|---|---|---|---|---|---|
| | Dual | IPv6 | IPv4 | Dual | IPv6 | IPv4 | |
| 1 | Yes | | | yes | | | IPv6 |
| 2 | Yes | | | | yes | | IPv6 |
| 3 | Yes | | | | | yes | IPv4 |
| 4 | | yes | | yes | | | IPv6 |
| 5 | | yes | | | yes | | IPv6 |
| 6 | | yes | | | | yes | Fails |
| 7 | | | yes | yes | | | IPv4 |
| 8 | | | yes | | yes | | Fails |
| 9 | | | yes | | | yes | IPv4 |

**Note** 11r roaming between IPv4 and IPv6 access points is not supported because the MDIE is different. Both AP and WDS use the first active IPv6 address in BV1 to register and advertise. Link-local is not used for registration.

# CDPv6 Support:

CDP is a layer2 protocol used to get information on the immediate neighbor's device-ID, capabilities, mac address, ip address or duplex. Each CDP enabled device sends information about itself to its immediate neighbor. As part of native IPv6, the access point sends its IPv6 address as well as part of the address TLV in the cdp message; it also parses the IPv6 address information it gets from the neighboring switch.

This command shows the connected IPv6 neighbor:

ap# **show cdp neighbors detail**

## RA filtering

RA filtering increases the security of the IPv6 network by dropping RAs coming from wireless clients. RA filtering prevents misconfigured or malicious IPv6 clients from connecting to the network, often with a high priority that takes precedence over legitimate IPv6 routers. In all cases, the IPv6 RA is dropped at some point, protecting other wireless devices and upstream wired network from malicious or misconfigured IPv6 devices.

However, RA filtering is not supported in the uplink direction.

# Automatic Configuring of the Access Point

The Autoconfig feature of autonomous access points allows the AP to download its configuration, periodically, from a Secure Copy Protocol (SCP) server. If the Autoconfig feaure is enabled, the AP downloads a configuration information file from the server at a pre-configured time and applies this configuration. The next configuration download is also scheduled along with this.

**Note** The AP does not apply a configuration if it is the same as the last downloaded configuration.

## Enabling Autoconfig

To enable Autoconfig:

**Step 1** Prepare a Configuration Information File

**Step 2** Enable environmental variables

**Step 3** Schedule the Configuration Information File Download

### Prepare a Configuration Information File

An Autoconfig-enabled AP downloads the configuration information file from the SCP server. The configuration information file is an XML file, containing the following information:

- The new startup-configuration.
- An Absolute time and a Range value. The AP schedules the next information file download at this absolute time plus a random value between 0 and the range value.

The configuration information file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<l2tp_cfg>
    <cfg_fetch_start_time>Absolute Time</cfg_fetch_start_time>
    <cfg_fetch_time_range>Random Jitter</cfg_fetch_time_range>
    <cfg_fetch_config>
        <![CDATA[
        <Startup config>
        ]]>
    </cfg_fetch_config>
```

```
</l2tp_cfg>
```

The xml tags used in the configuration information file are described below.

| XML Tags | Purpose |
|---|---|
| cfg_fetch_start_time | This tag contains the Absolute Time in the format DAY HH:MM, where:<br>• DAY can be any of these values–Sun, Mon, Tue, Wed, Thu, Fri, Sat, All.<br>• HH, indicates the hour, and can be a number from 0 to 23.<br>• MM, indicates the minute, and can be a number from 0 to 59.<br>Example: “Sun 10:30”, “Thu 00:00”, “All 12:40” |
| cfg_fetch_time_range | A random number of seconds between 0 to this value is added to the start time, to randomize the time when next information file is downloaded. |
| cfg_fetch_config | This tag contains the AP’s next startup configuration. |

## Enable environmental variables

After you have the configuration information file ready and hosted on the SCP server, you need to configure the following environmental variables.

| Environmental Variable | Purpose |
|---|---|
| AUTO_CONFIG_AP_FUNCTIONALITY | To enable Autoconfig, this variable must be set ‘YES’. |
| AUTO_CONFIG_USER | Username for accessing the SCP server |
| AUTO_CONFIG_PASSWD | Password for accessing the SCP server |
| AUTO_CONFIG_SERVER | Hostname/IP of SCP server |
| AUTO_CONFIG_INF_FILE | Name of the configuration information file to be fetched from the SCP server |

You can configure the environmental variables by using the following command in global configuration mode:

dot11 autoconfig add *environment-variable-name* **val** *value.*
For example:

```
dot11 autoconfig add AUTO_CONFIG_SERVER val 206.59.246.199
```

## Schedule the Configuration Information File Download

After setting the environmental variables, you need to schedule the download of the configuration information file from the SCP server. Follow these steps:

**Step 1** The AP's clock time must be in sync with a SNTP (Simple Network Time Protocol) server. You can set the SNTP server using the command, **sntp server** *sntp-server-ip,* where *sntp-server-ip* is the IP address of the SNTP server.

**Step 2** You need to set the correct time zone for the AP to have the correct time, This can be done using the command **clock timezone** *TIMEZONE HH MM,* where:

- TIMEZONE is name of timezone like IST, UTC, or others.
- HH is the Hours offset from the timezone
- MM is the Minutes offset from timezone

**Step 3** For instances where the download of the configuration information file from the SCP server fails, you can set a time interval after which the AP retries to download it again. This retry interval can be set using the command **dot11 autoconfig download retry interval min** *MIN* **max** *MAX***,** where:

- MIN is minimum number of seconds
- MAX is maximum number of seconds between retries. After every failed download, the retry interval doubles, but the retires stop the interval when becomes larger than MAX.

# Enabling Autoconfig via a Boot File

You can enable Autoconfig by also providing the following commands in a boot file as a part of the DHCP IP configuration.

The format of the contents of the boot file returned by the DHCP/BootTP server should be as shown in the following example:

```
dot11 autoconfig add env var AUTO_CONFIG_AP_FUNCTIONALITY val YES
dot11 autoconfig add env var AUTO_CONFIG_USER val someusername
dot11 autoconfig add env var AUTO_CONFIG_PASSWD val somepasswd
dot11 autoconfig add env var AUTO_CONFIG_SERVER val scp.someserver.com
dot11 autoconfig add env var AUTO_CONFIG_INF_FILE val some_inf_file.xml
sntp server 208.210.12.199
clock timezone IST 5 30
dot11 autoconfig download retry interval min 100 max 400
end
```

# Checking the Autoconfig Status

To know the Autoconfig status, use the **show dot11 autoconfig status** command.

**Examples**

```
AP1600-ATT# show dot11 autoconfig status
Dot11 l2tp auto config is disabled

1600-89-absim# show dot11 autoconfig status
Auto configuration download will occur after
45 seconds

1600-89-absim# show dot11 autoconfig status
Trying to download information file from server
```

# Debugging Autoconfig

You can use the following debugging commands as required:

- Debug commands to see Autoconfig state machine transition:
  **Deb dot11 autoconfigsm**
- Debug commands to see Autoconfig events:
  **Deb dot11 autoconfigev**