



## Administering the Wireless Device

---

The following sections describe administration tasks for the wireless device:

### Security on the Wireless Device

- [Disabling the Mode Button Function, page 295](#)
- [Preventing Unauthorized Access to Your Access Point, page 297](#)
- [Protecting Access to Privileged EXEC Commands, page 297](#)
- [Controlling Access Point Access with RADIUS, page 305](#)
- [Controlling Access Point Access with TACACS+, page 310](#)

### Administering the Wireless Device

- [Administering the Wireless Hardware and Software, page 314](#)
- [Resetting the Wireless Device to the Factory Default Configuration, page 314](#)
- [Monitoring the Wireless Device, page 315](#)
- [Managing the System Time and Date, page 315](#)
- [Configuring a System Name and Prompt, page 321](#)
- [Creating a Banner, page 324](#)

### Configuring Wireless Device Communication

- [Configuring Ethernet Speed and Duplex Settings, page 327](#)
- [Configuring the Access Point for Wireless Network Management, page 328](#)
- [Configuring the Access Point for Local Authentication and Authorization, page 328](#)
- [Configuring the Authentication Cache and Profile, page 330](#)
- [Configuring the Access Point to Provide DHCP Service, page 332](#)
- [Configuring the Access Point for Secure Shell, page 335](#)
- [Configuring Client ARP Caching, page 336](#)
- [Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging, page 337](#)

## Disabling the Mode Button Function

You can disable the mode button on the wireless device by using the **[no] boot mode-button** command.



Caution

This command disables password recovery. If you lose the privileged EXEC mode password for the access point after entering this command, you will need to contact the Cisco Technical Assistance Center (TAC) to regain access to the access point command line interface (CLI).



Note

To reboot the wireless device, use the **service-module wlan-ap reset** command from the Cisco IOS CLI. See the [“Rebooting the Wireless Device” section on page 314](#) for information about this command.

The mode button is enabled by default. To disable the access point’s mode button, Follow these steps, beginning in privileged EXEC mode.

SUMMARY STEPS

- 1. **configure terminal**
- 2. **no boot mode-button**
- 3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>no boot mode-button</b>	Disables the access point’s mode button.
Step 3	<b>end</b>	Returns to privileged EXEC mode.
		<b>Note</b> It is not necessary to save the configuration.

You can check the status of the mode button by executing the **show boot** or **show boot mode-button** command in privileged EXEC mode. The status does not appear in the running configuration. The following shows typical responses to the **show boot** and **show boot mode-button** commands:

```
ap# show boot
BOOT path-list: flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap#show boot mode-button
on
ap#
```



Note

As long as the privileged EXEC password is known, you can use the **boot mode-button** command to restore the mode button to normal operation.

# Preventing Unauthorized Access to Your Access Point

You can prevent unauthorized users from reconfiguring the wireless device and viewing configuration information. Typically, the network administrators must have access to the wireless device while restricting access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to the wireless device, configure one of these security features:

- Username and password pairs, which are locally stored on the wireless device. These pairs authenticate each user before the user can access the wireless device. You can also assign a specific privilege level (read only or read/write) to each username and password pair. For more information, see the [“Configuring Username and Password Pairs” section on page 301](#). The default username is *Cisco*, and the default password is *Cisco*. Usernames and passwords are case sensitive.



**Note** The characters TAB, ?, \$, +, and [ are invalid characters for passwords.

- Username and password pairs are stored centrally in a database on a security server. For more information, see the [“Controlling Access Point Access with RADIUS” section on page 305](#).

## Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can issue after they have logged in to a network device.



**Note**

For complete syntax and usage information for the commands used in this section, see *Cisco IOS Security Command Reference for Release 12.4*.

This section describes how to control access to the configuration file and privileged EXEC commands. It contains this configuration information:

- [Configuring Default Password and Privilege Level, page 298](#)
- [Setting or Changing a Static Enable Password, page 298](#)
- [Protecting Enable and Enable Secret Passwords with Encryption, page 299](#)
- [Configuring Username and Password Pairs, page 301](#)
- [Configuring Multiple Privilege Levels, page 302](#)

# Configuring Default Password and Privilege Level

Table 1 shows the default password and privilege level configuration.

Table 1 Default Passwords and Privilege Levels

Privilege Level	Default Setting
Username and password	Default username is <i>Cisco</i> , and the default password is <i>Cisco</i> .
Enable password and privilege level	Default password is <i>Cisco</i> . The default is level 15 (privileged EXEC level). The password is encrypted in the configuration file.
Enable secret password and privilege level	Default enable password is <i>Cisco</i> . The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	Default password is <i>Cisco</i> . The password is encrypted in the configuration file.

## Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.



Caution

The **no enable password** command in global configuration mode removes the enable password, but you should use extreme care when using this command. If you remove the enable password, you are locked out of the privileged EXEC mode.

To set or change a static enable password, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **enable password *password***
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>enable password</b> <i>password</i>	<p>Defines a new password or changes an existing password for access to privileged EXEC mode.</p> <p>The default password is <i>Cisco</i>.</p> <p>For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-V when you create the password; for example, to create the password abc?123, do this:</p> <ol style="list-style-type: none"> <li>1. Enter <b>abc</b>.</li> <li>2. Enter <b>Ctrl-V</b>.</li> <li>3. Enter <b>?123</b>.</li> </ol> <p>When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-V; you can simply enter <b>abc?123</b> at the password prompt.</p> <p><b>Note</b> The characters TAB, ?, \$, +, and [ are invalid characters for passwords.</p>
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

The enable password is not encrypted and can be read in the wireless device configuration file.

The following example shows how to change the enable password to *11u2c3k4y5*. The password is not encrypted and provides access to level 15 (standard privileged EXEC mode access):

```
AP(config)# enable password 11u2c3k4y5
```

## Protecting Enable and Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a TFTP server, you can use either the **enable password** or **enable secret** command in global configuration mode. The commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level that you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

To configure encryption for enable and enable secret passwords, follow these steps, beginning in privileged EXEC mode.

## SUMMARY STEPS

1. **configure terminal**
2. **enable password** [*level level*] {*password* | *encryption-type encrypted-password*}
- or
- enable secret** [*level level*] {*password* | *encryption-type encrypted-password*}
3. **service password-encryption**
4. **end**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>enable password</b> [ <i>level level</i> ] { <i>password</i>   <i>encryption-type encrypted-password</i> }	Defines a new password or changes an existing password for access to privileged EXEC mode.
	or	or
	<b>enable secret</b> [ <i>level level</i> ] { <i>password</i>   <i>encryption-type encrypted-password</i> }	Defines a secret password, which is saved using a nonreversible encryption method.
		<ul style="list-style-type: none"> <li>• (Optional) For <i>level</i>, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).</li> <li>• For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.</li> <li>• (Optional) For <i>encryption-type</i>, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another access point wireless device configuration.</li> </ul>
		<b>Note</b> If you specify an encryption type and then enter a clear text password, you cannot reenter privileged EXEC mode. You cannot recover a lost encrypted password by any method.
Step 3	<b>service password-encryption</b>	(Optional) Encrypts the password when the password is defined or when the configuration is written.  Encryption prevents the password from being readable in the configuration file.
Step 4	<b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** command in global configuration mode to specify commands accessible at various levels. For more information, see the “[Configuring Multiple Privilege Levels](#)” section on page 302.

If you enable password encryption, it applies to all passwords, including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

To remove a password and level, use the **no enable password [level level]** command or the **no enable secret [level level]** command in global configuration mode. To disable password encryption, use the **no service password-encryption** command in global configuration mode.

This example shows how to configure the encrypted password `$1$FaD0$Xyti5Rkls3LoyxzS8` for privilege level 2:

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

## Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the wireless device. These pairs are assigned to lines or interfaces, and they authenticate each user before the user can access the wireless device. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

To establish a username-based authentication system that requests a login username and a password, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **username *name* [privilege *level*] {password *encryption-type password*}**
3. **login local**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>username</b> <i>name</i> [ <b>privilege level</b> ] { <b>password</b> <i>encryption-type password</i> }	Enters the username, privilege level, and password for each user. <ul style="list-style-type: none"> <li>For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed.</li> <li>(Optional) For <i>level</i>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.</li> <li>For <i>encryption-type</i>, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.</li> <li>For <i>password</i>, specify the password the user must enter to gain access to the wireless device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the <b>username</b> command.</li> </ul>
Step 3	<b>login local</b>	Enables local password checking at login time. Authentication is based on the username specified in <a href="#">Step 2</a> .
Step 4	<b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>show running-config</b>	Verifies your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To disable username authentication for a specific user, use the **no username** *name* command in global configuration mode.

To disable password checking and allow connections without a password, use the **no login** command in line configuration mode.

**Note**

You must have at least one username configured, and you must have login local set to open a Telnet session to the wireless device. If you do not enter a username for the only username, you can be locked out of the wireless device.

## Configuring Multiple Privilege Levels

By default, Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the Level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it Level 3 security and distribute that password to a more restricted group of users.

This section includes this configuration information:

- [Setting the Privilege Level for a Command, page 303](#)
- [Logging Into and Exiting a Privilege Level, page 304](#)



## Setting the Privilege Level for a Command

To set the privilege level for a command mode, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **privilege mode level level command**
3. **enable password level level password**
4. **end**
5. **show running-config**  
or  
**show privilege**
6. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>privilege mode level level command</b>	Sets the privilege level for a command. <ul style="list-style-type: none"> <li>For <i>mode</i>, enter <b>configure</b> for global configuration mode, <b>exec</b> for EXEC mode, <b>interface</b> for interface configuration mode, or <b>line</b> for line configuration mode.</li> <li>For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the <b>enable</b> password.</li> <li>For <i>command</i>, specify the command to which you want to restrict access.</li> </ul>
Step 3	<b>enable password level level password</b>	Specifies the enable password for the privilege level. <ul style="list-style-type: none"> <li>For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</li> <li>For <i>password</i>, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.</li> </ul> <p><b>Note</b> The characters TAB, ?, \$, +, and [ are invalid characters for passwords.</p>
Step 4	<b>end</b>	Returns to privileged EXEC mode.

	Command	Purpose
Step 5	<b>show running-config</b>	Verifies your entries.
	or	The <b>show running-config</b> command displays the password and access level configuration.
	<b>show privilege</b>	The <b>show privilege</b> command displays the privilege level configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

To return to the default privilege for a given command, use the **no privilege mode level level command** command in global configuration mode.

The following example shows how to set the **configure** command to privilege level 14 and how to define *SecretPswd14* as the password users must enter to use level 14 commands:

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

## Logging Into and Exiting a Privilege Level

To log in to a specified privilege level or to exit to a specified privilege level, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **enable level**
2. **disable level**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable level</b>	Logs in to a specified privilege level.
		For <i>level</i> , the range is 0 to 15.
Step 2	<b>disable level</b>	Exits to a specified privilege level.
		For <i>level</i> , the range is 0 to 15.

# Controlling Access Point Access with RADIUS

This section describes how to control administrator access to the wireless device by using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the wireless device to support RADIUS, see the “[Configuring Radius and TACACS+ Servers](#)” chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

**Note**

For complete syntax and usage information for the commands used in this section, see [Cisco IOS Security Command Reference](#).

These sections describe RADIUS configuration:

- [Default RADIUS Configuration, page 305](#)
- [Configuring RADIUS Login Authentication, page 305](#) (required)
- [Defining AAA Server Groups, page 307](#) (optional)
- [Configuring RADIUS Authorization for User Privileged Access and Network Services, page 309](#) (optional)
- [Displaying the RADIUS Configuration, page 310](#)

## Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users who are accessing the wireless device through the command-line interface (CLI).

## Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply the list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any defined authentication methods are performed. The only exception is the default method list (which is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be used to authenticate a user. You can designate one or more security protocols for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users. If that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—that is, the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

To configure login authentication, follow these steps, beginning in privileged EXEC mode. This procedure is required.

## SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login {default | list-name} method1 [method2...]**
4. **line [console | tty | vty] line-number [ending-line-number]**
5. **login authentication {default | list-name}**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>aaa new-model</b>	Enables AAA.
Step 3	<b>aaa authentication login {default   list-name} method1 [method2...]</b>	<p>Creates a login authentication method list.</p> <ul style="list-style-type: none"> <li>• To create a default list that is used when a named list is <i>not</i> specified in the <b>login authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.</li> <li>• For <i>list-name</i>, specify a character string to name the list you are creating.</li> <li>• For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.</li> </ul> <p>Select one of these methods:</p> <ul style="list-style-type: none"> <li>• <b>local</b>—Use the local username database for authentication. You must enter username information in the database. Use the <b>username password</b> global configuration command.</li> <li>• <b>radius</b>—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the “<a href="#">Identifying the RADIUS Server Host</a>” section of the “<a href="#">Configuring Radius and TACACS+ Servers</a>” chapter in <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i>.</li> </ul>
Step 4	<b>line [console   tty   vty] line-number [ending-line-number]</b>	Enters line configuration mode, and configures the lines for which to apply the authentication list.

	Command	Purpose
Step 5	<b>login authentication</b> { <b>default</b>   <i>list-name</i> }	Applies the authentication list to a line or set of lines. <ul style="list-style-type: none"> <li>If you specify <b>default</b>, use the default list that you created with the <b>aaa authentication login</b> command.</li> <li>For <i>list-name</i>, specify the list that you created with the <b>aaa authentication login</b> command.</li> </ul>
Step 6	<b>end</b>	Returns to privileged EXEC mode.
Step 7	<b>show running-config</b>	Verifies your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** command in global command mode. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2*...] command in global command mode. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } command in line configuration mode.

## Defining AAA Server Groups

You can configure the wireless device to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups can also include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a failover backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

To define the AAA server group and associate a particular RADIUS server with it, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaa group server radius** *group-name*
5. **server** *ip-address*
6. **end**
7. **show running-config**

8. copy running-config startup-config
9. aaa authorization exec radius

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>aaa new-model</b>	Enables AAA.
Step 3	<b>radius-server host</b> {hostname   ip-address} [ <b>auth-port</b> port-number] [ <b>acct-port</b> port-number] [ <b>timeout</b> seconds] [ <b>retransmit</b> retries] [ <b>key</b> string]	<p>Specifies the IP address or hostname of the remote RADIUS server host.</p> <ul style="list-style-type: none"> <li>(Optional) For <b>auth-port</b> port-number, specify the user datagram protocol (UDP) destination port for authentication requests.</li> <li>(Optional) For <b>acct-port</b> port-number, specify the UDP destination port for accounting requests.</li> <li>(Optional) For <b>timeout</b> seconds, specify the time interval that the wireless device waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the <b>radius-server timeout</b> global configuration command setting. If no timeout is set with the <b>radius-server host</b> command, the setting of the <b>radius-server timeout</b> command is used.</li> <li>(Optional) For <b>retransmit</b> retries, specify the number of times that a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the <b>radius-server host</b> command, the setting of the <b>radius-server retransmit</b> global configuration command is used.</li> <li>(Optional) For <b>key</b> string, specify the authentication and encryption key used between the wireless device and the RADIUS daemon running on the RADIUS server.</li> </ul> <p><b>Note</b> The key is a text string that must match the encryption key that is used on the RADIUS server. Always configure the key as the last item in the <b>radius-server host</b> command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the wireless device to recognize more than one host entry that is associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The wireless device software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p>
Step 4	<b>aaa group server radius</b> group-name	<p>Defines the AAA server-group with a group name.</p> <p>This command puts the wireless device in a server group configuration mode.</p>
Step 5	<b>server</b> ip-address	<p>Associates a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group.</p> <p>Each server in the group must be previously defined in Step 2.</p>

	Command	Purpose
Step 6	<b>end</b>	Returns to privileged EXEC mode.
Step 7	<b>show running-config</b>	Verifies your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.
Step 9	<b>aaa authorization exec radius</b>	Enables RADIUS login authentication. See the “ <a href="#">Configuring RADIUS Login Authentication</a> ” section of the “ <a href="#">Configuring Radius and TACACS+ Servers</a> ” chapter in <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i> .

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* command in global configuration mode. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* command in global configuration mode. To remove the IP address of a RADIUS server, use the **no server** *ip-address* command in sg-radius configuration mode.

In the following is example, the wireless device is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server which are configured for the same services. The second host entry acts as a failover backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

## Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services that are available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user’s profile, which is in the local user database or on the security server, to configure the user session. The user is granted access to a requested service only if the user profile allows it.

You can use the **aaa authorization** command in global configuration mode with the **radius** keyword to set parameters that restrict a user’s network access to privileged EXEC mode.

The **aaa authorization exec radius** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.



### Note

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

To specify RADIUS authorization for privileged EXEC access and network services, follow these steps, beginning in privileged EXEC mode.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization network radius**
3. **aaa authorization exec radius**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>aaa authorization network radius</b>	Configures the wireless device for user RADIUS authorization for all network-related service requests.
Step 3	<b>aaa authorization exec radius</b>	Configures the wireless device for user RADIUS authorization to determine whether the user has privileged EXEC access.  The <b>exec</b> keyword might return user profile information (such as <b>autocommand</b> information).
Step 4	<b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>show running-config</b>	Verifies your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** command in global configuration mode.

# Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** command in privileged EXEC mode.

# Controlling Access Point Access with TACACS+

This section describes how to control administrator access to the wireless device using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the wireless device to support TACACS+, see the [“Configuring Radius and TACACS+ Servers”](#) chapter in *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.



**Note**

For complete syntax and usage information for the commands used in this section, see [Cisco IOS Security Command Reference](#).

These sections describe TACACS+ configuration:

- [Default TACACS+ Configuration, page 311](#)
- [Configuring TACACS+ Login Authentication, page 311](#)
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 313](#)
- [Displaying the TACACS+ Configuration, page 314](#)

## Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators who are accessing the wireless device through the CLI.

## Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply the list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any defined authentication methods are performed. The only exception is the default method list (which is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be used to authenticate a user. You can designate one or more security protocols for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users. If that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—that is, the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

To configure login authentication, follow these steps, beginning in privileged EXEC mode. This procedure is required.

### SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login {default | list-name} method1 [method2...]**
4. **line [console | tty | vty] line-number [ending-line-number]**
5. **login authentication {default | list-name}**
6. **end**

7. `show running-config`
8. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>aaa new-model</code>	Enables AAA.
Step 3	<code>aaa authentication login {default   list-name} method1 [method2...]</code>	<p>Creates a login authentication method list.</p> <ul style="list-style-type: none"> <li>To create a default list that is used when a named list is <i>not</i> specified in the <b>login authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.</li> <li>For <i>list-name</i>, specify a character string to name the list you are creating.</li> <li>For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.</li> </ul> <p>Select one of these methods:</p> <ul style="list-style-type: none"> <li><b>local</b>—Use the local username database for authentication. You must enter username information into the database. Use the <b>username password</b> command in global configuration mode.</li> <li><b>tacacs+</b>—Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.</li> </ul>
Step 4	<code>line [console   tty   vty] line-number [ending-line-number]</code>	Enters line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	<code>login authentication {default   list-name}</code>	<p>Applies the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> <li>If you specify <b>default</b>, use the default list created with the <b>aaa authentication login</b> command.</li> <li>For <i>list-name</i>, specify the list created with the <b>aaa authentication login</b> command.</li> </ul>
Step 6	<code>end</code>	Returns to privileged EXEC mode.
Step 7	<code>show running-config</code>	Verifies your entries.
Step 8	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** command in global configuration mode. To disable AAA authentication, use the **no aaa authentication login {default | list-name} method1 [method2...]** command in global configuration mode. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication {default | list-name}** command in line configuration mode.

## Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** command in global configuration mode with the **tacacs+** keyword to set parameters that restrict a user network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

**Note**

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

To specify TACACS+ authorization for privileged EXEC access and network services, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization network tacacs+**
3. **aaa authorization exec tacacs+**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>aaa authorization network tacacs+</b>	Configures the wireless device for user TACACS+ authorization for all network-related service requests.
Step 3	<b>aaa authorization exec tacacs+</b>	Configures the wireless device for user TACACS+ authorization to determine whether the user has privileged EXEC access.  The <b>exec</b> keyword might return user profile information (such as <b>autocommand</b> information).
Step 4	<b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>show running-config</b>	Verifies your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To disable authorization, use the **no aaa authorization {network | exec} method1** command in global configuration mode.

## Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** command in privileged EXEC mode.

# Administering the Wireless Hardware and Software

This section provides instructions for performing the following tasks:

- [Resetting the Wireless Device to the Factory Default Configuration, page 314](#)
- [Rebooting the Wireless Device, page 314](#)
- [Monitoring the Wireless Device, page 315](#)

## Resetting the Wireless Device to the Factory Default Configuration

To reset the wireless device hardware and software to its factory default configuration, use the **service-module wlan-ap0 reset default-config** command in the router's Cisco IOS privileged EXEC mode.



### Caution

Because you may lose data, use only the **service-module wlan-ap0 reset** command to recover from a shutdown or failed state.

## Rebooting the Wireless Device

To perform a graceful shutdown and reboot the wireless device, use the **service-module wlan-ap0 reload** command in the router's Cisco IOS privileged EXEC mode. At the confirmation prompt, press **Enter** to confirm the action, or enter **n** to cancel.

When running in autonomous mode, the reload command saves the configuration before rebooting. If the attempt is unsuccessful, the following message displays:

```
Failed to save service module configuration.
```

When running in Lightweight Access Point Protocol (LWAPP) mode, the reload function is typically handled by the wireless LAN controller (WLC). If you enter the **service-module wlan-ap0 reload** command, you are prompted with the following message:

```
The AP is in LWAPP mode. Reload is normally handled by WLC controller.
```

```
Still want to proceed? [yes]
```

## Monitoring the Wireless Device

This section provides commands for monitoring hardware on the router.

- [Displaying Wireless Device Statistics, page 315](#)
- [Displaying Wireless Device Status, page 315](#)

### Displaying Wireless Device Statistics

Use the **service-module wlan-ap0 statistics** command in privileged EXEC mode to display wireless device statistics. The following is sample output for the command:

```
CLI reset count = 0
CLI reload count = 1
Registration request timeout reset count = 0
Error recovery timeout reset count = 0
Module registration count = 10
```

The last IOS initiated event was a cli reload at \*04:27:32.041 UTC Fri Mar 8 2007

### Displaying Wireless Device Status

Use the **service-module wlan-ap0 status** command in privileged EXEC mode to display the status of the wireless device and its configuration information. The following is sample output for the command:

```
Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..

Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Integrated Services
Routers.
```

## Managing the System Time and Date

You can manage the system time and date on the wireless device automatically, by using the Simple Network Time Protocol (SNTP), or manually, by setting the time and date on the wireless device.



#### Note

For complete syntax and usage information for the commands used in this section, see *Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*.

This section provides the following configuration information:

- [Understanding Simple Network Time Protocol, page 316](#)
- [Configuring SNTP, page 316](#)
- [Configuring Time and Date Manually, page 316](#)

## Understanding Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP. SNTP can only receive the time from NTP servers; it cannot provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP.

You can configure SNTP to request and accept packets from configured servers or to accept NTP broadcast packets from any source. When multiple sources are sending NTP packets, the server with the best stratum is selected. Click this URL for more information on NTP and strata:

[http://www.cisco.com/en/US/docs/ios/12\\_1/configfun/configuration/guide/fcd303.html#wp1001075](http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075)

If multiple servers are at the same stratum, a configured server is preferred rather than a broadcast server. If multiple servers pass both tests, the first one to send a time packet is selected. SNTP chooses a new server only if the client stops receiving packets from the currently selected server, or if (according to the above criteria) SNTP discovers a better server.

## Configuring SNTP

SNTP is disabled by default. To enable SNTP on the access point, use one or both of the commands listed in Table 2 in global configuration mode.

**Table 2** SNTP Commands

Command	Purpose
<b>sntp server</b> { <i>address</i>   <i>hostname</i> } [ <i>version number</i> ]	Configures SNTP to request NTP packets from an NTP server.
<b>sntp broadcast client</b>	Configures SNTP to accept NTP packets from any NTP broadcast server.

Enter the **sntp server** command once for each NTP server. The NTP servers must be configured to respond to the SNTP messages from the access point.

If you enter both the **sntp server** command and the **sntp broadcast client** command, the access point accepts time from a broadcast server but prefers time from a configured server, if the strata are equal. To display information about SNTP, use the **show sntp EXEC** command.

## Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after restarting the system. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the wireless device can synchronize, you do not need to manually set the system clock.

This section contains the following configuration information:

- [Setting the System Clock, page 317](#)
- [Displaying the Time and Date Configuration, page 317](#)
- [Configuring the Time Zone, page 318](#)
- [Configuring Summer Time \(Daylight Saving Time\), page 318](#)

## Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

To set the system clock, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **clock set** *hh:mm:ss day month year*  
or  
**clock set** *hh:mm:ss month day year*
2. **show running-config**
3. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>clock set</b> <i>hh:mm:ss day month year</i> or <b>clock set</b> <i>hh:mm:ss month day year</i>	Manually sets the system clock by using one of these formats: <ul style="list-style-type: none"><li>• For <i>hh:mm:ss</i>, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.</li><li>• For <i>day</i>, specify the day by date in the month.</li><li>• For <i>month</i>, specify the month by its full name.</li><li>• For <i>year</i>, specify the year in four digits (no abbreviation).</li></ul>
Step 2	<b>show running-config</b>	Verifies your entries.
Step 3	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
AP# clock set 13:32:00 23 July 2001
```

## Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock [detail]** command in privileged EXEC mode.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- \*—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

## Configuring the Time Zone

To manually configure the time zone, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **clock timezone** *zone hours-offset* [*minutes-offset*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>clock timezone</b> <i>zone hours-offset</i> [ <i>minutes-offset</i> ]	Sets the time zone.  Because the wireless device keeps internal time in UTC <sup>1</sup> , this command is used only for display purposes and when the time is manually set. <ul style="list-style-type: none"> <li>• For <i>zone</i>, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC.</li> <li>• For <i>hours-offset</i>, enter the hours offset from UTC.</li> <li>• (Optional) For <i>minutes-offset</i>, enter the minutes offset from UTC.</li> </ul>
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

1. UTC = universal time coordinated

The *minutes-offset* variable in the **clock timezone** command in global configuration mode is available for situations where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours, and the .5 means 50 percent. In this case, the necessary command is **clock timezone AST -3 30**.

To set the time to UTC, use the **no clock timezone** command in global configuration mode.

## Configuring Summer Time (Daylight Saving Time)

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **clock summer-time** *zone recurring* [*week day month hh:mm week day month hh:mm* [*offset*]]
3. **end**



4. **show running-config**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>clock summer-time zone recurring</b> [ <i>week day month hh:mm week day month hh:mm [offset]</i> ]	Configures summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify <b>clock summer-time zone recurring</b> without parameters, the summer time rules default to the United States rules. <ul style="list-style-type: none"> <li>For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</li> <li>(Optional) For <i>week</i>, specify the week of the month (1 to 5 or <b>last</b>).</li> <li>(Optional) For <i>day</i>, specify the day of the week (for example, Sunday).</li> <li>(Optional) For <i>month</i>, specify the month (for example, January).</li> <li>(Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes.</li> <li>(Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.</li> </ul>
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

If summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events), follow these steps, beginning in privileged EXEC mode.

## SUMMARY STEPS

1. **clock summer-time zone date** [*month date year hh:mm month date year hh:mm [offset]*]  
or  
**clock summer-time zone date** [*date month year hh:mm date month year hh:mm [offset]*]
2. **end**
3. **show running-config**
4. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>clock summer-time zone date</b> [ <i>month date year hh:mm month date year hh:mm [offset]</i> ] or <b>clock summer-time zone date</b> [ <i>date month year hh:mm date month year hh:mm [offset]</i> ]	Configures summer time to start on the first date and end on the second date.  Summer time is disabled by default. <ul style="list-style-type: none"> <li>For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</li> <li>(Optional) For <i>week</i>, specify the week of the month (1 to 5 or <b>last</b>).</li> <li>(Optional) For <i>day</i>, specify the day of the week (for example, Sunday).</li> <li>(Optional) For <i>month</i>, specify the month (for example, January).</li> <li>(Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes.</li> <li>(Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.</li> </ul>
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the **no clock summer-time** command in global configuration mode.

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

# Configuring a System Name and Prompt

You configure the system name on the wireless device to identify it. By default, the system name and prompt are *ap*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol (>) is appended. The prompt is updated whenever the system name changes, unless you manually configure the prompt by using the **prompt** command in global configuration mode.

**Note**

For complete syntax and usage information for the commands used in this section, see [Cisco IOS Configuration Fundamentals Command Reference](#) and [Cisco IOS IP Addressing Services Command Reference](#).

This section contains the following configuration information:

- [Default System Name and Prompt Configuration, page 321](#)
- [Configuring a System Name, page 321](#)
- [Understanding DNS, page 322](#)

## Default System Name and Prompt Configuration

The default access point system name and prompt are *ap*.

## Configuring a System Name

To manually configure a system name, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **hostname *name***
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>hostname</b> <i>name</i>	Manually configures a system name. The default setting is <i>ap</i> .  <b>Note</b> When you change the system name, the wireless device radios reset, and associated client devices disassociate and quickly reassociate.  <b>Note</b> You can enter up to 63 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 devices, make sure that a unique portion of the system name appears in the first 15 characters.
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

When you set the system name, the name is also used as the system prompt.

To return to the default hostname, use the **no hostname** command in global configuration mode.

## Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on the wireless device, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

This section contains the following configuration information:

- [Default DNS Configuration, page 323](#)
- [Setting Up DNS, page 323](#)
- [Displaying the DNS Configuration, page 324](#)

## Default DNS Configuration

Table 3 describes the default DNS configuration.

**Table 3**      **Default DNS Configuration**

Feature	Default Setting
DNS enable state	Disabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

## Setting Up DNS

To set up the wireless device to use the DNS, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **ip domain-name** *name*
3. **ip name-server** *server-address1* [*server-address2* ... *server-address6*]
4. **ip domain-lookup**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>ip domain-name</b> <i>name</i>	<p>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</p> <p>Do not include the initial period that separates an unqualified name from the domain name.</p> <p>At boot time, no domain name is configured. However, if the wireless device configuration comes from a BOOTP or DHCP server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</p>
Step 3	<b>ip name-server</b> <i>server-address1</i> [ <i>server-address2</i> ... <i>server-address6</i> ]	<p>Specifies the address of one or more name servers to use for name and address resolution.</p> <p>You can specify up to six name servers. Separate server addresses with a space. The first server specified is the primary server. The wireless device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.</p>

	Command	Purpose
Step 4	<b>ip domain-lookup</b>	(Optional) Enables DNS-based hostname-to-address translation on the wireless device. This feature is enabled by default.  If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	<b>end</b>	Returns to privileged EXEC mode.
Step 6	<b>show running-config</b>	Verifies your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

If you use the wireless device IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** command in global configuration mode. If there is a period (.) in the hostname, Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

To remove a domain name, use the **no ip domain-name** *name* command in global configuration mode. To remove a name server address, use the **no ip name-server** *server-address* command in global configuration mode. To disable DNS on the wireless device, use the **no ip domain-lookup** command in global configuration mode.

## Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** command in privileged EXEC mode.



### Note

When DNS is configured on the wireless device, the **show running-config** command sometimes displays a server IP address instead of its name.

## Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner also appears on all connected terminals. It appears after the MOTD banner and appears before the login prompts appear.



### Note

For complete syntax and usage information for the commands used in this section, see [Cisco IOS Configuration Fundamentals Command Reference](#).

This section contains the following configuration information:

- [Default Banner Configuration, page 325](#)
- [Configuring a Message-of-the-Day Login Banner, page 325](#)
- [Configuring a Login Banner, page 326](#)

## Default Banner Configuration

The MOTD and login banners are not configured.

## Configuring a Message-of-the-Day Login Banner

You can create a single-line or multiline message banner that appears on the screen when someone logs into the wireless device.

To configure an MOTD login banner, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **banner motd *c message c***
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>banner motd <i>c message c</i></b>	Specifies the message of the day.  For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the <b>Return</b> key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  For <i>message</i> , enter a banner message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To delete the MOTD banner, use the **no banner motd** command in global configuration mode.

The following example shows how to configure a MOTD banner for the wireless device. The pound sign (#) is used as the beginning and ending delimiter:

```
AP(config)# banner motd #
```

```
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#

This example shows the banner that results from the previous configuration:
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

Configuring a Login Banner

You can configure a login banner to appear on all connected terminals. This banner appears after the MOTD banner and appears before the login prompt appears.

To configure a login banner, follow these steps, beginning in privileged EXEC mode.

SUMMARY STEPS

- 1. **configure terminal**
- 2. **banner login *c message c***
- 3. **end**
- 4. **show running-config**
- 5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>banner login <i>c message c</i></b>	Specifies the login message.  For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the <b>Return</b> key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  For <i>message</i> , enter a login message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.



To delete the login banner, use the **no banner login** command in global configuration mode.

The following example shows how to configure a login banner for the wireless device using the dollar sign (\$) as the beginning and ending delimiter:

```
AP(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
AP(config)#
```

## Configuring Ethernet Speed and Duplex Settings

The Cisco 1941-W ISR interface supports only 1000 Mbps speed and duplex settings by default, and the interface is always up. When the wireless device receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the wireless device.



**Note** The speed and duplex settings on the wireless device Ethernet port must match the Ethernet settings on the port to which the wireless device is connected. If you change the settings on the port to which the wireless device is connected, change the settings on the wireless device Ethernet port to match.

The Ethernet speed and duplex are set to **auto** by default. To configure Ethernet speed and duplex, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **interface fastethernet0**
3. **speed {10 | 100 | auto}**
4. **duplex {auto | full | half}**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>interface fastethernet0</b>	Enters configuration interface mode.
Step 3	<b>speed {10   100   auto}</b>	Configures the Ethernet speed. we recommend that you use <b>auto</b> , the default setting.
Step 4	<b>duplex {auto   full   half}</b>	Configures the duplex setting. we recommend that you use <b>auto</b> , the default setting.
Step 5	<b>end</b>	Returns to privileged EXEC mode.

	Command	Purpose
Step 6	<b>show running-config</b>	Verifies your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring the Access Point for Wireless Network Management

You can enable the wireless device for wireless network management. The wireless network manager (WNM) manages the devices on your wireless LAN.

Enter the following command to configure the wireless device to interact with the WNM:

```
AP(config)# wlccp wnm ip address ip-address
```

Enter the following command to check the authentication status between the WDS access point and the WNM:

```
AP# show wlccp wnm status
```

Possible statuses are *not authenticated*, *authentication in progress*, *authentication fail*, *authenticated*, and *security keys setup*.

## Configuring the Access Point for Local Authentication and Authorization

You can configure AAA to operate without a server by configuring the wireless device to implement AAA in local mode. The wireless device then handles authentication and authorization. No accounting is available in this configuration.



### Note

You can configure the wireless device as a local authenticator for 802.1x-enabled client devices to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See *Using the Access Point as a Local Authenticator* at Cisco.com for detailed instructions on configuring the wireless device as a local authenticator:  
<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html>.

To configure the wireless device for local AAA, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login default local**
4. **aaa authorization exec local**
5. **aaa authorization network local**
6. **username name [privilege level] {password encryption-type password}**
7. **end**

8. `show running-config`
9. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>aaa new-model</code>	Enables AAA.
Step 3	<code>aaa authentication login default local</code>	Sets the login authentication to use the local username database. The <b>default</b> keyword applies the local user database authentication to all interfaces.
Step 4	<code>aaa authorization exec local</code>	Configures user AAA authorization to determine whether the user is allowed to run an EXEC shell by checking the local database.
Step 5	<code>aaa authorization network local</code>	Configures user AAA authorization for all network-related service requests.
Step 6	<code>username name [privilege level] {password encryption-type password}</code>	<p>Enters the local database, and establishes a username-based authentication system.</p> <p>Repeat this command for each user.</p> <ul style="list-style-type: none"> <li>For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed.</li> <li>(Optional) For <i>level</i>, specify the privilege level that the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</li> <li>For <i>encryption-type</i>, enter <b>0</b> to specify that an unencrypted password follows. Enter <b>7</b> to specify that a hidden password follows.</li> <li>For <i>password</i>, specify the password that the user must enter to gain access to the wireless device. The password must be from 1 to 25 characters long, can contain embedded spaces, and must be the last option specified in the <b>username</b> command.</li> </ul> <p><b>Note</b> The characters TAB, ?, \$, +, and [ are invalid characters for passwords.</p>
Step 7	<code>end</code>	Returns to privileged EXEC mode.
Step 8	<code>show running-config</code>	Verifies your entries.
Step 9	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** command in global configuration mode. To disable authorization, use the **no aaa authorization {network | exec} method1** command in global configuration mode.

# Configuring the Authentication Cache and Profile

The authentication cache and profile feature allows the access point to cache the authentication and authorization responses for a user so that subsequent authentication and authorization requests do not need to be sent to the AAA server.



## Note

On the access point, this feature is supported only for Admin authentication.

The following commands that support this feature are included in Cisco IOS Release 12.3(7):

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```



## Note

See [Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4\(10b\)JA and 12.3\(8\)JEC](#) for information about these commands.

The following is a configuration example for an access point configured for Admin authentication using TACACS+ with the authorization cache enabled. Although this example is based on a TACACS server, the access point could be configured for Admin authentication using RADIUS:

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
```

```
!  
aaa group server radius rad_pmip  
!  
aaa group server radius dummy  
!  
aaa authentication login default local cache tac_admin group tac_admin  
aaa authentication login eap_methods group rad_eap  
aaa authentication login mac_methods local  
aaa authorization exec default local cache tac_admin group tac_admin  
aaa accounting network acct_methods start-stop group rad_acct  
aaa cache profile admin_cache  
all  
!  
aaa session-id common  
!  
!  
!  
bridge irb  
!  
!  
interface Dot11Radio0  
no ip address  
no ip route-cache  
shutdown  
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0  
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  
bridge-group 1 spanning-disabled  
!  
interface Dot11Radio1  
no ip address  
no ip route-cache  
shutdown  
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0  
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  
bridge-group 1 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 BVI1  
ip address 192.168.133.207 255.255.255.0  
no ip route-cache  
!  
ip http server  
ip http authentication aaa  
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
```

```

!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end

```

## Configuring the Access Point to Provide DHCP Service

The following sections describe how to configure the wireless device to act as a DHCP server:

- [Setting up the DHCP Server, page 332](#)
- [Monitoring and Maintaining the DHCP Server Access Point, page 334](#)

## Setting up the DHCP Server

By default, access points are configured to receive IP settings from a DHCP server on your network. You can also configure an access point to act as a DHCP server to assign IP settings to devices on both wired and wireless LANs.



### Note

When you configure the access point as a DHCP server, it assigns IP addresses to devices on its subnet. The devices communicate with other devices on the subnet but not beyond it. If data needs to be passed beyond the subnet, you must assign a default router. The IP address of the default router should be on the same subnet as the access point configured as the DHCP server.

For detailed information on DHCP-related commands and options, see the DHCP part in *Cisco IOS IP Addressing Services Configuration Guide, Release 12.4*. Click this URL to browse to the DHCP part:

[http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad\\_dhcp\\_rdmf\\_ps6350\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmf_ps6350_TSD_Products_Configuration_Guide_Chapter.html)

To configure an access point to provide DHCP service and to specify a default router, follow these steps, beginning in privileged EXEC mode.

## SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp excluded-address** *low\_address* [*high\_address*]
3. **ip dhcp pool** *pool\_name*
4. **network** *subnet\_number* [*mask* | *prefix-length*]
5. **lease** {*days* [*hours*] [*minutes*] | **infinite**}
6. **default-router** *address* [*address2* ... *address 8*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>ip dhcp excluded-address</b> <i>low_address</i> [ <i>high_address</i> ]	Excludes the wireless device IP address from the range of addresses that the wireless device assigns. Enter the IP address in four groups of characters, such as 10.91.6.158.  The wireless device assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients.  (Optional) To enter a range of excluded addresses, enter the address at the low end of the range, followed by the address at the high end of the range.
Step 3	<b>ip dhcp pool</b> <i>pool_name</i>	Creates a name for the pool of IP addresses that the wireless device assigns in response to DHCP requests, and enters DHCP configuration mode.
Step 4	<b>network</b> <i>subnet_number</i> [ <i>mask</i>   <i>prefix-length</i> ]	Assigns the subnet number for the address pool. The wireless device assigns IP addresses within this subnet.  (Optional) Assigns a subnet mask for the address pool, or specifies the number of bits that compose the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).
Step 5	<b>lease</b> { <i>days</i> [ <i>hours</i> ] [ <i>minutes</i> ]   <b>infinite</b> }	Configures the duration of the lease for IP addresses assigned by the wireless device. <ul style="list-style-type: none"> <li>• days—configure the lease duration in number of days</li> <li>• (optional) hours—configure the lease duration in number of hours</li> <li>• (optional) minutes—configure the lease duration in number of minutes</li> <li>• infinite—set the lease duration to infinite</li> </ul>

	Command	Purpose
Step 6	<b>default-router</b> <i>address</i> [ <i>address2</i> ... <i>address</i> 8]	Specifies the IP address of the default router for DHCP clients on the subnet. One IP address is required; however, you can specify up to eight addresses in one command line.
Step 7	<b>end</b>	Returns to privileged EXEC mode.
Step 8	<b>show running-config</b>	Verifies your entries.
Step 9	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

Use the **no** forms of these commands to return to default settings.

The following example shows how to configure the wireless device as a DHCP server, how to exclude a range of IP address, and how to assign a default router:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

## Monitoring and Maintaining the DHCP Server Access Point

The following sections describe commands you can use to monitor and maintain the DHCP server access point:

- [show Commands, page 334](#)
- [clear Commands, page 335](#)
- [debug Command, page 335](#)

### show Commands

To display information about the wireless device as DHCP server, enter the commands in [Table 4](#), in privileged EXEC mode.

**Table 4** Show Commands for DHCP Server

Command	Purpose
<b>show ip dhcp conflict</b> [ <i>address</i> ]	Displays a list of all address conflicts recorded by a specific DHCP Server. Enter the wireless device IP address to show conflicts recorded by the wireless device.
<b>show ip dhcp database</b> [ <i>url</i> ]	Displays recent activity on the DHCP database. <b>Note</b> Use this command in privileged EXEC mode.
<b>show ip dhcp server statistics</b>	Displays count information about server statistics and messages sent and received.



## clear Commands

To clear DHCP server variables, use the commands in [Table 5](#), in privileged EXEC mode.

**Table 5** Clear Commands for DHCP Server

Command	Purpose
<b>clear ip dhcp binding</b> { <i>address</i>   *}	Deletes an automatic address binding from the DHCP database. Specifying the address argument clears the automatic binding for a specific (client) IP address. Specifying an asterisk (*) clears all automatic bindings.
<b>clear ip dhcp conflict</b> { <i>address</i>   *}	Clears an address conflict from the DHCP database. Specifying the address argument clears the conflict for a specific IP address. Specifying an asterisk (*) clears conflicts for all addresses.
<b>clear ip dhcp server statistics</b>	Resets all DHCP server counters to 0.

## debug Command

To enable DHCP server debugging, use the following command in privileged EXEC mode:

**debug ip dhcp server** {*events* | *packets* | *linkage*}

Use the **no** form of the command to disable debugging for the wireless device DHCP server.

# Configuring the Access Point for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.



### Note

For complete syntax and usage information for the commands used in this section, see the “Secure Shell Commands” section in *Cisco IOS Security Command Reference for Release 12.4*.

## Understanding SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports both SSH versions. If you do not specify the version number, the access point defaults to version 2.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. The SSH feature has an SSH server and an SSH integrated client. The client supports the following user authentication methods:

- RADIUS (for more information, see the [“Controlling Access Point Access with RADIUS”](#) section on page 305)
- Local authentication and authorization (for more information, see the [“Configuring the Access Point for Local Authentication and Authorization”](#) section on page 328)

For more information about SSH, see Part 5, “Other Security Features” in the *Cisco IOS Security Configuration Guide for Release 12.4*.

**Note**

The SSH feature in this software release does not support IP Security (IPsec).

## Configuring SSH

Before configuring SSH, download the cryptographic software image from Cisco.com. For more information, see the release notes for this release.

For information about configuring SSH and displaying SSH settings, see Part 6, “Other Security Features” in the *Cisco IOS Security Configuration Guide for Release 12.4*, which is available at Cisco.com at the following link:

[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12\\_4/sec\\_12\\_4\\_book.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html)

## Configuring Client ARP Caching

You can configure the wireless device to maintain an address resolution protocol (ARP) cache for associated client devices. Maintaining an ARP cache on the wireless device reduces the traffic load on your wireless LAN. ARP caching is disabled by default.

This section contains this information:

- [Understanding Client ARP Caching, page 336](#)
- [Configuring ARP Caching, page 337](#)

## Understanding Client ARP Caching

ARP caching on the wireless device reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the wireless device. Instead of forwarding ARP requests to client devices, the wireless device responds to requests on behalf of associated client devices.

When ARP caching is disabled, the wireless device forwards all ARP requests through the radio port to associated clients. The client that receives the ARP request responds. When ARP caching is enabled, the wireless device responds to ARP requests for associated clients and does not forward requests to clients. When the wireless device receives an ARP request for an IP address not in the cache, the wireless device drops the request and does not forward it. In its beacon, the wireless device includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

## Optional ARP Caching

When a non-Cisco client device is associated to an access point and is not passing data, the wireless device might not know the client IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the wireless device responds on behalf of clients with IP addresses known to the wireless device but forwards out of its radio port any ARP requests addressed to unknown clients. When the wireless device learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

## Configuring ARP Caching

To configure the wireless device to maintain an ARP cache for associated clients, follow these steps, beginning in privileged EXEC mode.

### SUMMARY STEPS

1. **configure terminal**
2. **dot11 arp-cache [optional]**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>dot11 arp-cache [optional]</b>	Enables ARP caching on the wireless device. <ul style="list-style-type: none"><li>• (Optional) Use the <b>optional</b> keyword to enable ARP caching only for the client devices whose IP addresses are known to the wireless device.</li></ul>
Step 3	<b>end</b>	Returns to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verifies your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

The following example shows how to configure ARP caching on an access point:

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

## Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging

This feature modifies the way that point-to-multipoint bridging can be configured to operate on multiple VLANs with the ability to control traffic rates on each VLAN.



#### Note

A rate-limiting policy can be applied only to Fast Ethernet ingress ports on non-root bridges.

In a typical scenario, multiple-VLAN support permits users to set up point-to-multipoint bridge links with remote sites, with each remote site on a separate VLAN. This configuration provides the capability for separating and controlling traffic to each site. Rate limiting ensures that no remote site consumes more than a specified amount of the entire link bandwidth. Only uplink traffic can be controlled by using the Fast Ethernet ingress ports of non-root bridges.

Using the class-based policing feature, you can specify the rate limit and apply it to the ingress of the Ethernet interface of a non-root bridge. Applying the rate at the ingress of the Ethernet interface ensures that all incoming Ethernet packets conform to the configured rate.