



Administering the Access Point

This chapter describes how to administer your access point. This chapter contains these sections:

- [Preventing Unauthorized Access to Your Access Point, page 5-2](#)
- [Protecting Access to Privileged EXEC Commands, page 5-2](#)
- [Controlling Access Point Access with RADIUS, page 5-7](#)
- [Controlling Access Point Access with TACACS+, page 5-12](#)
- [Configuring the Access Point for Wireless Network Management, page 5-15](#)
- [Configuring the Access Point for Local Authentication and Authorization, page 5-16](#)
- [Configuring the Access Point to Provide DHCP Service, page 5-17](#)
- [Configuring the Access Point for Secure Shell, page 5-19](#)
- [Configuring Client ARP Caching, page 5-20](#)
- [Managing the System Time and Date, page 5-21](#)
- [Configuring a System Name and Prompt, page 5-36](#)
- [Creating a Banner, page 5-38](#)

Preventing Unauthorized Access to Your Access Point

You can prevent unauthorized users from reconfiguring your access point and viewing configuration information. Typically, you want network administrators to have access to the access point while you restrict access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to your access point, you should configure one of these security features:

- Username and password pairs, which are locally stored on the access point. These pairs authenticate each user before that user can access the access point. 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 5-5. The default username is *Cisco*, and the default password is *Cisco*. Usernames and passwords are case-sensitive.
- Username and password pairs stored centrally in a database on a security server. For more information, see the [“Controlling Access Point Access with RADIUS”](#) section on page 5-7.

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 into a network device.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

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

- [Default Password and Privilege Level Configuration](#), page 5-2
- [Setting or Changing a Static Enable Password](#), page 5-3
- [Protecting Enable and Enable Secret Passwords with Encryption](#), page 5-4
- [Configuring Username and Password Pairs](#), page 5-5
- [Configuring Multiple Privilege Levels](#), page 5-6

Default Password and Privilege Level Configuration

[Table 5-1](#) shows the default password and privilege level configuration.

Table 5-1 Default Password and Privilege Levels

Feature	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.

Table 5-1 Default Password and Privilege Levels (continued)

Feature	Default Setting
Enable secret password and privilege level	The 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.



Note

The **no enable password** global configuration command 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 EXEC mode.

Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	enable password <i>password</i>	Define a new password or change an existing password for access to privileged EXEC mode. The default password is <i>Cisco</i> . 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: <ol style="list-style-type: none"> 1. Enter abc. 2. Enter Ctrl-V. 3. Enter ?123. 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 abc?123 at the password prompt.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file. The enable password is not encrypted and can be read in the access point configuration file.

This example shows how to change the enable password to *11u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional 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 Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both 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 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.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	enable password [level <i>level</i>] { <i>password</i> <i>encryption-type encrypted-password</i> } or enable secret [level <i>level</i>] { <i>password</i> <i>encryption-type encrypted-password</i> }	Define a new password or change an existing password for access to privileged EXEC mode. or Define a secret password, which is saved using a nonreversible encryption method. <ul style="list-style-type: none"> (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). 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. (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 configuration. <p>Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.</p>
Step 3	service password-encryption	(Optional) Encrypt 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	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save 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** global configuration command to specify commands accessible at various levels. For more information, see the “[Configuring Multiple Privilege Levels](#)” section on page 5-6.

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

This example shows how to configure the encrypted password `1FaD0$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 access point. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the access point. 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.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	username name [privilege level] { password encryption-type password }	Enter the username, privilege level, and password for each user. <ul style="list-style-type: none"> For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (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. 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. For <i>password</i>, specify the password the user must enter to gain access to the access point. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
Step 3	login local	Enable local password checking at login time. Authentication is based on the username specified in Step 2.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

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



Note You must have at least one username configured and you must have login local set to open a Telnet session to the access point. If you enter no username for the only username, you can be locked out of the access point.

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 5-6](#)
- [Logging Into and Exiting a Privilege Level, page 5-7](#)

Setting the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	privilege mode level level command	Set the privilege level for a command. <ul style="list-style-type: none"> • For <i>mode</i>, enter configure for global configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode. • 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 enable password. • For <i>command</i>, specify the command to which you want to restrict access.
Step 3	enable password level level password	Specify the enable password for the privilege level. <ul style="list-style-type: none"> • For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • 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.

	Command	Purpose
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config or show privilege	Verify your entries. The first command displays the password and access level configuration. The second command displays the privilege level configuration.
Step 6	copy running-config startup-config	(Optional) Save 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** global configuration command.

This example shows how to set the **configure** command to privilege level 14 and 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

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

	Command	Purpose
Step 1	enable level	Log in to a specified privilege level. For <i>level</i> , the range is 0 to 15.
Step 2	disable level	Exit 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 access point using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the access point to support RADIUS, see [Chapter 12, “Configuring RADIUS and TACACS+ Servers.”](#)

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS 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, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe RADIUS configuration:

- [Default RADIUS Configuration, page 5-8](#)
- [Configuring RADIUS Login Authentication, page 5-8](#) (required)
- [Defining AAA Server Groups, page 5-9](#) (optional)
- [Configuring RADIUS Authorization for User Privileged Access and Network Services, page 5-11](#) (optional)
- [Displaying the RADIUS Configuration, page 5-12](#)

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 accessing the access point through the CLI.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that 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 of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, 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 queried to authenticate a user. You can designate one or more security protocols to be used 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—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>aaa new-model</code>	Enable AAA.

	Command	Purpose
Step 3	<code>aaa authentication login { default list-name } method1 [method2...]</code>	<p>Create a login authentication method list.</p> <ul style="list-style-type: none"> To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For <i>list-name</i>, specify a character string to name the list you are creating. 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. <p>Select one of these methods:</p> <ul style="list-style-type: none"> local—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. radius—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the “Identifying the RADIUS Server Host” section on page 12-4.
Step 4	<code>line [console tty vty] line-number [ending-line-number]</code>	Enter 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>Apply the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> If you specify default, use the default list created with the aaa authentication login command. For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>show running-config</code>	Verify your entries.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

Defining AAA Server Groups

You can configure the access point 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 also can 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 fail-over 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.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>]	<p>Specify the IP address or host name of the remote RADIUS server host.</p> <ul style="list-style-type: none"> (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. (Optional) For timeout <i>seconds</i>, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit <i>retries</i>, specify the number of times 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 radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key <i>string</i>, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host 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 access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point 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>

	Command	Purpose
Step 4	<code>aaa group server radius group-name</code>	Define the AAA server-group with a group name. This command puts the access point in a server group configuration mode.
Step 5	<code>server ip-address</code>	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>show running-config</code>	Verify your entries.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the “ Configuring RADIUS Login Authentication ” section on page 5-8.

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

In this example, the access point is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over 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 available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user’s profile, which is in the local user database or on the security server, to configure the user’s 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** global configuration command with the **radius** keyword to set parameters that restrict a user’s network access to privileged EXEC mode.

The **aaa authorization exec radius local** 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.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network radius	Configure the access point for user RADIUS authorization for all network-related service requests.
Step 3	aaa authorization exec radius	Configure the access point for user RADIUS authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Displaying the RADIUS Configuration

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

Controlling Access Point Access with TACACS+

This section describes how to control administrator access to the access point using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the access point to support TACACS+, see [Chapter 12, “Configuring RADIUS and TACACS+ Servers.”](#)

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, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

These sections describe TACACS+ configuration:

- [Default TACACS+ Configuration, page 5-13](#)
- [Configuring TACACS+ Login Authentication, page 5-13](#)
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 5-14](#)
- [Displaying the TACACS+ Configuration, page 5-15](#)

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 accessing the access point through the CLI.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that 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 of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used 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, 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—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>aaa new-model</code>	Enable AAA.

	Command	Purpose
Step 3	aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	<p>Create a login authentication method list.</p> <ul style="list-style-type: none"> To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For <i>list-name</i>, specify a character string to name the list you are creating. 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. <p>Select one of these methods:</p> <ul style="list-style-type: none"> local—Use the local username database for authentication. You must enter username information into the database. Use the username password global configuration command. tacacs+—Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	line [console tty vty] <i>line-number</i> [<i>ending-line-number</i>]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	login authentication { default <i>list-name</i> }	<p>Apply the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> If you specify default, use the default list created with the aaa authentication login command. For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

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 access point uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's 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** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's 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.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa authorization network tacacs+	Configure the access point for user TACACS+ authorization for all network-related service requests.
Step 3	aaa authorization exec tacacs+	Configure the access point for user TACACS+ authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Displaying the TACACS+ Configuration

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

Configuring the Access Point for Wireless Network Management

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

Enter this command to configure the access point to interact with the WNM:

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

Enter this 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 access point to implement AAA in local mode. The access point then handles authentication and authorization. No accounting is available in this configuration.



Note

You can configure your access point 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 [Chapter 8, “Configuring an Access Point as a Local Authenticator,”](#) for detailed instructions on configuring your access point as a local authenticator.

Beginning in privileged EXEC mode, follow these steps to configure the access point for local AAA:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication login default local	Set the login authentication to use the local username database. The default keyword applies the local user database authentication to all interfaces.
Step 4	aaa authorization exec local	Configure user AAA authorization to determine if the user is allowed to run an EXEC shell by checking the local database.
Step 5	aaa authorization network local	Configure user AAA authorization for all network-related service requests.
Step 6	username name [privilege level] { password encryption-type password }	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. <ul style="list-style-type: none"> For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (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 0 gives user EXEC mode access. For <i>encryption-type</i>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. For <i>password</i>, specify the password the user must enter to gain access to the access point. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
Step 7	end	Return to privileged EXEC mode.
Step 8	show running-config	Verify your entries.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Configuring the Access Point to Provide DHCP Service

These sections describe how to configure the access point to act as a DHCP server:

- [Setting up the DHCP Server, page 5-17](#)
- [Monitoring and Maintaining the DHCP Server Access Point, page 5-18](#)

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 your wired and wireless LANs.

The 1100 series access point becomes a mini-DHCP server by default when it is configured with factory default settings and it cannot receive IP settings from a DHCP server. As a mini-DHCP server, the 1100 series access point provides up to 20 IP addresses between 10.0.0.11 and 10.0.0.30 to a PC connected to its Ethernet port and to wireless client devices configured to use either no SSID or *tsunami* as the SSID, and with all security settings disabled. The mini-DHCP server feature is disabled automatically when you assign a static IP address to the 1100 series access point. Because it has a console port to simplify initial setup, the 1200 series access point does not become a DHCP server automatically.

For detailed information on DHCP-related commands and options, refer to the Configuring DHCP chapter in the *Cisco IOS IP Configuration Guide, Release 12.2*. Click this URL to browse to the “Configuring DHCP” chapter:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca75c.html

Beginning in privileged EXEC mode, follow these steps to configure an access point to provide DHCP service:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp excluded-address <i>low_address</i> [<i>high_address</i>]	Exclude the access point’s IP address from the range of addresses the access point assigns. Enter the IP address in four groups of characters, such as 10.91.6.158. The access point 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	ip dhcp pool <i>pool_name</i>	Create a name for the pool of IP addresses that the access point assigns in response to DHCP requests, and enter DHCP configuration mode.
Step 4	network <i>subnet_number</i> [<i>mask</i> <i>prefix-length</i>]	Assign the subnet number for the address pool. The access point assigns IP addresses within this subnet. (Optional) Assign a subnet mask for the address pool, or specify the number of bits that comprise the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).

	Command	Purpose
Step 5	<code>lease { days [hours] [minutes] infinite }</code>	Configure the duration of the lease for IP addresses assigned by the access point. <ul style="list-style-type: none"> days—configure the lease duration in number of days (optional) hours—configure the lease duration in number of hours (optional) minutes—configure the lease duration in number of minutes infinite—set the lease duration to infinite
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>show running-config</code>	Verify your entries.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

This example shows how to configure the access point as a DHCP server:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.117
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)# end
```

Monitoring and Maintaining the DHCP Server Access Point

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

- [Show Commands, page 5-18](#)
- [Clear Commands, page 5-19](#)
- [Debug Command, page 5-19](#)

Show Commands

In Exec mode, enter the commands in [Table 5-2](#) to display information about the access point as DHCP server.

Table 5-2 Show Commands for DHCP Server

Command	Purpose
<code>show ip dhcp conflict [address]</code>	Displays a list of all address conflicts recorded by a specific DHCP Server. Enter the access point's IP address to show conflicts recorded by the access point.

Table 5-2 Show Commands for DHCP Server

Command	Purpose
<code>show ip dhcp database [url]</code>	Displays recent activity on the DHCP database. Note Use this command in privileged EXEC mode.
<code>show ip dhcp server statistics</code>	Displays count information about server statistics and messages sent and received.

Clear Commands

In privileged Exec mode, use the commands in [Table 5-3](#) to clear DHCP server variables.

Table 5-3 Clear Commands for DHCP Server

Command	Purpose
<code>clear ip dhcp binding { address * }</code>	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.
<code>clear ip dhcp conflict { address * }</code>	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.
<code>clear ip dhcp server statistics</code>	Resets all DHCP Server counters to 0.

Debug Command

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

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

Use the **no** form of the command to disable debugging for the access point 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, refer to the “Secure Shell Commands” section in the *Cisco IOS Security Command Reference for Release 12.2*.

Understanding SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports only SSH version 1.

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 these user authentication methods:

- RADIUS (for more information, see the [“Controlling Access Point Access with RADIUS”](#) section on page 5-7)
- Local authentication and authorization (for more information, see the [“Configuring the Access Point for Local Authentication and Authorization”](#) section on page 5-16)

For more information about SSH, refer to the “Configuring Secure Shell” section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

**Note**

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

Configuring SSH

Before configuring SSH, download the crypto software image from Cisco.com. For more information, refer to the release notes for this release.

For information about configuring SSH and displaying SSH settings, refer to the “Configuring Secure Shell” section in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Configuring Client ARP Caching

You can configure the access point to maintain an ARP cache for associated client devices. Maintaining an ARP cache on the access point reduces the traffic load on your wireless LAN. ARP caching is disabled by default.

This section contains this information:

- [Understanding Client ARP Caching, page 5-20](#)
- [Configuring ARP Caching, page 5-21](#)

Understanding Client ARP Caching

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

When ARP caching is disabled, the access point forwards all ARP requests through the radio port to associated clients, and the client to which the ARP request is directed responds. When ARP caching is enabled, the access point responds to ARP requests for associated clients and does not forward requests to clients. When the access point receives an ARP request for an IP address not in the cache, the access point drops the request and does not forward it.

Optional ARP Caching

When a non-Cisco client device is associated to an access point and is not passing data, the access point might not know the client’s IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the access point responds on behalf of

clients with IP addresses known to the access point but forwards out its radio port any ARP requests addressed to unknown clients. When the access point learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Configuring ARP Caching

Beginning in privileged EXEC mode, follow these steps to configure the access point to maintain an ARP cache for associated clients:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>dot11 arp-cache [optional]</code>	Enable ARP caching on the access point. <ul style="list-style-type: none"> (Optional) Use the optional keyword to enable ARP caching only for the client devices whose IP addresses are known to the access point.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

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

Managing the System Time and Date

You can manage the system time and date on your access point automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the access point.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- [Understanding the System Clock, page 5-21](#)
- [Understanding Network Time Protocol, page 5-22](#)
- [Configuring NTP, page 5-23](#)
- [Configuring Time and Date Manually, page 5-31](#)

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- Network Time Protocol
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock determines time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time is correctly displayed for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed. For configuration information, see the [“Configuring Time and Date Manually” section on page 5-31](#).

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access-list-based restriction scheme and an encrypted authentication mechanism.

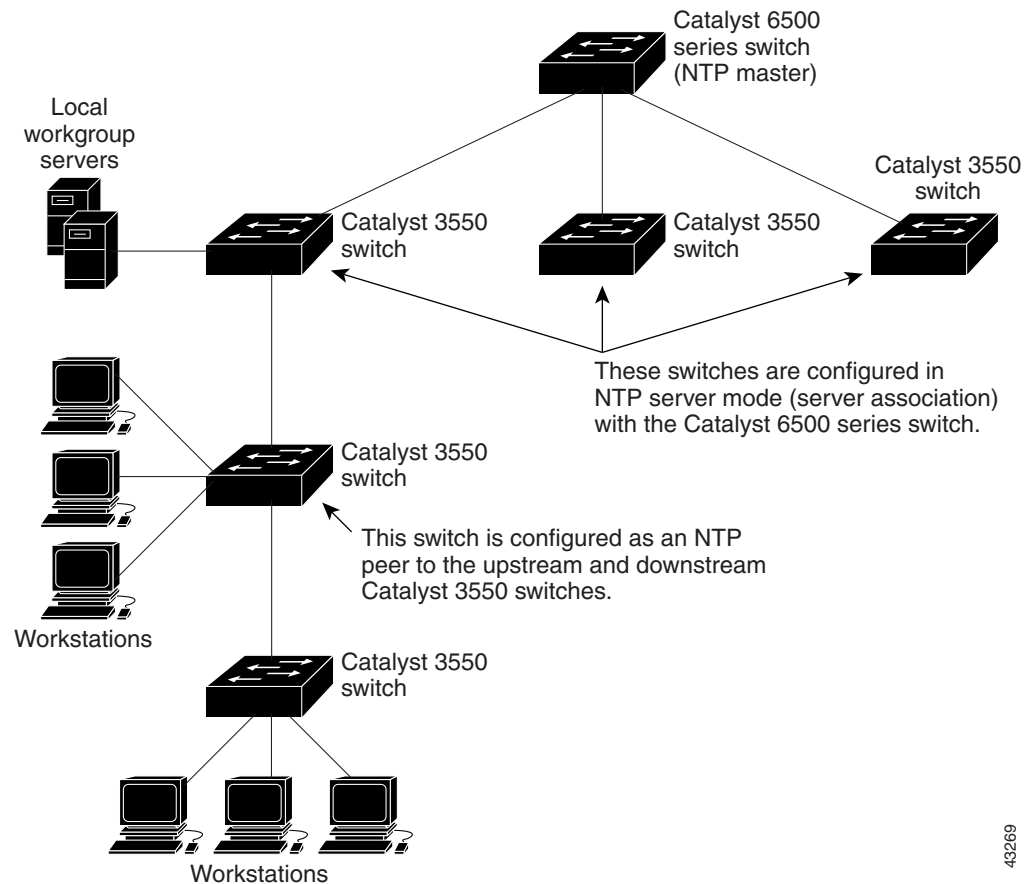
Cisco’s implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet. [Figure 5-1](#) shows a typical network example using NTP.

If the network is isolated from the Internet, Cisco’s implementation of NTP allows a device to act as though it is synchronized through NTP, when in fact it has determined the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

Figure 5-1 Typical NTP Network Configuration



43269

Configuring NTP

Cisco Aironet 1100 Series Access Points do not have a hardware-supported clock, and they cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. These access points also have no hardware support for a calendar. As a result, the `ntp update-calendar` and the `ntp master` global configuration commands are not available.

This section contains this configuration information:

- [Default NTP Configuration, page 5-24](#)
- [Configuring NTP Authentication, page 5-24](#)
- [Configuring NTP Associations, page 5-26](#)
- [Configuring NTP Broadcast Service, page 5-27](#)
- [Configuring NTP Access Restrictions, page 5-28](#)

- [Configuring the Source IP Address for NTP Packets, page 5-30](#)
- [Displaying the NTP Configuration, page 5-31](#)

Default NTP Configuration

Table 5-4 shows the default NTP configuration.

Table 5-4 Default NTP Configuration

Feature	Default Setting
NTP authentication	Disabled. No authentication key is specified.
NTP peer or server associations	None configured.
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets.
NTP access restrictions	No access control is specified.
NTP packet source IP address	The source address is determined by the outgoing interface.

NTP is disabled by default.

Configuring NTP Authentication

This procedure must be coordinated with the administrator of the NTP server; the information you configure in this procedure must be matched by the servers used by the access point to synchronize its time to the NTP server.

Beginning in privileged EXEC mode, follow these steps to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp authenticate	Enable the NTP authentication feature, which is disabled by default.
Step 3	ntp authentication-key <i>number</i> md5 <i>value</i>	<p>Define the authentication keys. By default, none are defined.</p> <ul style="list-style-type: none"> • For <i>number</i>, specify a key number. The range is 1 to 4294967295. • md5 specifies that message authentication support is provided by using the message digest algorithm 5 (MD5). • For <i>value</i>, enter an arbitrary string of up to eight characters for the key. <p>The access point does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the ntp trusted-key <i>key-number</i> command.</p>

	Command	Purpose
Step 4	ntp trusted-key <i>key-number</i>	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this access point to synchronize to it. By default, no trusted keys are defined. For <i>key-number</i> , specify the key defined in Step 3. This command provides protection against accidentally synchronizing the access point to a device that is not trusted.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable NTP authentication, use the **no ntp authenticate** global configuration command. To remove an authentication key, use the **no ntp authentication-key** *number* global configuration command. To disable authentication of the identity of a device, use the **no ntp trusted-key** *key-number* global configuration command.

This example shows how to configure the access point to synchronize only to devices providing authentication key 42 in the device's NTP packets:

```
AP(config)# ntp authenticate
AP(config)# ntp authentication-key 42 md5 aNiceKey
AP(config)# ntp trusted-key 42
```

Configuring NTP Associations

An NTP association can be a peer association (this access point can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this access point synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp peer <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]	Configure the access point system clock to synchronize a peer or to be synchronized by a peer (peer association).
	or	or
	ntp server <i>ip-address</i> [version <i>number</i>] [key <i>keyid</i>] [source <i>interface</i>] [prefer]	Configure the access point system clock to be synchronized by a time server (server association).
		No peer or server associations are defined by default. <ul style="list-style-type: none"> For <i>ip-address</i> in a peer association, specify either the IP address of the peer providing, or being provided, the clock synchronization. For a server association, specify the IP address of the time server providing the clock synchronization. (Optional) For <i>number</i>, specify the NTP version number. The range is 1 to 3. By default, version 3 is selected. (Optional) For <i>keyid</i>, enter the authentication key defined with the ntp authentication-key global configuration command. (Optional) For <i>interface</i>, specify the interface from which to pick the IP source address. By default, the source IP address is taken from the outgoing interface. (Optional) Enter the prefer keyword to make this peer or server the preferred one that provides synchronization. This keyword reduces switching back and forth between peers and servers.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

You need to configure only one end of an association; the other device can automatically establish the association. If you are using the default NTP version (version 3) and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

To remove a peer or server association, use the **no ntp peer** *ip-address* or the **no ntp server** *ip-address* global configuration command.

This example shows how to configure the access point to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP version 2:

```
AP(config)# ntp server 172.16.22.44 version 2
```

Configuring NTP Broadcast Service

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP addresses of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, the information flow is one-way only.

The access point can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. The access point can send NTP broadcast packets to a peer so that the peer can synchronize to it. The access point can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

Beginning in privileged EXEC mode, follow these steps to configure the access point to send NTP broadcast packets to peers so that they can synchronize their clock to the access point:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to send NTP broadcast packets.
Step 3	ntp broadcast [<i>version number</i>] [<i>key keyid</i>] [<i>destination-address</i>]	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. <ul style="list-style-type: none"> (Optional) For <i>number</i>, specify the NTP version number. The range is 1 to 3. If you do not specify a version, version 3 is used. (Optional) For <i>keyid</i>, specify the authentication key to use when sending packets to the peer. (Optional) For <i>destination-address</i>, specify the IP address of the peer that is synchronizing its clock to this access point.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.
Step 7		Configure the connected peers to receive NTP broadcast packets as described in the next procedure.

To disable the interface from sending NTP broadcast packets, use the **no ntp broadcast** interface configuration command.

This example shows how to configure an interface to send NTP version 2 packets:

```
AP(config)# interface gigabitethernet0/1
AP(config-if)# ntp broadcast version 2
```

Beginning in privileged EXEC mode, follow these steps to configure the access point to receive NTP broadcast packets from connected peers:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to receive NTP broadcast packets.
Step 3	ntp broadcast client	Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.
Step 4	exit	Return to global configuration mode.
Step 5	ntp broadcastdelay <i>microseconds</i>	(Optional) Change the estimated round-trip delay between the access point and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable an interface from receiving NTP broadcast packets, use the **no ntp broadcast client** interface configuration command. To change the estimated round-trip delay to the default, use the **no ntp broadcastdelay** global configuration command.

This example shows how to configure an interface to receive NTP broadcast packets:

```
AP(config)# interface gigabitethernet0/1
AP(config-if)# ntp broadcast client
```

Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

- [Creating an Access Group and Assigning a Basic IP Access List, page 5-29](#)
- [Disabling NTP Services on a Specific Interface, page 5-30](#)

Creating an Access Group and Assigning a Basic IP Access List

Beginning in privileged EXEC mode, follow these steps to control access to NTP services by using access lists:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp access-group { query-only serve-only serve peer } <i>access-list-number</i>	Create an access group, and apply a basic IP access list. The keywords have these meanings: <ul style="list-style-type: none"> • query-only—Allows only NTP control queries. • serve-only—Allows only time requests. • serve—Allows time requests and NTP control queries, but does not allow the access point to synchronize to the remote device. • peer—Allows time requests and NTP control queries and allows the access point to synchronize to the remote device. For <i>access-list-number</i> , enter a standard IP access list number from 1 to 99.
Step 3	access-list <i>access-list-number</i> permit <i>source</i> [<i>source-wildcard</i>]	Create the access list. <ul style="list-style-type: none"> • For <i>access-list-number</i>, enter the number specified in Step 2. • Enter the permit keyword to permit access if the conditions are matched. • For <i>source</i>, enter the IP address of the device that is permitted access to the access point. • (Optional) For <i>source-wildcard</i>, enter the wildcard bits to be applied to the source. Note When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The access group keywords are scanned in this order, from least restrictive to most restrictive:

1. **peer**—Allows time requests and NTP control queries and allows the access point to synchronize itself to a device whose address passes the access list criteria.
2. **serve**—Allows time requests and NTP control queries, but does not allow the access point to synchronize itself to a device whose address passes the access list criteria.
3. **serve-only**—Allows only time requests from a device whose address passes the access list criteria.
4. **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all devices. If any access groups are specified, only the specified access types are granted.

To remove access control to the access point NTP services, use the **no ntp access-group {query-only | serve-only | serve | peer}** global configuration command.

This example shows how to configure the access point to allow itself to synchronize to a peer from access list 99. However, the access point restricts access to allow only time requests from access list 42:

```
AP# configure terminal
AP(config)# ntp access-group peer 99
AP(config)# ntp access-group serve-only 42
AP(config)# access-list 99 permit 172.20.130.5
AP(config)# access list 42 permit 172.20.130.6
```

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and specify the interface to disable.
Step 3	ntp disable	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To re-enable receipt of NTP packets on an interface, use the **no ntp disable** interface configuration command.

Configuring the Source IP Address for NTP Packets

When the access point sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** global configuration command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets.

Beginning in privileged EXEC mode, follow these steps to configure a specific interface from which the IP source address is to be taken:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp source <i>type number</i>	Specify the interface type and number from which the IP source address is taken. By default, the source address is determined by the outgoing interface.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** global configuration command as described in the “[Configuring NTP Associations](#)” section on page 5-26.

Displaying the NTP Configuration

You can use two privileged EXEC commands to display NTP information:

- **show ntp associations [detail]**
- **show ntp status**

For detailed information about the fields in these displays, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.1*.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. 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 access point can synchronize, you do not need to manually set the system clock.

This section contains this configuration information:

- [Setting the System Clock, page 5-32](#)
- [Displaying the Time and Date Configuration, page 5-32](#)
- [Configuring the Time Zone, page 5-33](#)
- [Configuring Summer Time \(Daylight Saving Time\), page 5-34](#)

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.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
Step 1	<code>clock set hh:mm:ss day month year</code> or <code>clock set hh:mm:ss month day year</code>	Manually set the system clock using one of these formats. <ul style="list-style-type: none"> 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. For <i>day</i>, specify the day by date in the month. For <i>month</i>, specify the month by name. For <i>year</i>, specify the year (no abbreviation).
Step 2	<code>show running-config</code>	Verify your entries.
Step 3	<code>copy running-config startup-config</code>	(Optional) Save 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]** privileged EXEC command.

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

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	clock timezone <i>zone hours-offset</i> [<i>minutes-offset</i>]	Set the time zone. The access point keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. <ul style="list-style-type: none"> For <i>zone</i>, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. For <i>hours-offset</i>, enter the hours offset from UTC. (Optional) For <i>minutes-offset</i>, enter the minutes offset from UTC.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The *minutes-offset* variable in the **clock timezone** global configuration command is available for those cases 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 .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** global configuration command.

Configuring Summer Time (Daylight Saving Time)

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

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

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	clock summer-time zone date [<i>month date year hh:mm month date year hh:mm [offset]</i>] or clock summer-time zone date [<i>date month year hh:mm date month year hh:mm [offset]</i>]	Configure 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"> For <i>zone</i>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. (Optional) For <i>week</i>, specify the week of the month (1 to 5 or last). (Optional) For <i>day</i>, specify the day of the week (Sunday, Monday...). (Optional) For <i>month</i>, specify the month (January, February...). (Optional) For <i>hh:mm</i>, specify the time (24-hour format) in hours and minutes. (Optional) For <i>offset</i>, specify the number of minutes to add during summer time. The default is 60.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save 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** global configuration command.

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 access point 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** global configuration command.



Note

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference* and the *Cisco IOS IP and IP Routing Command Reference for Release 12.1*.

This section contains this configuration information:

- [Default System Name and Prompt Configuration, page 5-36](#)
- [Configuring a System Name, page 5-36](#)
- [Understanding DNS, page 5-37](#)

Default System Name and Prompt Configuration

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

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	hostname name	Manually configure a system name. The default setting is <i>ap</i> . The name must follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters. Note When you change the system name, the access point radios reset, and associated client devices disassociate and quickly reassociate.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

To return to the default host name, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map host names to IP addresses. When you configure DNS on your access point, you can substitute the host name 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 host names, specify the name server that is present on your network, and enable the DNS.

This section contains this configuration information:

- [Default DNS Configuration, page 5-37](#)
- [Setting Up DNS, page 5-37](#)
- [Displaying the DNS Configuration, page 5-38](#)

Default DNS Configuration

Table 5-5 shows the default DNS configuration.

Table 5-5 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

Beginning in privileged EXEC mode, follow these steps to set up your access point to use the DNS:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip domain-name <i>name</i>	Define a default domain name that the software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the access point configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).

	Command	Purpose
Step 3	ip name-server <i>server-address1</i> [<i>server-address2</i> ... <i>server-address6</i>]	Specify the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The access point sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	ip domain-lookup	(Optional) Enable DNS-based host name-to-address translation on your access point. 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	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If you use the access point IP address as its host name, the IP address is used and no DNS query occurs. If you configure a host name that contains no periods (.), a period followed by the default domain name is appended to the host name 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** global configuration command. If there is a period (.) in the host name, Cisco IOS software looks up the IP address without appending any default domain name to the host name.

To remove a domain name, use the **no ip domain-name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To disable DNS on the access point, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

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



Note

When DNS is configured on the access point, the **show running-config** command sometimes displays a server's 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 before the login prompts.

**Note**

For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This section contains this configuration information:

- [Default Banner Configuration, page 5-39](#)
- [Configuring a Message-of-the-Day Login Banner, page 5-39](#)
- [Configuring a Login Banner, page 5-40](#)

Default Banner Configuration

The MOTD and login banners are not configured.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs into the access point.

Beginning in privileged EXEC mode, follow these steps to configure a MOTD login banner:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>banner motd c message c</code>	Specify the message of the day. For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the Return 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	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

This example shows how to configure a MOTD banner for the access point using the pound sign (#) symbol 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 displayed from the previous configuration:

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
```

Escape character is '^]'.
 ^Z

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 before the login prompt.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	banner login c message c	Specify the login message. For <i>c</i> , enter the delimiting character of your choice, such as a pound sign (#), and press the Return 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	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

This example shows how to configure a login banner for the access point using the dollar sign (\$) symbol as the beginning and ending delimiter:

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