

Administering the Wireless Device

Revised: , OL-18906-02

This module describes the following wireless device administration tasks.

Securing Access to the Wireless Device

- [Disabling the Mode Button Function, page 10-2](#)
 - [Preventing Unauthorized Access to Your Access Point, page 10-3](#)
 - [Protecting Access to Privileged EXEC Commands, page 10-3](#)
 - [Controlling Access Point Access with RADIUS, page 10-9](#)
 - [Controlling Access Point Access with TACACS+, page 10-14](#)

Administering the Access Point Hardware and Software

- [Administering the Wireless Hardware and Software, page 10-17](#)
 - [Resetting the Wireless Device to the Factory Default Configuration, page 10-17](#)
 - [Rebooting the Wireless Device, page 10-17](#)
 - [Monitoring the Wireless Device, page 10-18](#)
- [Managing the System Time and Date, page 10-18](#)
- [Configuring a System Name and Prompt, page 10-24](#)
- [Creating a Banner, page 10-27](#)

Administering Wireless Device Communication

- [Configuring Ethernet Speed and Duplex Settings, page 10-29](#)
 - [Configuring the Access Point for Wireless Network Management, page 10-30](#)
 - [Configuring the Access Point for Local Authentication and Authorization, page 10-30](#)
 - [Configuring the Authentication Cache and Profile, page 10-31](#)
 - [Configuring the Access Point to Provide DHCP Service, page 10-34](#)
 - [Configuring the Access Point for Secure Shell, page 10-37](#)
 - [Configuring Client ARP Caching, page 10-38](#)
 - [Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging, page 10-39](#)

Disabling the Mode Button Function

[no] boot mode-button



Caution

(TAC) to regain access to the access point command line interface (CLI).



Note

Use the **service-module wlan-ap reset** command from the router's Cisco IOS CLI. See the [“Rebooting the Wireless Device”](#) section on page 10-17 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:

	Command	Purpose
Step 1	configure terminal	
	no boot mode-button	
Step 3		Note

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#
```



Preventing Unauthorized Access to Your Access Point

•

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 10-6. The default username is *Cisco*.



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 10-9.

Protecting Access to Privileged EXEC Commands

**Note**

Security Command Reference for Release 12.4

Cisco IOS

, page 10-5

[Configuring Username and Password Pairs](#), page 10-6

[Configuring Multiple Privilege Levels](#), page 10-7

Configuring Default Password and Privilege Level

Table 1 *Default Passwords and Privilege Levels*

Privilege Level	Default Setting
	<i>Cisco</i> , <i>Cisco</i> .
	<i>Cisco</i>

Default Passwords and Privilege Levels (continued)

Setting or Changing a Static Enable Password



Note

<i>password</i>	<p style="text-align: right;"><i>Cisco</i></p> <p><i>password</i></p> <p>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"> 1. Enter . 2. Enter Ctrl-V ?123 <p style="text-align: right;">abc?123</p>
end	
Step 4 show running-config	
Step 5 copy running-config startup-config	

11u2c3k4y5

AP(config)# enable password 11u2c3k4y5

Protecting Enable and Enable Secret Passwords with Encryption

	Command	Purpose
Step 1		
Step 2	<pre>enable password [level] { encryption-type encrypted-password } or enable secret [] { }</pre>	<p>Defines a new password or changes an existing password for access to privileged EXEC mode.</p> <p>or</p> <p>Defines a secret password, which is saved using a nonreversible encryption method.</p> <p>(Optional) For <code>level</code>, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).</p> <p>For <code>encrypted-password</code>, 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.</p> <p>(Optional) For <code>encryption-type</code>, 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.</p> <p>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.</p>
		<p>(Optional) Encrypts the password when the password is defined or when the configuration is written.</p> <p>Encryption prevents the password from being readable in the configuration file.</p>

	Command	Purpose
Step 4		
Step 5		

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

Use the `enable password` 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 `enable secret` command in global configuration mode to specify commands accessible at various levels. For more information, see the [“Configuring Multiple Privilege Levels” section on page 10-7](#).

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 `enable password [level] no` command or `enable secret [level] no` command in global configuration mode. To disable password encryption, use the `enable secret no` command in global configuration mode.

This example shows how to configure the encrypted password `1FaD0$Xyti5Rkls3LoyxzS8`

```
enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Configuring Username and Password Pairs

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> • • • •
Step 3		

	Command	Purpose
Step 4		
Step 5		
Step 6		



Note

Configuring Multiple Privilege Levels

-
-

Setting the Privilege Level for a Command

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> • interface exec line • enable •



	Command	Purpose
Step 3		<ul style="list-style-type: none"> • • <p>Note</p>
Step 4		
Step 5		
Step 6		

SecretPswd14

```
privilege exec level 14 configure
enable password level 14 SecretPswd14
```

Logging Into and Exiting a Privilege Level

	Command	Purpose
Step 1		
Step 2		

Controlling Access Point Access with RADIUS

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points



Security Command Reference

Cisco IOS

[Defining AAA Server Groups, page 10-11 \(optional\)](#)

[Configuring RADIUS Authorization for User Privileged Access and Network Services, page 10-13 \(optional\)](#)

[Displaying the RADIUS Configuration, page 10-14](#)

Default RADIUS Configuration

Configuring RADIUS Login Authentication

Command	Purpose
Step 1	
Step 2	
Step 3 <i>list-name method1 method2...</i>	<ul style="list-style-type: none"> • <i>not</i> • <i>list-name</i> • <i>method1...</i> • <i>password</i> • <p style="text-align: right; color: blue;"><i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i></p>
Step 4 <i>ending-line-number line-number</i>	
<i>list-name</i>	<i>list-name</i>
Step 7	
Step 8	

method1 method2...

list-name

Defining AAA Server Groups

	Command	Purpose
Step 1		
Step 2		

Command	Purpose
<p>Step 3</p> <p>key</p>	<ul style="list-style-type: none"> • auth-port • acct-port • timeout <p>radius-server timeout</p> <p>radius-server host</p> <p>radius-server timeout</p> <ul style="list-style-type: none"> • retransmit <p>radius-server host</p> <p>radius-server retransmit</p> <ul style="list-style-type: none"> • key <p>Note</p> <p>radius-server host</p>
<p>Step 4</p> <p>aaa group server radius</p>	
<p>Step 5</p> <p>server</p>	
<p>Step 6</p> <p>end</p>	
<p>Step 7</p> <p>show running-config</p>	
<p>Step 8</p> <p>copy running-config startup-config</p>	
<p>Step 9</p>	

```

server radius
no radius-server host
no aaa group
no server

```

```

aaa new-model
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
aaa group server radius group1
server 172.20.0.1 auth-port 1000 acct-port 1001
exit
aaa group server radius group2
server 172.20.0.1 auth-port 2000 acct-port 2001
exit

```

Configuring RADIUS Authorization for User Privileged Access and Network Services

```

aaa authorization
radius

```

```

aaa authorization exec radius

```

-
-



Note

	Command	Purpose
Step 1	configure terminal	
Step 2	aaa authorization network radius	
Step 3	aaa authorization exec radius	exec autocommand
Step 4	end	

	Command	Purpose
Step 5		
Step 6		

Displaying the RADIUS Configuration

Controlling Access Point Access with TACACS+



Note

-
-
-
-

Default TACACS+ Configuration

Configuring TACACS+ Login Authentication

	Command	Purpose
Step 1		
Step 2		
Step 3		<ul style="list-style-type: none"> • • • • • tacacs+
Step 4	line console tty vty	
Step 5	login authentication default	<ul style="list-style-type: none"> • default authentication login aaa • login aaa authentication

	Command	Purpose
Step 6		
Step 7		
Step 8		

```
no aaa new-model
no aaa authentication login default
```

```
no login authentication default
```

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

•

•



Note

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

Displaying the TACACS+ Configuration

Administering the Wireless Hardware and Software

-
-
-

Resetting the Wireless Device to the Factory Default Configuration

```
service-module wlan-ap0 reset default-config
```



Caution

```
service-module wlan-ap0 reset
```

Rebooting the Wireless Device

```
service-module wlan-ap0 reload
Enter                               n
```

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

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

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

Monitoring the Wireless Device

-
-

Displaying Wireless Device Statistics

```
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

```
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



Note

-
-
-

Understanding Simple Network Time Protocol

http://www.cisco.com/en/US/docs/ios/12_1/configun/configuration/guide/fcd303.html#wp1001075

Table 2 **SNTP Commands**

[Configuring the Time Zone](#), page 10-21

[Configuring Summer Time \(Daylight Saving Time\)](#), page 10-22

Setting the System Clock

: :	
clock set : :	: :
show running-config	
copy running-config startup-config	

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

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

Displaying the Time and Date Configuration

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

Configuring the Time Zone

configure terminal	
clock timezone	
end	
show running-config	
copy running-config startup-config	

clock timezone AST -3 30

no clock timezone

Configuring Summer Time (Daylight Saving Time)

clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00

clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00

Configuring a System Name and Prompt

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, refer to the [System Name and Prompt Configuration](#) and the [Configuring a System Name](#).

This section contains the following configuration information:

- [Default System Name and Prompt Configuration, page 10-24](#)
- [Configuring a System Name, page 10-24](#)
- [Understanding DNS, page 10-25](#)

Default System Name and Prompt Configuration

The default access point system name and prompt are `AP1` and `AP1>`.

Configuring a System Name

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

Command	Purpose
Step 1	Enters global configuration mode.
Step 2	Manually configures a system name. The default setting is <code>AP1</code> . Note When you change the system name, the wireless device radios reset, and associated client devices disassociate and quickly reassociate. Note 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	Returns to privileged EXEC mode.
Step 4	Verifies your entries.
Step 5	(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 `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`, `ssh`, 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 10-25](#)
- [Setting Up DNS, page 10-26](#)
- [Displaying the DNS Configuration, page 10-27](#)

Default DNS Configuration

Table 10-3 *Default DNS Configuration*

Feature	Default Setting

Setting Up DNS

	Command	Purpose
Step 1		
Step 2		
Step 3	<i>server-address6</i>	



Default Banner Configuration

Configuring a Message-of-the-Day Login Banner

	Return
end	
show running-config	
copy running-config startup-config	

sign (#) is used as the beginning and ending delimiter:

```

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

```

```

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

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Configuring Ethernet Speed and Duplex Settings





	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

Configuring the Access Point for Wireless Network Management

ip-address

Configuring the Access Point for Local Authentication and Authorization



Note

Command	Purpose
Step 1	
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	<ul style="list-style-type: none"> • • • <p style="text-align: center;">7</p> <p style="text-align: center;">username</p>
end	
show running-config	
copy running-config startup-config	

Configuring the Authentication Cache and Profile



Note

cache expiry
cache authorization profile
cache authentication profile
aaa cache profile



Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC

```
!  
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
```

Setting up the DHCP Server



Note

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

<i>high_address</i>	<i>low_address</i>
<i>pool_name</i>	
<i>subnet_number</i> <i>mask prefix-length</i>	
<i>days hours minutes</i>	
<i>address 8</i>	<i>address address2 ...</i>

show Commands

Table 10-4 *Show Commands for DHCP Server*

clear Commands

Table 10-5 *Clear Commands for DHCP Server*

*	*
clear ip dhcp conflict *	
clear ip dhcp server statistics	*

debug Command

Configuring the Access Point for Secure Shell



Note

Understanding SSH

-
-



Note

Configuring SSH

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

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 10-38](#)

[Configuring ARP Caching, page 10-38](#)

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

Configuring ARP Caching

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none">•
Step 3		
Step 4		
Step 5		

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



Note

