



Cisco Aironet 1200 Series Access Point Command Reference

IOS Release 12.2(8)JA
February 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-3447-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)



Preface	vii
Audience	vii
Purpose	vii
Organization	viii
Conventions	viii
Related Publications	ix
Obtaining Documentation	ix
Cisco.com	ix
Documentation CD-ROM	ix
Ordering Documentation	ix
Documentation Feedback	x
Obtaining Technical Assistance	x
Cisco.com	x
Technical Assistance Center	xi
Cisco TAC Website	xi
Cisco TAC Escalation Center	xi
Obtaining Additional Publications and Information	xii

CHAPTER 1

Using the Command-Line Interface	1-1
Type of Memory	1-1
CLI Command Modes	1-1
User EXEC Mode	1-2
Privileged EXEC Mode	1-2
Global Configuration Mode	1-3
Interface Configuration Mode	1-3

CHAPTER 2

Cisco IOS Commands for Access Points	2-1
accounting (ssid configuration mode)	2-1
antenna	2-3
authentication network-eap (ssid configuration mode)	2-4
authentication open (ssid configuration mode)	2-5
authentication shared (ssid configuration mode)	2-7
beacon	2-8

bridge-group port-protected	2-9
broadcast-key	2-10
channel	2-11
class-map	2-14
clear dot11 client	2-16
clear dot11 hold-list	2-17
clear dot11 statistics	2-18
clear iapp rogue-ap-list	2-19
clear iapp statistics	2-20
clear ip proxy-mobile traffic	2-21
clear ip proxy-mobile subnet-map	2-22
debug dot11	2-23
debug dot11 aaa	2-24
debug dot11 dot11radio	2-25
debug iapp	2-27
debug ip proxy-mobile	2-28
dot11 dot11radio antenna-alignment	2-30
dot11 dot11radio linktest	2-31
dot11 dot11radio meter	2-33
dot11 extension aironet	2-34
dot11 holdoff-time	2-35
dot11 igmp snooping-helper	2-36
dot11 network-map	2-37
dot11 phone	2-38
dot1x client-timeout	2-39
dot1x reauth-period	2-40
encryption key	2-41
encryption mode wep	2-43
fragment-threshold	2-44
guest-mode (ssid configuration mode)	2-45
iapp standby mac-address	2-46
iapp standby poll-frequency	2-47
iapp standby timeout	2-48
infrastructure-client	2-49
infrastructure-ssid (ssid configuration mode)	2-50

interface dot11radio	2-51
ip proxy-mobile	2-52
ip proxy-mobile (ssid configuration mode)	2-54
ip proxy-mobile aap	2-56
ip proxy-mobile enable	2-57
ip proxy-mobile pause	2-58
ip proxy-mobile secure	2-59
l2-filter bridge-group-acl	2-60
led flash	2-61
logging buffered	2-62
match (class-map configuration)	2-63
max-associations (ssid configuration mode)	2-65
packet retries	2-66
parent	2-67
parent timeout	2-68
payload-encapsulation	2-69
power client maximum	2-70
power local	2-72
preamble-short	2-73
rts	2-74
show controllers dot11radio	2-75
show dot11 associations	2-76
show dot11 network-map	2-77
show dot11 statistics client-traffic	2-78
show iapp rogue-ap-list	2-79
show iapp standby-parms	2-81
show iapp statistics	2-82
show interfaces dot11radio	2-83
show interfaces dot11radio aaa	2-84
show interfaces dot11radio statistics	2-85
show ip proxy-mobile	2-86
show ip proxy-mobile aaa requests	2-87
show ip proxy-mobile agent	2-88
show ip proxy-mobile detail	2-89
show ip proxy-mobile node	2-90

show ip proxy-mobile registration 2-91

show ip proxy-mobile subnet-map 2-92

show ip proxy-mobile traffic 2-93

show ip proxy-mobile visitor 2-94

show led flash 2-95

speed 2-96

ssid 2-98

station-role 2-100

traffic-class 2-101

vlan (ssid configuration mode) 2-102

world-mode 2-103

APPENDIX A

List of Supported Cisco IOS Commands B-1

A B-1

B B-2

C B-2

D B-3

E B-4

F B-4

G B-4

H B-5

I B-5

L B-6

M B-6

N B-7

P B-7

R B-7

S B-8

T B-10

U B-11

V B-11

W B-11

INDEX



Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Cisco Aironet 1200 Series Access Point, hereafter referred to as the *access point*. Before using this guide, you should have experience working with Cisco IOS commands and access point software features; you also need to be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide provides information about new and revised IOS commands. For information about the standard IOS Release 12.2 commands, refer to the IOS documentation set available from the Cisco.com home page by selecting **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select Release 12.2 from the Cisco IOS Software drop-down list.

This guide does not provide procedures for configuring your access point. For detailed configuration procedures, refer to the *Cisco Aironet 1200 Series Access Point Installation and Configuration Guide* for this release.

Organization

This guide is organized into these sections:

[Chapter 1, “Using the Command-Line Interface,”](#) describes how to access the command modes and use the command-line interface (CLI) to configure software features.

[Chapter 2, “Cisco IOS Commands for Access Points,”](#) describes in alphabetical order the IOS commands that you use to configure and monitor your access point.

[Appendix A, “List of Supported Cisco IOS Commands,”](#) lists the Cisco IOS commands that the access point supports. Cisco IOS commands that are not in this list have not been tested on access points and might not be supported.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([]) means optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ({ { | } }) mean a required choice within an optional element.

Notes, cautions, and warnings use these conventions and symbols:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Warning

The warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Related Publications

These documents provide complete information about the access point and are available from this Cisco.com site:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>

- *Cisco Aironet 1200 Series Access Point Installation and Configuration Guide* describes the major features and how to install and configure the access point.
- *Quick Start Guide: Cisco Aironet 1200 Series Access Point* describes how to attach cables, mount the access point, and how to obtain access point documentation. This document is included in the shipping box with your access point.
- *Release Notes for Cisco Aironet 1200 Series Access Point* describes features, important notes, and caveats for the 1200 series access points running IOS Release 12.2.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can email your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:
http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:
http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Using the Command-Line Interface

This chapter describes how to use the IOS command-line interface (CLI) for configuring software features in the access point.

For a complete description of the new and revised IOS commands supported by the access point, see [Chapter 2, “Cisco IOS Commands for Access Points.”](#)

For more information on Cisco IOS Release 12.2, refer to the *Cisco IOS Release 12.2 Command Summary*.

For task-oriented configuration steps, refer to the *Cisco Aironet 1200 Series Access Point Installation and Configuration Guide*.

Type of Memory

The access point Flash memory stores the Cisco IOS software image, the startup configuration file, and helper files.

CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface** *interface-id* command works only when entered in global configuration mode.

These are the main command modes for the access point:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration

[Table 1-1](#) lists the main command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed use the default name *AP*.

Table 1-1 Command Modes Summary

Command Mode	Access Method	Prompt	Exit
User EXEC	This is the first level of access. Change terminal settings, perform basic tasks, and list system information.	AP>	Enter the logout command.
Privileged EXEC	From user EXEC mode, enter the enable command.	AP#	To exit to user EXEC mode, enter the disable command.
Global configuration	From privileged EXEC mode, enter the configure command.	AP(config)#	To exit to privileged EXEC mode, enter the exit or end command, or press Ctrl-Z .
Interface configuration	From global configuration mode, specify terminal then specify an interface by entering the interface command followed by the interface type and number.	AP(config-if)#	To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z . To exit to global configuration mode, enter the exit command.

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
AP> ?
```

Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#):

```
AP#
```

Enter the **enable** command to access privileged EXEC mode:

```
AP> enable
AP#
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
AP# ?
```

To return to user EXEC mode, enter the **disable** privileged EXEC command.

Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
AP# configure
Configuring from terminal, memory, or network [terminal]?
```

You can specify the terminal or memory as the source of configuration commands.

This example shows you how to access global configuration mode:

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)#
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt:

```
AP(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface** *interface-id* command to access interface configuration mode. The new prompt means interface configuration mode:

```
AP(config-if)#
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt:

```
AP(config-if)# ?
```

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.



Cisco IOS Commands for Access Points

This chapter lists and describes Cisco IOS commands in Cisco IOS Release 12.2(8)JA that you use to configure and manage your access point and your wireless LAN. The commands are listed alphabetically. Refer to [Appendix A, “List of Supported Cisco IOS Commands,”](#) for a complete list of IOS commands supported by the access point.

accounting (ssid configuration mode)

Use the **accounting** ssid configuration mode command to enable RADIUS accounting for the radio interface (for the specified SSID). Use the **no** form of the command to disable accounting.

[no] accounting *list-name*

Syntax Description	<i>list-name</i>	Specifies the name of an accounting list.
---------------------------	------------------	---

Defaults	This command has no defaults.	
-----------------	-------------------------------	--

Command Modes	SSID configuration interface	
----------------------	------------------------------	--

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines	You create accounting lists using the aaa accounting command. These lists indirectly reference the server where the accounting information is stored.
-------------------------	--

Examples	This example shows how to enable RADIUS accounting and set the RADIUS server name: <pre>AP(config-if-ssid)# accounting radius1</pre>
-----------------	--

This example shows how to disable RADIUS accounting:

```
AP(config-if-ssid)# no accounting
```

Related Commands	Command	Description
	ssid	Specifies the SSID and enters the ssid configuration mode

antenna

Use the **antenna** configuration interface command to configure the radio receive or transmit antenna settings. Use the **no** form of this command to reset the receive antenna to defaults.

[no] antenna {receive | transmit} {diversity | left | right}

Syntax Description		
	receive	Specifies the antenna that the access uses to receive radio signals
	transmit	Specifies the antenna that the access uses to transmit radio signals
	diversity	Specifies the antenna with the best signal
	left	Specifies the left antenna
	right	Specifies the right antenna

Defaults The default antenna configuration is **diversity**.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify the right receive antenna option:

```
AP(config-if)# antenna receive right
```

This example shows how to set the receive antenna option to defaults:

```
AP(config-if)# no antenna receive
```

Related Commands	Command	Description
	authentication open (ssid configuration mode)	Configures the radio transmit antenna settings
	show running-config	Displays the current access point operating configuration

authentication network-eap (ssid configuration mode)

Use the **authentication network-eap** ssid configuration mode command to configure the radio interface (for the specified SSID) to support network-EAP authentication with optional MAC address authentication. Use the **no** form of the command to disable network-eap authentication for the SSID.

```
[no] authentication
      network-eap list-name
      [mac-address list-name]
```

Syntax Description		
	<i>list-name</i>	Specifies the list name for EAP authentication
	mac-address <i>list-name</i>	Specifies the list name for MAC authentication

Defaults This command has no defaults.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Use this command to authenticate clients using the network EAP method, with optional MAC address screening. You define list names for MAC addresses and EAP using the **aaa authentication login** command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.

Examples This example shows how to set the authentication to open for devices on a specified address list:

```
AP(config-if-ssid)# authentication network-eap list1
```

This example shows how to reset the authentication to default values:

```
AP(config-if-ssid)# no authentication network-eap
```

Related Commands	Command	Description
	authentication open (ssid configuration mode)	Specifies open authentication
	authentication shared (ssid configuration mode)	Specifies shared-key authentication
	ssid	Specifies the SSID and enters the ssid configuration mode
	show running-config	Displays the current access point operating configuration

authentication open (ssid configuration mode)

Use the **authentication open** ssid configuration mode command to configure the radio interface (for the specified SSID) to support open authentication and optionally MAC address authentication or EAP authentication. Use the **no** form of the command to disable open authentication for the SSID.

```
[no] authentication open
      [mac-address list-name [alternate] ]
      [eap list-name]
```

Syntax Description		
	mac-address list-name	Specifies the list name for MAC authentication
	alternate	Specifies the use of either EAP authentication or MAC address authentication
	eap list-name	Specifies the list name for EAP authentication

Defaults This command has no defaults.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Use this command to authenticate clients using the open method, with optional MAC address or EAP screenings. If you use the **alternate** keyword, the client must pass either the MAC address or EAP authentication. Otherwise, the client must pass both authentications. You define list names for MAC addresses and EAP using the **aaa authentication login** command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.

Examples This example shows how to enable open authentication with MAC address restrictions:

```
AP(config-if-ssid)# authentication open mac-address mac-list1
```

This example shows how to disable open authentication for the SSID:

```
AP(config-if-ssid)# no authentication open
```

Related Commands	Command	Description
	authentication shared (ssid configuration mode)	Specifies shared key authentication

■ authentication open (ssid configuration mode)

Command	Description
authentication network-eap (ssid configuration mode)	Specifies network EAP authentication
ssid	Specifies the SSID and enters the ssid configuration mode

authentication shared (ssid configuration mode)

Use the **authentication shared** ssid configuration mode command to configure the radio interface (for the specified SSID) to support shared authentication with optional MAC address authentication and EAP authentication. Use the **no** form of the command to disable shared authentication for the SSID.

```
[no] authentication shared
      [mac-address list-name]
      [eap list-name]
```

Syntax Description	mac-address list-name	Specifies the list name for MAC authentication
	eap list-name	Specifies the list name for EAP authentication

Defaults This command has no defaults.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Use this command to authenticate clients using the shared method, with optional MAC address or EAP screenings. You define list names for MAC addresses and EAP using the **aaa authentication login** command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.

Examples This example shows how to set the authentication to shared for devices on a MAC address list:

```
AP(config-if-ssid)# authentication shared mac-address mac-list1
```

This example shows how to reset the authentication to default values:

```
AP(config-if-ssid)# no authentication shared
```

Related Commands	Command	Description
	authentication open (ssid configuration mode)	Specifies open authentication
	authentication network-eap (ssid configuration mode)	Specifies network EAP authentication
	ssid	Specifies the SSID and enters the ssid configuration mode
	show running-config	Displays the current access point operating configuration

beacon

Use the **beacon** configuration interface command to specify how often the beacon contains a Delivery Traffic Indicator Message (DTIM). Use the **no** form of this command to reset the beacon interval to defaults.

[no] beacon {period *Kms* | dtim-period *count*}

Syntax Description	period <i>Kms</i>	dtim-period <i>count</i>
	Specifies the beacon time in Kilomicroseconds (Kms). Kms is a unit of measurement in software terms. K = 1024, m = 10 ⁻⁶ , and s = seconds, so Kms = 0.001024 seconds, 1.024 milliseconds, or 1024 microseconds.	Specifies the number of DTIM beacon periods to wait before delivering multicast packets.

Defaults
 The default **period** is 100.
 The default **dtim-period** is 2.

Command Modes
 Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines
 Clients normally wake up each time a beacon is sent to check for pending packets. Longer beacon periods let the client sleep longer and preserve power. Shorter beacon periods reduce the delay in receiving packets.
 Controlling the DTIM period has a similar power-saving result. Increasing the DTIM period count lets clients sleep longer, but delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

Examples
 This example shows how to specify a beacon period of 15 Kms (15.36 milliseconds):

```
AP(config-if)# beacon period 15
```

This example shows how to set the beacon parameter to defaults:

```
AP(config-if)# no beacon
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

bridge-group port-protected

Use the **bridge-group port-protected** configuration interface command to enable protected port for public secure mode configuration. In IOS, there is no exchange of unicast, broadcast, or multicast traffic between protected ports.

```
bridge-group bridge-group
port-protected
```

Syntax Description	<i>bridge-group</i>	Specifies the bridge group for port protection
---------------------------	---------------------	--

Defaults	This command has no defaults.
-----------------	-------------------------------

Command Modes	Configuration interface
----------------------	-------------------------

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to enable protected port for bridge group 71:

```
AP(config-if)# bridge-group 71 port-protected
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

broadcast-key

Use the **broadcast-key** configuration interface command to configure the time interval between rotations of the broadcast encryption key used for clients. Use the **no** form of the command to disable broadcast key rotation.

```
[no] broadcast-key
      [vlan vlan-id]
      [change secs]
```

Syntax Description	vlan <i>vlan-id</i>	(Optional) Specifies the virtual LAN identification value
	change <i>secs</i>	(Optional) Specifies the amount of time (in seconds) between the rotation of the broadcast encryption key

Defaults The default **change** time is specified by the IEEE 802.11 dot1x EAP.

Command Modes Configuration interface

Command History	Release	Modification
		12.2(4)JA

Examples This example shows how to configure vlan10 to support broadcast key encryption with a 5-minute key rotation interval:

```
AP(config-if)# broadcast-key vlan 10 change 300
```

This example shows how to disable broadcast key rotation:

```
AP(config-if)# no broadcast-key
```

channel

Use the **channel** configuration interface command to set the radio channel frequency. Use the **no** form of this command to reset the channel frequency to defaults.

[no] channel { *number* | *frequency* | **least-congested** }

Syntax Description		
<i>number</i>	Specifies a channel number. For a list of channels for the 2.4-GHz radio, see Table 2-1 . For a list of channels for the 5-GHz radio, see Table 2-2 .	Note The valid numbers depend on the channels allowed in your regulatory region and are set during manufacturing.
<i>frequency</i>	Specifies the center frequency for the radio channel. For a list of center frequencies for the 2.4-GHz radio, see Table 2-1 . For a list of center frequencies for the 5-GHz radio, see Table 2-2 .	Note The valid frequencies depend on the channels allowed in your regulatory region and are set during manufacturing.
least-congested	Enables or disables the scanning for a least busy radio channel to communicate with the client adapter	

Table 2-1 Channels and Center Frequencies for 2.4-GHz Radios

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Japan (-J)	Israel (-I)	China (-C)
1	2412	X	X	X	-	X
2	2417	X	X	X	-	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	X	-	X
11	2462	X	X	X	-	X
12	2467	-	X	X	-	-
13	2472	-	X	X	-	-
14	2484	-	-	X	-	-

Table 2-2 Channels and Center Frequencies for 5-GHz Radios

Channel Identifier	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170	-	X	-	-
36	5180	X	-	X	-
38	5190	-	X	-	-
40	5200	X	-	X	-
42	5210	-	X	-	-
44	5220	X	-	X	-
46	5230	-	X	-	-
48	5240	X	-	X	-
52	5260	X	-	-	X
56	5280	X	-	-	X
60	5300	X	-	-	X
64	5320	X	-	-	X
149	5745	-	-	-	-
153	5765	-	-	-	-
157	5785	-	-	-	-
161	5805	-	-	-	-



Note All channel sets for the 5-GHz radio are restricted to indoor usage except the Americas (-A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.

Defaults

The default channel is **least-congested**.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(8)JA	Parameters were added to support the 5-GHz radio.

Examples

This example shows how to set the access point radio to channel 10 with a center frequency of 2457.

```
AP(config-if)# channel 2457
```

This example shows how to set the access point to scan for the least-congested radio channel.

```
AP(config-if)# channel least-congested
```

This example shows how to set the beacon parameter to defaults:

```
AP(config-if)# no channel
```

Related Commands

Command	Description
show controllers dot11radio	Displays the radio controller information and status

class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map and return to global configuration mode.

[no] class-map *name*

Syntax	Description
<i>name</i>	Specifies the name of the class map

Defaults	Description
	This command has no defaults, and there is not a default class map.

Command Modes	Description
	Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines	Description
	Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode. In this mode, you can enter one match command to configure the match criterion for this class.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class-map.
- **exit**: exits from QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the [match \(class-map configuration\)](#) command.
- **no**: removes a match statement from a class map.
- **rename**: renames the current class map. If you rename a class map with a name already in use, the message `A class-map with this name already exists` is displayed.

Only one match criterion per class map is supported. For example, when defining a class map, only one **match** command can be issued.

Because only one **match** command per class map is supported, the **match-all** and **match-any** keywords function the same.

Only one access control list (ACL) can be configured in a class map. The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called *class1*. *class1* has one match criterion, which is an access list called *103*.

```
AP(config)# access-list 103 permit any any dscp 10
AP(config)# class-map class1
AP(config-cmap)# match access-group 103
AP(config-cmap)# exit
```

This example shows how to delete the class map *class1*:

```
AP(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
match (class-map configuration)	Defines the match criteria ACLs, IP precedence, or IP Differentiated Services Code Point (DSCP) values to classify traffic
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy
show class-map	Displays QoS class maps

clear dot11 client

Use the **clear dot11 client** privileged EXEC command to deauthenticate a radio client with a specified media access control (MAC) address. The client must be directly associated with the access point, not a repeater.

clear dot11 client *{mac-address}*

Syntax Description	<i>mac-address</i>	Specifies a radio client MAC address (in xxxx.xxxx.xxxx format)
--------------------	--------------------	---

Defaults	This command has no defaults.
----------	-------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples	This example shows how to deauthenticate a specific radio client:
----------	---

```
AP# clear dot11 client 0040.9645.2196
```

You can verify that the client was deauthenticated by entering the following privileged EXEC command:

```
AP# show dot11 associations 0040.9645.2196
```

Related Commands	Command	Description
	show dot11 associations	Displays the radio association table or optionally displays association statistics or association information about repeaters or clients

clear dot11 hold-list

Use the **clear dot11 hold-list** privileged EXEC command to reset the MAC, LEAP, and EAP authentications hold list.

clear dot11 hold-list

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to clear the hold-off list of MAC authentications:

```
AP# clear dot11 hold-list
```

clear dot11 statistics

Use the **clear dot11 statistics** privileged EXEC command to reset statistic information for a specific radio interface or for a particular client with a specified MAC address.

```
clear dot11 statistics
    {interface | mac-address}
```

Syntax Description		
	<i>interface</i>	Specifies a radio interface number
	<i>mac-address</i>	Specifies a client MAC address (in xxxx.xxxx.xxxx format)

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to clear radio statistics for radio interface 0:

```
AP# clear dot11 statistics dot11radio 0
```

This example shows how to clear radio statistics for the client radio with a MAC address of 0040.9631.81cf:

```
AP# clear dot11 statistics 0040.9631.81cf
```

You can verify that the radio interface statistics are reset by entering the following privileged EXEC command:

```
AP# show dot11 associations statistics
```

Related Commands	Command	Description
	show dot11 statistics client-traffic	Displays client traffic statistics
	show interfaces dot11radio	Displays radio interface information
	show interfaces dot11radio statistics	Displays radio interface statistics

clear iapp rogue-ap-list

Use the **clear iapp rogue-ap-list** privileged EXEC command to clear the list of IAPP rogue access points.

clear iapp rogue-ap-list

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to clear the IAPP rogue access point list:

```
AP# clear iapp rogue-ap-list
```

You can verify that the rogue AP list was deleted by entering the **show iapp rogue-ap-list** privileged EXEC command.

Related Commands	Command	Description
	show iapp rogue-ap-list	Displays the IAPP rogue access point list

clear iapp statistics

Use the **clear iapp statistics** privileged EXEC command to clear all the IAPP statistics.

clear iapp statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to clear the IAPP statistics:

```
AP# clear iapp statistics
```

You can verify that the IAPP statistics were cleared by entering the following privileged EXEC command:

```
AP# show iapp statistics
```

Related Commands	Command	Description
	show iapp statistics	Displays the IAPP transmit and receive statistics

clear ip proxy-mobile traffic

Use the **clear ip proxy-mobile traffic** privileged EXEC command to clear all the statistics related to proxy Mobile IP.

clear ip proxy-mobile traffic

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to clear the proxy-mobile statistics:

```
AP# clear ip proxy-mobile traffic
```

You can verify that traffic statistics are cleared by entering the **show ip proxy-mobile traffic** privileged EXEC command.

Related Commands	Command	Description
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile traffic	Displays proxy Mobile IP statistics

clear ip proxy-mobile subnet-map

Use the **clear ip proxy-mobile subnet-map** privileged EXEC command to clear the proxy Mobile IP subnet map table and obtain a new table from the AAP. On an AAP, this command immediately synchronizes its tables with the other AAPs.

clear ip proxy-mobile subnet-map

This command has no arguments or keywords.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Examples

This example shows how to clear the proxy Mobile IP subnet map:

```
AP# clear ip proxy-mobile subnet-map
```

You can verify that information was deleted by entering the **show ip proxy-mobile subnet-map** privileged EXEC command.

Related Commands

Command	Description
show ip proxy-mobile subnet-map	Displays the subnet map table
show ip proxy-mobile	Displays information about proxy Mobile IP
show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

debug dot11

Use the **debug dot11** privileged EXEC command to begin debugging of radio functions. Use the **no** form of this command to stop the debug operation.

[no] debug dot11
 {events | packets | forwarding | mgmt | network-map | syslog | virtual-interface }

Syntax Description		
	events	Activates debugging of all radio related events
	packets	Activates debugging of radio packets received and transmitted
	forwarding	Activates debugging of radio forwarded packets
	mgmt	Activates debugging of radio access point management activity
	network-map	Activates debugging of radio association management network map
	syslog	Activates debugging of radio system log
	virtual-interface	Activates debugging of radio virtual interfaces

Defaults Debugging is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to begin debugging of all radio-related events:

```
AP# debug dot11 events
```

This example shows how to begin debugging of radio packets:

```
AP# debug dot11 packets
```

This example shows how to begin debugging of the radio system log:

```
AP# debug dot11 syslog
```

This example shows how to stop debugging of all radio related events:

```
AP# no debug dot11 events
```

Related Commands	Command	Description
	show debugging	Displays all debug settings and the debug packet headers
	show interfaces dot11radio	Displays configuration and status information for the radio interface

debug dot11 aaa

Use the **debug dot11 aaa** privileged EXEC command to begin debugging of dot11 authentication, authorization, and accounting (AAA) operations. Use the **no** form of this command to stop the debug operation.

```
[no] debug dot11 aaa
      {accounting | dispatcher |
      dot1x {all | broadcast-key | process} | rxdata | state-machine | txdata} | mac-authen}
```

Syntax Description		
	accounting	Activates debugging of 802.11 AAA accounting packets
	dispatcher	Activates debugging of 802.11 AAA dispatcher (interface between Association & Manager) packets
	all	Activates debugging of all IEEE 802.1x AAA packets
	broadcast-key	Activates debugging of IEEE 802.1x AAA broadcast-key change packets
	process	Activates debugging of IEEE 802.1x AAA process packets
	rxdata	Activates debugging of IEEE 802.1x AAA receive packets from clients
	state-machine	Activates debugging of IEEE the 802.1x AAA state machine
	txdata	Activates debugging of IEEE 802.1x AAA transmit packets to clients
	mac-authen	Activates debugging of 802.11 AAA MAC authentication packets

Defaults Debugging is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to begin debugging of dot11 AAA accounting packets:

```
AP# debug dot11 aaa accounting
```

This example shows how to begin debugging of all dot1x AAA packets:

```
AP# debug dot11 aaa dot1x all
```

Related Commands	Command	Description
	show debugging	Displays all debug settings
	show interfaces dot11radio aaa	Optionally displays all radio clients

debug dot11 dot11radio

Use the **debug dot11 dot11radio** privileged EXEC command to turn on radio debug options. These options include run RF monitor mode and trace frames received or transmitted on the radio interface. Use the **no** form of this command to stop the debug operation.

```
[no] debug dot11 dot11radio interface-number { dump | flash |
monitor { ack | address | beacon | crc | lines | plcp | print | probe | store } |
trace { lines | off | print | store } }
```

Syntax Description

<i>interface-number</i>	Specifies a radio interface number (the 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1).
dump	Enables driver event dumping
flash	Enables flash radio firmware debugging
monitor	Enables RF monitor mode
ack	Displays ACK packets. ACK packets acknowledge receipt of a signal, information, or packet.
address	Displays packets to or from the specified IP address
beacon	Displays beacon packets
crc	Displays packets with CRC errors
lines	Specifies a print line count
plcp	Displays plcp packets
print	Enables RF monitor printing mode
probe	Displays probe packets
store	Enables RF monitor storage mode
trace	Enables trace mode
lines	Specifies a trace print line count
off	Turns tracing off
print	Enables trace printing
store	Enables trace storage mode

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Examples

This example shows how to begin dumping of driver event packets to the logging buffer:

■ debug dot11 dot11radio

```
AP# debug dot11 dot11radio 0 dump
```

This example shows how to begin debugging of the radio firmware:

```
AP# debug dot11 dot11radio 0 flash
```

This example shows how to begin monitoring of all 801.11 radio packets:

```
AP# debug dot11 dot11radio 0 monitor
```

This example shows how to stop monitoring of all radio packets:

```
AP# no debug dot11 dot11radio 0 monitor
```

Related Commands

Command	Description
show debugging	Displays all debug settings and the debug packet headers
show interfaces dot11radio	Displays configuration and status information for the radio interface
show interfaces dot11radio statistics	Displays radio interface statistics

debug iapp

Use the **debug iapp** privileged EXEC command to begin debugging of IAPP operations. Use the **no** form of this command to stop the debug operation.

```
[no] debug iapp
      {packets | event | error}
```

Syntax Description		
	packets	Displays IAPP packets sent and received by the access point. Link test packets are not displayed
	event	Displays significant IAPP events
	error	Displays IAPP software and protocol errors

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to begin debugging of IAPP packets:

```
AP# debug iapp packet
```

This example shows how to begin debugging of IAPP events:

```
AP# debug iapp events
```

This example shows how to begin debugging of IAPP errors:

```
AP# debug iapp errors
```

Related Commands	Command	Description
	show debugging	Displays all debug settings

debug ip proxy-mobile

Use the **debug ip proxy-mobile** privileged EXEC command to begin debugging of proxy Mobile IP activities. If a component is not specified in the command, debugging of all components is activated. Use the **no** form of this command to stop the debug operation and return to the default configuration.

[no] debug ip proxy-mobile
[subnet-map] [agent-disc] [registration]

Syntax Description	Command	Description
	subnet-map	(Optional) Activates debugging of subnet mapping
	agent-disc	(Optional) Activates debugging of agent discovery
	registration	(Optional) Activates debugging of registration events

Defaults Debugging is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was first introduced.

Examples This example shows how to begin debugging of all proxy-mobile activities:

```
AP# debug ip proxy-mobile
```

This example shows how to begin debugging of registration events:

```
AP# debug ip proxy-mobile registration
```

This example shows how to stop debugging of registration events:

```
AP# no debug ip proxy-mobile registration
```

You can check debugging information by entering the **show debugging** privileged EXEC command.

Related Commands	Command	Description
	show debugging	Displays all debug settings and the debug packet headers
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile aaa requests	Displays information about MN that have pending proxy Mobile IP AAA requests
	show ip proxy-mobile agent	Displays information about the discovered agents
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

Command	Description
show ip proxy-mobile node	Displays information about a specific node or about all the nodes on the access point
show ip proxy-mobile registration	Displays information about the pending and accepted registrations
show ip proxy-mobile subnet-map	Displays the subnet map table
show ip proxy-mobile traffic	Displays proxy Mobile IP statistics
show ip proxy-mobile visitor	Displays visiting proxy Mobile IP nodes

dot11 dot11radio antenna-alignment

Use the **dot11 dot11radio antenna-alignment** privileged EXEC command to activate the antenna-alignment tool for a radio interface. Use this tool to test and align the access point antenna with another remote antenna.

dot11 dot11radio *interface-number* **antenna-alignment** [*timeout*]

Syntax Description		
	<i>interface-number</i>	Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)
	<i>timeout</i>	Specifies the duration of the alignment test, in seconds

Defaults The default alignment timeout is 5 seconds.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines During the antenna alignment test, the radio disassociates from its parent, probes adjacent access points, and records the MAC address and signal strength of responses it receives. After the timeout, the radio reassociates with its parent. Clients connected to the access point through its parent lose their connection for the duration of the test; clients connected to a repeater maintain their connection and can abort the test using the escape sequence (Ctrl key and ^ key).

You display the last 10 results using the **show dot11 antenna-alignment** command, which lists the MAC address and signal level for the access points that responded to the probe.

Examples This example shows how to start the antenna-alignment test for radio interface 0:

```
AP# dot11 dot11radio 0 antenna-alignment
```

Related Commands	Command	Description
	show dot11 associations	Displays the radio association table
	show dot11 network-map	Displays the radio network map

dot11 dot11radio linktest

Use the **dot11 dot11radio linktest** privileged EXEC command to test a radio link between the access point and a client device.

```
dot11 dot11radio interface-number linktest
  [target mac-address]
  [count packet-number]
  [interval sec]
  [packet-size size]
  [rate value]
```

Syntax Description		
<i>interface-number</i>		Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)
target <i>mac-address</i>		(Optional) Specifies the MAC address (in xxxx.xxxx.xxxx format) of the client device
count <i>packet-number</i>		(Optional) Specifies the number of packets (1 to 9999) to send to the client device
interval <i>sec</i>		(Optional) Specifies the time interval between tests (from 1 to 10000 seconds)
packet-size <i>size</i>		(Optional) Specifies the size of each packet (from 1 to 1400 bytes)
rate <i>value</i>		(Optional) Specifies a specific link test data rate. Rates for the 2.4-GHz radio are 1, 2, 5, or 11 Mbps. Rates for the 5-GHz radio are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

Defaults

The default **target** for a root access point is the first client. The default **target** for a repeater is its parent access point.

The default **count** specifies that test runs once.

The default **interval** is 5 seconds.

The default **packet-size** is 512 bytes.

The default **rate** is the automatic rate-shifting algorithm.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Usage Guidelines

The link test verifies the radio link between the access point and a client device by sending the client a series of special packets, which the client returns to the access point. The client adds information to the packets that quantify how well it received the request. Results are displayed as a table of packet statistics, quality, and signal-level information.

If you specify an interval, the test repeats continuously separated by the specified number of seconds. To abort the test, type the escape sequence (**Ctrl** key and **^** key). Without an interval, the test runs once.

Examples

This example shows how to initiate a radio link test to send 10 packets to client MAC address 0040963181CF on radio interface 0:

```
AP# dot11 dot11radio 0 linktest target 0040.9631.81CF count 10
```

This example shows how to initiate a radio link test to send 100 packets of 500 bytes to client MAC address 0040963181CF on radio interface 0:

```
AP# dot11 dot11radio 0 linktest target 0040.9631.81CF packet-size 500 count 100
```

Related Commands

Command	Description
show interfaces dot11radio statistics	Displays the radio statistics
show dot11 associations	Displays the radio association table
show dot11 network-map	Displays the radio network map

dot11 dot11radio meter

Use the **dot11 dot11radio meter** privileged EXEC command to measure the performance of packet forwarding. To display the results, use the **show dot11 statistics metered-traffic** command.

dot11 dot11radio *interface-number* **meter**

Syntax Description	<i>interface-number</i>	Specifies the radio interface number. The 2.4-GHz radio is radio 0. The 5-GHz radio is radio 1.
---------------------------	-------------------------	---

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to activate the meter tool for radio interface 0:

```
AP# dot11 dot11radio 0 meter
```

Related Commands	Command	Description
	show dot11 statistics metered-traffic	Displays packet forwarding performance

dot11 extension aironet

Use the **dot11 extension aironet** configuration interface command to enable or disable Cisco Aironet extensions to the IEEE 802.11b standard. Use the **no** form of this command to disable the Cisco Aironet extensions.

[no] dot11 extension aironet

Syntax Description This command has no arguments or keywords.

Defaults Cisco Aironet extensions are disabled by default.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines The Cisco Aironet extensions help clients choose the best access point. You must enable these extensions to use advanced features such as Cisco MIC and key hashing. Disable these extensions for non-Cisco clients that misinterpret the extensions.

Examples This example shows how to enable Cisco Aironet extensions for the radio interface:

```
AP(config-if)# dot11 extension aironet
```

This example shows how to disable Cisco Aironet extensions for the radio interface:

```
AP(config-if)# no dot11 extension aironet
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

dot11 holdoff-time

Use the **dot11 holdoff-time** configuration interface command to specify the hold-off time for MAC address authentication. Use the **no** form of the command to reset the parameter to defaults.

[no] dot11 holdoff-time *seconds*

Syntax Description	<i>seconds</i>	Specifies the hold-off time (1 to 65555 seconds)				
Defaults	The default holdoff-time is 0 (disabled).					
Command Modes	Configuration interface					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(4)JA</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(4)JA	This command was introduced.	
Release	Modification					
12.2(4)JA	This command was introduced.					
Examples	<p>This example shows how to specify a 2-minute hold-off time.</p> <pre>AP(config-if)# dot11 holdoff-time 120</pre> <p>This example shows how reset the hold-off time to defaults.</p> <pre>AP(config-if)# dot11 no holdoff-time</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show running-config</td> <td>Displays information on the current running access point configuration</td> </tr> </tbody> </table>	Command	Description	show running-config	Displays information on the current running access point configuration	
Command	Description					
show running-config	Displays information on the current running access point configuration					

dot11 igmp snooping-helper

Use the **dot11 igmp snooping-helper** global configuration command to begin sending IGMP Query requests when a new client associates with the access point. Use the **no** form of this command to disable the IGMP Query requests.

[no] dot11 igmp snooping-helper

Syntax Description This command has no arguments or keywords.

Defaults IGMP Query requests are disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to enable IGMP Query requests:

```
AP(config)# dot11 igmp snooping-helper
```

This example shows how to stop or disable the IGMP Query requests:

```
AP(config)# no dot11 igmp snooping-helper
```

dot11 network-map

Use the **dot11 network-map** global configuration command to enable the radio network map feature. When enabled, the access point broadcasts a IAPP GenInfo Request every collection interval. This request solicits information from all Cisco access points in the same Layer 2 domain. Upon receiving a GetInfo Request, the access point sends a unicast IAPP GenInfo Response back to the requester. The access point uses these IAPP GenInfo Responses to build a network-map.

dot11 network-map [*collect-interval*]

Syntax Description	<i>collect-interval</i>	Specifies the time interval between IAPP GenInfo Requests (1 to 60 seconds)
Defaults	The default collect interval is 5 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(4)JA	This command was introduced.
Examples	<p>This example shows how to generate a radio network map with a collection interval of 30 seconds:</p> <pre>AP(config)# dot11 network-map 30</pre> <p>You can verify the network map by using the show dot11 network-map EXEC command.</p>	
Related Commands	Command	Description
	show dot11 network-map	Displays the radio network map

dot11 phone

Use the **dot11 phone** global configuration command to enable or disable IEEE 802.11 compliance phone support. Use the **no** form of this command to disable the IEEE 802.11 phone.

[no] dot11 phone

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Enabling IEEE 802.11 compliance phone support adds information to the access point beacons and probe responses. This information helps some 802.11 phones make intelligent choices about the access point to which they should associate. Some phones do not associate with an access point without this additional information.

Examples This example shows how to enable IEEE 802.11 phone support:

```
AP(config)# dot11 phone
```

This example shows how to stop or disable the IEEE 802.11 phone support:

```
AP(config)# no dot11 phone
```

dot1x client-timeout

Use the **dot1x client-timeout** configuration interface command to configure the IEEE 802.1x (dot1x) client timeout value.

```
dot1x client-timeout 1-65555
```

Syntax Description	<i>1-65555</i>	Specifies a number of seconds (1 to 65555)
Defaults	The default timeout is 10 seconds.	
Command Modes	Configuration interface	
Command History	Release	Modification
	12.2(4)JA	This command was introduced.
Examples	This example shows how to configure a 2-minute dot1x client timeout value: <pre>AP(config-if)# dot1x client-timeout 120</pre>	
Related Commands	Command	Description
	show interfaces dot1x radio aaa	Displays radio AAA timeout values

dot1x reauth-period

Use the **dot1x reauth-period** configuration interface command to configure the dot1x client-reauthentication period. The no form of the command disables reauthentication.

[no] dot1x reauth-period {1-65555 / server}

Syntax Description		
	<i>1-65555</i>	Specifies a number of seconds (1 to 65555)
	server	Specifies server reauthentication

Defaults The default is disabled.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to configure a 2-minute dot1x client-reauthentication period:

```
AP(config-if)# dot1x reauth-period 120
```

Related Commands	Command	Description
	show interfaces dot11radio aaa	Displays radio AAA timeout values

encryption key

Use the **encryption key** configuration interface command to define a WEP key used for data encryption on the wireless LAN or on a specific virtual LAN (VLAN). Use the **no** form of the command to remove a specific encryption key.

```
[no] encryption
    [vlan vlan-id ]
    key 1-4
    size {40bit | 128Bit}
    encryption-key
    [transmit-key]
```

Syntax Description		
vlan <i>vlan-id</i>		Specifies the VLAN number (1 to 4095)
key <i>1-4</i>		Specifies the number of the key (1 to 4) that is being configured. (A total of four encryption keys can be configured for each VLAN.)
size 40bit		Specifies a 40-bit encryption key
size 128bit		Specifies a 128-bit encryption key
<i>encryption-key</i>		Specifies the value of the encryption key: <ul style="list-style-type: none"> • A 40-bit encryption key requires 10 (hexadecimal) digits. • A 128-bit encryption key requires 26 (hexadecimal) digits.
transmit-key		Specifies the key for encrypting transmit data from the access point

Defaults This command has no defaults.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to configure a 40-bit encryption key with a value of *11aa33bb55* as WEP key 1 used on VLAN number 1:

```
AP(config-if)# encryption vlan 1 key 1 size 40bit 11aa33bb55 transmit-key
```

This example shows how to remove WEP key 1 on VLAN 1:

```
AP(config-if)# no encryption vlan 1 key 1
```

■ encryption key

Related Commands

Command	Description
show running-config	Displays the current access point operating configuration

encryption mode wep

Use the **encryption mode wep** configuration interface command to enable a specific encryption type that is used to communicate on the wireless LAN or on a specific VLAN. When encryption is enabled, all client devices on the wireless LAN or on a VLAN must support the specified encryption methods to communicate with the access point. Use the **no** form of the command to disable the encryption features on a specific VLAN.

```
[no] encryption [vlan vlan-id ] mode wep
      { mandatory | optional }
      { key-hash | mic [key-hash] }
```

Syntax Description		
vlan <i>vlan-id</i>	(Optional)	Specifies the VLAN number
mandatory		Specifies that encryption is mandatory for the client to communicate with the access point
optional		Specifies that client devices can communicate with the access point with or without using encryption
key-hash	(Optional)	Specifies that encryption key hashing is required for client devices to communicate with the access point
mic	(Optional)	Specifies that encryption with message integrity check (MIC) is required for client devices to communicate with the access point

Defaults This command has no defaults.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify that encryption key hashing must be used on VLAN number 1:

```
AP(config-if)# encryption vlan 1 mode wep mandatory key-hash
```

This example shows how to disable mandatory encryption on VLAN 1:

```
AP(config-if)# no encryption vlan 1 mode wep mandatory
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

fragment-threshold

Use the **fragment-threshold** configuration interface command to set the size at which packets are fragmented. Use the **no** form of the command to reset the parameter to defaults.

[no] fragment-threshold 256-2346

Syntax Description	<i>256-2346</i>	Specifies the packet fragment threshold size (256 to 2346 bytes)
---------------------------	-----------------	--

Defaults The default threshold is 2346 bytes

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to set the packet fragment threshold size to 1800 bytes:

```
AP(config-if)# fragment-threshold 1800
```

This example shows how to reset the packet fragment threshold size to defaults:

```
AP(config-if)# no fragment-threshold
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

guest-mode (ssid configuration mode)

Use the **guest-mode** ssid configuration mode command to configure the radio interface (for the specified SSID) to support guest mode. Use the **no** form of the command to disable the guest mode.

[no] guest-mode

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines The access point can have one guest-mode SSID or none at all. The guest-mode SSID is used in beacon frames and response frames to probe requests that specify the empty or wildcard SSID. If no guest-mode SSID exists, the beacon contains no SSID and probe requests with the wildcard SSID are ignored. Disabling the guest mode makes the networks slightly more secure. Enabling the guest mode helps clients that passively scan (do not transmit) associate with the access point. It also allows clients configured without a SSID to associate.

Examples This example shows how to set the wireless LAN for the specified SSID into guest mode:

```
AP(config-if-ssid)# guest-mode
```

This example shows how to reset the guest-mode parameter to default values:

```
AP(config-if-ssid)# no guest-mode
```

Related Commands	Command	Description
	ssid	Specifies the SSID and enters the ssid configuration mode
	show running-config	Displays the current access point operating configuration

iapp standby mac-address

Use the **iapp standby mac-address** global configuration command to configure an access point to be in standby mode and specify the active access point's MAC address. Use the **no** form of this command to disable the access point standby mode.

[no] iapp standby mac-address *mac-address*

Syntax	Description
<i>mac-address</i>	Specifies the MAC address (in xxxx.xxxx.xxxx format) of the active access point

Defaults This command has no default setting.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to place the access point in standby mode and indicate the MAC address of the active access point:

```
AP(config)# iapp standby mac-address 0040.9631.81cf
```

This example shows how to stop or disable the standby mode:

```
AP(config)# no iapp standby mac-address 0040.9631.81cf
```

Related Commands	Command	Description
	iapp standby poll-frequency	Configures the polling interval in standby mode
	iapp standby timeout	Configures the polling timeout value in standby mode

iapp standby poll-frequency

Use the **iapp standby poll-frequency** global configuration command to configure the standby mode polling interval. Use the **no** form of this command to clear the access point standby mode poll frequency.

[no] iapp standby poll-frequency *sec* [*mac-address*]

Syntax Description		
	<i>sec</i>	Specifies the standby mode poll frequency in seconds
	<i>mac-address</i>	Specifies the MAC address of an access point

Defaults This command has no defaults.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify the standby mode poll frequency of 5 minutes:

```
AP(config)# iapp standby poll-frequency 300
```

This example shows how to stop or disable the standby mode:

```
AP(config)# no iapp standby mac-address 0040.9631.81cF
```

Related Commands	Command	Description
	logging buffered	Places the access point into standby mode and identifies the MAC address of the active access point
	iapp standby timeout	Specifies the access point standby mode polling timeout value

iapp standby timeout

Use the **iapp standby timeout** global configuration command to configure the standby mode polling timeout value. Use the **no** form of this command to clear the standby mode polling timeout value.

[no] iapp standby timeout *sec*

Syntax Description	<i>sec</i>	Specifies the standby mode polling timeout in seconds
---------------------------	------------	---

Defaults This command has no defaults.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify the standby mode polling timeout of 1 minute:

```
AP(config)# iapp standby timeout 60
```

This example shows how to clear the standby mode timeout value:

```
AP(config)# no iapp standby timeout
```

Related Commands	Command	Description
	logging buffered	Places the access point into standby mode and identifies the MAC address of the active access point
	iapp standby poll-frequency	Specifies the standby mode polling interval

infrastructure-client

Use the **infrastructure-client** configuration interface command to configure a virtual interface for a workgroup bridge client. Use the **no** form of the command to disable the workgroup bridge client virtual interface.

[no] infrastructure-client

Syntax Description This command has no arguments or keywords.

Defaults The default is infrastructure client disabled.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Enable the infrastructure client feature to increase the reliability of multicast messages to workgroup bridges. When enabled, the access point sends directed packets containing the multicasts, which are retried if necessary, to the associated workgroup bridge. Enable only when necessary because it can greatly increase the load on the radio cell.

Examples This example shows how to configure a virtual interface for a workgroup bridge client.

```
AP(config-if)# infrastructure-client
```

This example shows how to specify that a workgroup bridge client virtual interface is not supported.

```
AP(config-if)# no infrastructure-client
```

Related Commands	Command	Description
	show running-config	Displays information on the current running access point configuration

infrastructure-ssid (ssid configuration mode)

Use the **infrastructure-ssid** command in ssid configuration mode to reserve this SSID for infrastructure associations, such as those from one access point to another. Use the **no** form of the command to revert to a normal non-infrastructure SSID.

[no] infrastructure-ssid

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines This command controls the SSID that access points use when associating with one another. A root access point only allows a repeater access point to associate using this SSID. A repeater access point uses this SSID to associate with its parent. Configure authentication types and VLANs for an SSID to control the security of the access points.

Examples This example shows how to reserve the specified SSID for infrastructure associations on the wireless LAN:

```
AP(config-if-ssid)# infrastructure-ssid
```

This example shows how to restore the SSID to non-infrastructure associations:

```
AP(config-if-ssid)# no infrastructure-ssid
```

Related Commands	Command	Description
	ssid	Specifies the SSID and enters the ssid configuration mode

interface dot11radio

Use the **interface dot11radio** global configuration command to place access point into the radio configuration mode.

interface dot11radio *interface-number*

Syntax Description	<i>interface-number</i>	Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)
--------------------	-------------------------	--

Defaults The default radio interface number is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to place the access point into the radio configuration mode:

```
AP# interface dot11radio 0
```

Related Commands	Command	Description
	show interfaces dot11radio	Displays the radio interface configuration and statistics

ip proxy-mobile

Use the **ip proxy-mobile** configuration interface command to enable the access point to participate in proxy Mobile IP operations. Use the **no** form of this command to disable proxy Mobile IP operations on the access point.

[no] ip proxy-mobile

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to enable the proxy Mobile IP interface on the access point.

```
AP(config-if)# ip proxy-mobile
```

This example shows how to disable proxy Mobile IP operations on the access point.

```
AP(config-if)# no ip proxy-mobile
```

Related Commands	Command	Description
	clear ip proxy-mobile subnet-map	Clears the proxy Mobile IP subnet map and obtains a new table from the AAP
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile aaa requests	Displays information about mobile nodes that have pending proxy Mobile IP AAA requests
	show ip proxy-mobile agent	Displays information about the discovered proxy Mobile IP agents
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations
	show ip proxy-mobile node	Displays information about a specific proxy Mobile IP node or about all the nodes on the access point
	show ip proxy-mobile registration	Displays information about the pending and accepted proxy Mobile IP registrations
	show ip proxy-mobile subnet-map	Displays the proxy Mobile IP subnet map table
	show ip proxy-mobile traffic	Displays the proxy Mobile IP statistics

Command	Description
show ip proxy-mobile visitor	Displays visiting proxy Mobile IP nodes
clear ip proxy-mobile subnet-map	Clears the proxy Mobile IP subnet map and obtains a new table from the AAP

ip proxy-mobile (ssid configuration mode)

Use the **ip proxy-mobile** ssid configuration mode command to configure the radio interface (for the specified SSID) to support proxy Mobile IP. Use the **no** form of the command to reset the parameter to the default value.

[no] ip proxy-mobile

Syntax Description This command has no arguments or keywords.

Defaults No proxy Mobile IP support is the default setting.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to enable proxy Mobile IP support on the wireless LAN for the specified SSID:

```
AP(config-if-ssid)# ip proxy-mobile
```

This example shows how to disable proxy Mobile IP support:

```
AP(config-if-ssid)# no ip proxy-mobile
```

Related Commands	Command	Description
	clear ip proxy-mobile subnet-map	Clears the proxy Mobile IP subnet map and obtains a new table from the AAP
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile aaa requests	Displays information about mobile nodes that have pending proxy Mobile IP AAA requests
	show ip proxy-mobile agent	Displays information about the discovered proxy Mobile IP agents
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations
	show ip proxy-mobile node	Displays information about a specific proxy Mobile IP node or about all the nodes on the access point
	show ip proxy-mobile registration	Displays information about the pending and accepted proxy Mobile IP registrations
	show ip proxy-mobile subnet-map	Displays the proxy Mobile IP subnet map table
	show ip proxy-mobile traffic	Displays the proxy Mobile IP statistics

Command	Description
<code>show ip proxy-mobile visitor</code>	Displays visiting proxy Mobile IP nodes
<code>ssid</code>	Specifies the SSID and enters the ssid configuration mode

ip proxy-mobile aap

Use the **ip proxy-mobile aap** global configuration command to specify the IP addresses for the primary and secondary AAPs. Use the **no** form of this command to clear the primary AAP and secondary AAP addresses.

```
[no] ip proxy-mobile aap address
      [ address2 address3]
```

Syntax Description	address	Specifies the primary AAP IP address
	address2	(Optional) Specifies the secondary AAP IP address
	address3	(Optional) Specifies a second secondary AAP IP address

Defaults AAP address information is not defined by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify the IP addresses for proxy Mobile IP primary and secondary AAPs:

```
AP(config)# ip proxy-mobile aap 10.10.9.21 10.10.9.22 10.10.9.23
```

This example shows how to clear out the IP addresses for the proxy Mobile IP AAPs:

```
AP(config)# no ip proxy-mobile aap
```

Related Commands	Command	Description
	ip proxy-mobile enable	Enables and disables proxy Mobile IP and removes the configuration information when disabled
	show ip proxy-mobile	Displays proxy Mobile IP information

ip proxy-mobile enable

Use the **ip proxy-mobile enable** global configuration command to enable or disable proxy Mobile IP. Use the **no** form of this command to disable proxy Mobile IP and remove all associated CLIs.

[no] ip proxy-mobile enable

Syntax Description This command has no arguments or keywords.

Defaults Disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to enable proxy Mobile IP:

```
AP(config)# ip proxy-mobile enable
```

This example shows how to disable proxy Mobile IP and remove all associated CLIs:

```
AP(config)# no ip proxy-mobile enable
```

Related Commands	Command	Description
	ip proxy-mobile pause	Disables proxy Mobile IP without removing the configuration
	ip proxy-mobile aap	Specifies the IP addresses for the primary and secondary AAP servers for proxy Mobile IP
	ip proxy-mobile secure	Specifies the proxy Mobile IP security association information
	show ip proxy-mobile	Displays proxy Mobile IP information

ip proxy-mobile pause

Use the **ip proxy-mobile pause** global configuration command to enable or disable proxy Mobile IP without removing all associated CLIs. Use the **no** form of this command to re-enable proxy Mobile IP.

[no] ip proxy-mobile pause

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to disable proxy Mobile IP without removing the configuration:

```
AP(config)# ip proxy-mobile pause
```

This example shows how to re-enable proxy Mobile IP:

```
AP(config)# no ip proxy-mobile pause
```

Related Commands	Command	Description
	show ip proxy-mobile	Displays proxy Mobile IP information

ip proxy-mobile secure

Use the **ip proxy-mobile secure** global configuration command to specify the proxy Mobile IP security association information for a range of IP addresses. Use the **no** form of this command to reset the parameters to default values.

```
[no] ip proxy-mobile secure
      node address-start address-end
      spi spi
      key {hex / ascii} string
```

Syntax Description		
node <i>address-start</i> <i>address-end</i>	Specifies a range of IP addresses from <i>address-start</i> (beginning of range) to <i>address-end</i> (end of range)	
spi <i>spi</i>	Specifies the security parameter index	
key hex <i>string</i>	Specifies a hexadecimal key value	
key ascii <i>string</i>	Specifies an ASCII key value	

Defaults The default **key** setting is ASCII.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to configure proxy Mobile IP security association information for an IP address range of 10.9.1.20 to 10.9.1.60 with an ASCII key of 123456789abcd:

```
AP(config)# ip proxy-mobile secure 10.9.1.20 10.9.1.60 spi 100 key ascii 123456789abcd
```

This example shows how to reset the proxy Mobile IP security association information to defaults:

```
AP(config)# no ip proxy-mobile secure
```

Related Commands	Command	Description
	ip proxy-mobile enable	Enables and disables proxy Mobile IP and removes the configuration information when disabled
	show ip proxy-mobile	Displays proxy Mobile IP information

l2-filter bridge-group-acl

Use the **l2-filter bridge-group-acl** configuration interface command to apply a Layer 2 ACL filter to the bridge group incoming and outgoing packets between the access point and the host (upper layer). Use the **no** form of the command to disable the Layer 2 ACL filter

[no] l2-filter bridge-group-acl

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to apply a Layer 2 ACL filter to the bridge group packets:

```
AP(config-if)# l2-filter bridge-group-acl
```

This example shows how to activate a Layer 2 ACL filter:

```
AP(config-if)# no l2-filter bridge-group-acl
```

Related Commands	Command	Description
	bridge-group port-protected	Enables protected port for public secure mode configuration
	show bridge	Displays information on the bridge group or classes of entries in the bridge forwarding database
	show bridge group	Displays information about configured bridge groups

led flash

Use the **led flash** privileged EXEC command to start or stop the blinking of the LED indicators on the access point for a specified number of seconds. Without arguments, this command blinks the LEDs continuously.

led flash [*seconds* | **disable**]

Syntax	Description
<i>seconds</i>	Specifies the number of seconds (1 to 3600) that the LEDs blink
disable	Stops the blinking of the LEDs

Defaults The default is continuous blinking of the LEDs.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to blink the access point LEDs for 30 seconds:

```
AP# led flash 30
```

This example shows how to stop the blinking of the access point LEDs:

```
AP# led flash disable
```

Related Commands	Command	Description
	show led flash	Displays the blinking status of the LEDs

logging buffered

Use the **logging buffered** global configuration command to begin logging of messages to an internal buffer. Use the **no** form of this command to stop logging messages.

[no] logging buffered [*size*] [*severity*]

Syntax Description		
<i>size</i>		Specifies the size of the internal buffer (4096 to 2147483647 bytes)
<i>severity</i>		Specifies the message severity to log (1-7)
		Severity 1: alerts
		Severity 2: critical
		Severity 3: errors
		Severity 4: warnings
		Severity 5: notifications
		Severity 6: informational
		Severity 7: debugging

Defaults This command has no defaults.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to begin logging severity 3 messages to an internal 5000-byte buffer:

```
AP(config)# logging buffered 5000 3
```

This example shows how to stop the message logging:

```
AP(config)# no logging buffered
```

Related Commands	Command	Description
	show logging	Displays recent logging event headers or complete events
	clear logging	Clears logging status count and the trace buffer

match (class-map configuration)

Use the **match** class-map configuration command to define the match criteria to classify traffic. Use the **no** form of this command to remove the match criteria.

```
[no] match {access-group acl-index-or-name |
            ip [dscp dscp-list | precedence precedence-list] |
            vlan vlan-id}
```

Syntax Description		
access-group <i>acl-index-or-name</i>		Specifies the number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index ranges are 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index ranges are 100 to 199 and 2000 to 2699.
ip dscp <i>dscp-list</i>		Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63.
ip precedence <i>precedence-list</i>		Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7.
vlan <i>vlan-id</i>		Specifies the virtual LAN identification number. Valid IDs are from 1 to 4095; do not enter leading zeros.



Note

Though visible in the command-line help strings, the **any**, **class-map**, **destination-address**, **input-interface**, **mpls**, **not**, **protocol**, and **source-address** keywords are not supported.

Defaults This command has no defaults.

Command Modes Class-map configuration

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Use the **class-map** global configuration command to enter the class-map configuration mode. The **match** command in the class-map configuration mode is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

You can use the **match ip dscp** *dscp-list* command only in a policy map that is attached to an egress interface.

Only one **match** command per class map is supported.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Examples

This example shows how to create a class map called *class2*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
AP(config)# class-map class2
AP(config-cmap)# match ip dscp 10 11 12
AP(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
AP(config)# class-map class3
AP(config-cmap)# match ip precedence 5 6 7
AP(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic by vlan:

```
AP(config)# class-map class2
AP(config-cmap)# match ip precedence 5 6 7
AP(config-cmap)# no match ip precedence
AP(config-cmap)# match vlan 2
AP(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify
show class-map	Displays quality of service (QoS) class maps

max-associations (ssid configuration mode)

Use the **max-associations** ssid configuration mode command to configure the maximum number of associations supported by the radio interface (for the specified SSID). Use the **no** form of the command to reset the parameter to the default value.

[no] max-associations *value*

Syntax Description	<i>value</i>	Specifies the maximum number (1 to 255) of associations supported
---------------------------	--------------	---

Defaults This default maximum is 255.

Command Modes SSID configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to set the maximum number of associations to 5 on the wireless LAN for the specified SSID:

```
AP(config-if-ssid)# max-associations 5
```

This example shows how to reset the maximum number of associations to the default value:

```
AP(config-if-ssid)# no max-associations
```

Related Commands	Command	Description
	ssid	Specifies the SSID and enters the ssid configuration mode

packet retries

Use the **packet retries** configuration interface command to specify the maximum number of attempts to send a packet. Use the **no** form of the command to reset the parameter to defaults.

[no] packet retries 1-128

Syntax Description	<i>1-128</i>	Specifies the maximum number of retries (1 to 128)
---------------------------	--------------	--

Defaults The default number of retries is 32.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify 15 as the maximum number of retries.

```
AP(config-if)# packet retries 15
```

This example shows how reset the packet retries to defaults.

```
AP(config-if)# no packet retries
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

parent

Use the **parent** configuration interface command to add a parent to a list of valid parent access points. Use the **no** form of the command to remove a parent from the list.

[no] parent *1-4 mac-address*

Syntax Description		
	<i>1-4</i>	Specifies the parent root access point number (1 to 4)
	<i>mac-address</i>	Specifies the MAC address (in xxxx.xxxx.xxxx format) of a parent access point

Defaults Repeater access point operation is disabled by default.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines The **parent** command adds a parent to the list of valid parent access points. Use this command multiple times to define up to four valid parents. A repeater access point operates best when configured to associate with specific root access points that are connected to the wired LAN.

Examples This example shows how to set up repeater operation with the parent 1 access point:

```
AP(config-if)# parent 1 0040.9631.81cf
```

This example shows how to set up repeater operation with the parent 2 access point:

```
AP(config-if)# parent 2 0040.9631.81da
```

This example shows how to remove a parent from the parent list:

```
AP(config-if)# no parent
```

Related Commands	Command	Description
	parent timeout	Sets the parent association timeout

parent timeout

Use the **parent timeout** configuration interface command to define the amount of time to associate with a parent access point. Use the **no** form of the command to disable the timeout.

[no] parent timeout *sec*

Syntax Description	<i>sec</i>	Specifies the amount of time the access point attempts to associate with the specified parent access point (0 to 65535 seconds)
---------------------------	------------	---

Defaults Parent timeout is disabled by default.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines The **parent timeout** defines how long the access point attempts to associate with a parent in the parent list. After the timeout, another acceptable parent is used. You set up the parent list using the **parent** command. With the timeout disabled, the parent must come from the parent list.

Examples This example shows how to set up repeater operation with the parent 1 access point with a timeout of 60 seconds:

```
AP(config-if)# parent timeout 60
```

This example shows how to disable repeater operation:

```
AP(config-if)# no parent
```

Related Commands	Command	Description
	parent	Specify valid parent access points

payload-encapsulation

Use the **payload-encapsulation** configuration interface command to specify the Ethernet encapsulation type used to format Ethernet data packets that are not formatted using IEEE 802.3 headers. Data packets that are not IEEE 802.3 packets must be reformatted using IEEE 802.1H or RFC1042. Use the **no** form of the command to reset the parameter to defaults.

```
[no] payload-encapsulation
      {snap | dot1h}
```

Syntax Description	
snap	(Optional) Specifies the RFC1042 encapsulation
dot1h	(Optional) Specifies the IEEE 802.1H encapsulation

Defaults The default payload encapsulation is snap.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to specify the use of IEEE 802.1H encapsulation:

```
AP(config-if)# payload-encapsulation dot1h
```

This example shows how to reset the parameter to defaults:

```
AP(config-if)# no payload-encapsulation
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

power client maximum

Use the **power client maximum** configuration interface command to configure the maximum power level clients should use for IEEE 802.11b radio transmissions to the access point. The power setting is transmitted to the client device during association with the access point. Use the **no** form of the command to not specify a power level.

2.4-GHz Radio (dot11radio0)

```
[no] power client
    { 1 | 5 | 20 | 30 | 50 | 100 }
```

5-GHz Radio (dot11radio1)

```
[no] power client
    { 5 | 10 | 20 | 40 }
```

Syntax Description

For the 2.4-GHz radio: 1, 5, 20, 30, 50, 100	Specifies a specific power level in mW. Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the access point and client device.
For the 5-GHz radio: 5, 10, 20, 40	For a list of maximum power levels allowed in each regulatory domain for the 2.4-GHz radio, see Table 2-3 . For a list of maximum power levels allowed in each regulatory domain for the 5-GHz radio, see Table 2-4 .

Table 2-3 Maximum Power Levels for 2.4-GHz Radios

Regulatory Domain	Maximum Power Level (mW)
Americas (-A) (4W EIRP maximum)	100
EMEA (-E) (100 mW EIRP maximum)	50
Japan (-J) (10 mW/MHz EIRP maximum)	30
Israel (-I) (100 mW EIRP maximum)	50

Table 2-4 Maximum Power Levels for 5-GHz Radios

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Americas (-A) (160 mW EIRP maximum on channels 36-48, 800 mW EIRP maximum on channels 52-64)	40
Japan (-J) (10 mW/MHz EIRP maximum)	40

Table 2-4 Maximum Power Levels for 5-GHz Radios (continued)

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Singapore (-S) (100 mW EIRP maximum)	20
Taiwan (-T) (800 mW EIRP maximum)	40

Defaults

The default is no power level specification during association with the client.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Usage Guidelines

Use this command to specify the desired transmitter power level for clients. Lower power levels reduce the radio cell size and interference between cells. The client software chooses the actual transmit power level, choosing between the lower of the access point value and the locally configured value. The maximum transmit power is limited according to regulatory region.

Examples

This example shows how to specify a 20-mW power level for client devices associated to the access point radio:

```
AP(config-if)# power client 20
```

This example shows how to disable power level requests:

```
AP(config-if)# no power client
```

Related Commands

Command	Description
show running-config	Displays the current access point operating configuration

power local

Use the **power local** configuration interface command to configure the access point radio power level. Use the **no** form of the command to reset the parameter to defaults.

2.4-GHz Radio (dot11radio0)

[no] power local { 1 | 5 | 20 | 30 | 50 | 100 | maximum }

5-GHz Radio (dot11radio1)

[no] power local { 5 | 10 | 20 | 40 | maximum }

Syntax Description	For the 2.4-GHz radio: 1, 5, 20, 30, 50, 100, or maximum	Specifies access point power setting in mW. (Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the access point. Refer to Table 2-3 .)
	For the 5-GHz radio: 5, 10, 20, 40, or maximum	

Defaults The default local power level is **maximum**.

Command Modes Configuration interface

Command History	Release	Modification
		12.2(4)JA
	12.2(8)JA	Parameters were added to support the 5-GHz radio.

Usage Guidelines Use this command to specify the local transmit power level. Lower power levels reduce the radio cell size and interference between cells. The maximum transmit power is limited by region.

Examples This example shows how to specify a 20-mW transmit power level for one of the the access point radios:

```
AP(config-if)# power local 20
```

This example shows how to reset power to defaults on one of the access point radios:

```
AP(config-if)# no power local
```

Related Commands	Command	Description
		show running-config

preamble-short

Use the **preamble-short** configuration interface command to enable short radio preambles. The radio preamble is a selection of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. Use the **no** form of the command to change back to default values.

[no] preamble-short



Note

This command is not supported on the 5-GHz radio interface (dot11radio1).

Syntax Description This command has no arguments or keywords.

Defaults The default is short radio preamble.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines If short radio preambles are enabled, clients may request either short or long preambles and the access point formats packets accordingly. Otherwise, clients are told to use long preambles.

Examples This example shows how to set the radio packet to use a short preamble.

```
AP(config-if)# preamble-short
```

This example shows how to set the radio packet to use a long preamble.

```
AP(config-if)# no preamble-short
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

rts

Use the **rts** configuration interface command to set the Request-To-Send (RTS) threshold and the number of retries. Use the **no** form of the command to reset the parameter to defaults.

```
[no] rts
    {threshold 0-2347 | retries 1-128}
```

Syntax Description	threshold 0-2347	retries 1-128
	Specifies the packet size, in bytes, above which the access point negotiates an RTS/CTS before sending out the packet (0 to 2347 bytes).	Specifies the number of times the access point issues an RTS before stopping the attempt to send the packet over the radio.

Defaults
 The default **threshold** is 2330 bytes.
 The default number of **retries** is 32.

Command Modes
 Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples
 This example shows how to set the RTS threshold to 1400 bytes:

```
AP(config-if)# rts threshold 1400
```

This example shows how to set the RTS retries count to 3:

```
AP(config-if)# rts retries 3
```

This example shows how to reset the parameter to defaults:

```
AP(config-if)# no rts
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuration

show controllers dot11radio

Use the **show controllers dot11radio** privileged EXEC command to display the radio controller status.

show controllers dot11radio *interface-number*

Syntax Description	<i>interface-number</i>	Specifies the radio interface number. The 2.4-GHz radio is radio 0. The 5-GHz radio is radio 1.
--------------------	-------------------------	---

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the radio controller status for radio interface 0:

```
AP# show controllers dot11radio 0
```

Related Commands	Command	Description
	show interfaces dot11radio	Displays configuration and status information for the radio interface

show dot11 associations

Use the **show dot11 associations** privileged EXEC command to display the radio association table, radio association statistics, or to selectively display association information about all repeaters, all clients, a specific client, or basic service clients.

show dot11 associations
[client | repeater | statistics | *H.H.H* / bss-only | all-client]

Syntax Description	
client	(Option) Displays all client devices associated with the access point
repeater	(Option) Displays all repeater devices associated with the access point
statistics	(Option) Displays access point association statistics for the radio interface
<i>H.H.H (mac-address)</i>	(Option) Displays details about the client device with the specified MAC address (in xxxx.xxxx.xxxx format)
bss-only	(Option) Displays only the basic service set clients that are directly associated with the access point
all-client	(Option) Displays the status of all clients associated with the access point

Defaults When parameters are not specified, this command displays the complete radio association table.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the radio association table:

```
AP# show dot11 associations
```

This example shows how to display all client devices associated with the access point:

```
AP# show dot11 associations client
```

This example shows how to display access point radio statistics:

```
AP# show dot11 associations statistics
```

Related Commands	Command	Description
	clear dot11 client	Deauthenticates a client with a specified MAC address
	clear dot11 statistics	Resets the statistics for a specified radio interface or client device
	dot11 dot11radio linktest	Starts a link test between the access point and a client device

show dot11 network-map

Use the **show dot11 network-map** privileged EXEC command to display the radio network map. The radio network map contains information from Cisco access points in the same Layer 2 domain as this access point.

show dot11 network-map

Syntax Description This command has no arguments or keywords.

Defaults/Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines This command displays network map information only if you first enable the network map feature with the **dot11 network map** command.

Examples This example shows how to display the radio network map:

```
AP# show dot11 network-map
```

Related Commands	Command	Description
	dot11 network-map	Enables the network map feature

show dot11 statistics client-traffic

Use the **show dot 11 statistics client-traffic** privileged EXEC command to display the radio client traffic statistics.

show dot11 statistics client-traffic

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the radio client traffic statistics:

```
AP# show dot11 statistics client-traffic
```

Related Commands	Command	Description
	clear dot11 client	Deauthenticates a client with a specified MAC address
	clear dot11 statistics	Resets the statistics for a specified radio interface or client device

show iapp rogue-ap-list

Use the **show iapp rogue-ap-list** privileged EXEC command to display a list of rogue access points.

show iapp rogue-ap-list

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines The list contains an entry for each access point that a client station reported as a possible rogue access point. Each list entry contains the following information:

Rogue AP—MAC address of the reported rogue access point

Count—The number of times the access point was reported

Last Rpt Src—The MAC address of the last client to report the rogue access point

R—The last reason code

Prev Rpt Src—The MAC address of any previous client that reported the rogue access point

R—The previous reason code

Last(Min)—The number of minutes since the last report

1st(Min)—The number of minutes since the access point was first reported as a possible rogue

Name—The name of a Cisco rogue access point

The following reason codes are displayed:

1—The rogue was not running 802.1x

2—Authentication with the rogue timed out

3—Bad user password

4—Authentication challenge failed

Examples This example shows how to display the list of IAPP rogue access points:

```
AP# show iapp rogue-ap-list
```

■ show iapp rogue-ap-list

Related Commands

Command	Description
clear iapp rogue-ap-list	Clears the rogue access point list

show iapp standby-params

Use the **show iapp standby-params** privileged EXEC command to display IAPP standby parameters when a standby MAC address is configured. The information displayed includes the standby MAC address, the time-out value, and the poll-frequency value.

show iapp standby-params

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the IAPP standby parameters:

```
AP# show iapp standby-params
```

Related Commands	Command	Description
	logging buffered	Configures an access point with a specified MAC address as the standby
	iapp standby poll-frequency	Configures the standby access point polling interval
	iapp standby timeout	Configures the standby access point polling time-out value

show iapp statistics

Use the **show iapp statistics** privileged EXEC command to display the IAPP transmit and receive statistics.

show iapp statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines This command displays IAPP transmit and receive packet counts and IAPP error counts. The operating mode for the access point is also displayed.

Examples This example shows how to display the IAPP statistics:

```
AP# show iapp statistics
```

Related Commands	Command	Description
	clear iapp statistics	Clears the IAPP transmit and receive statistics

show interfaces dot11radio

Use the **show interfaces dot11radio** privileged EXEC command to display the radio interface configuration and statistics.

show interfaces dot11radio *interface-number*

Syntax Description	<i>interface-number</i>	Specifies the radio interface number. The 2.4-GHz radio is radio 0. The 5-GHz radio is radio 1.
--------------------	-------------------------	---

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the radio interface configuration and statistics:

```
AP# show interfaces dot11radio 0
```

Related Commands	Command	Description
	interface dot11radio	Configures a specified radio interface
	show running-config	Displays the access point run time configuration information

show interfaces dot11radio aaa

Use the **show interfaces dot11radio aaa** privileged EXEC command to display the radio interface information.

```
show interfaces dot11radio interface-number
aaa [timeout]
```

Syntax Description		
	<i>interface-number</i>	Specifies the radio interface number. The 2.4-GHz radio is radio 0. The 5-GHz radio is radio 1.
	timeout	Displays the AAA timeout value

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display AAA information for interface 0:

```
AP# show interfaces dot11radio 0 aaa
```

Related Commands	Command	Description
	debug dot11 aaa	Debug radio AAA operations
	show dot11 associations	Displays radio association information

show interfaces dot11radio statistics

Use the **show interfaces dot11radio statistics** privileged EXEC command to display the radio interface statistics.

show interfaces dot11radio *interface-number* **statistics**

Syntax Description	<i>interface-number</i>	Specifies the radio interface number. The 2.4-GHz radio is radio 0. The 5-GHz radio is radio 1.
--------------------	-------------------------	---

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the radio interface statistics for interface 0:

```
AP# show interfaces dot11radio 0 statistics
```

Related Commands	Command	Description
	clear dot11 statistics	Resets the statistics for a specified radio interface
	interface dot11radio	Configures a specified radio interface
	show running-config	Displays the access point run time configuration information
	show interfaces dot11radio	Displays configuration and statistics for a specified radio interface

show ip proxy-mobile

Use the **show ip proxy-mobile** privileged EXEC command to display information about proxy Mobile IP functionality.

show ip proxy-mobile

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display information about proxy Mobile IP functionality:

```
AP# show ip proxy-mobile
```

Related Commands	Command	Description
	clear ip proxy-mobile subnet-map	Clears the proxy Mobile IP subnet map and obtains a new table from the authoritative access point (AAP)
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile aaa requests	Displays information about mobile node that have pending proxy Mobile IP AAA requests
	show ip proxy-mobile agent	Displays information about the discovered proxy Mobile IP agents
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations
	show ip proxy-mobile node	Displays information about a specific proxy Mobile IP node or about all the nodes on the access point
	show ip proxy-mobile registration	Displays information about the pending and accepted proxy Mobile IP registrations
	show ip proxy-mobile subnet-map	Displays the proxy Mobile IP subnet map table
	show ip proxy-mobile traffic	Displays the IP statistics for proxy Mobile IP
	show ip proxy-mobile visitor	Displays visiting proxy Mobile IP nodes

show ip proxy-mobile aaa requests

Use the **show ip proxy-mobile aaa requests** privileged EXEC command to display information about mobile nodes that have pending proxy Mobile IP AAA requests.

show ip proxy-mobile aaa requests

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display information about mobile nodes that have pending proxy Mobile IP AAA requests:

```
AP# show ip proxy-mobile aaa requests
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show ip proxy-mobile agent

Use the **show ip proxy-mobile agent** privileged EXEC command to display information about the proxy Mobile IP agents discovered by the access point.

show ip proxy-mobile agent

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display all proxy Mobile IP agents discovered by the access point:

```
AP# show ip proxy-mobile agent
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show ip proxy-mobile detail

Use the **show ip proxy-mobile detail** privileged EXEC command to display proxy Mobile IP statistics, the subnet map, and all security associations.

show ip proxy-mobile detail

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the proxy Mobile IP statistics, the subnet map, and all security associations:

```
AP# show ip proxy-mobile detail
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP

show ip proxy-mobile node

Use the **show ip proxy-mobile node** privileged EXEC command to display information about a specific proxy Mobile IP node or all proxy Mobile IP nodes on the access point.

show ip proxy-mobile node [*address-start*]

Syntax Description	address-start	(Optional) Specifies the IP address for a specific proxy Mobile IP node
---------------------------	---------------	---

Defaults Displays all proxy Mobile IP nodes on the access point when an IP address is not specified.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display information about all proxy Mobile IP nodes on the access point:

```
AP# show ip proxy-mobile nodes
```

Related Commands	Command	Description
		ip proxy-mobile
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show ip proxy-mobile registration

Use the **show ip proxy-mobile registration** privileged EXEC command to display pending or accepted proxy Mobile IP registrations.

show ip proxy-mobile registration

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display pending or accepted proxy Mobile IP registrations:

```
AP# show ip proxy-mobile registrations
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show ip proxy-mobile subnet-map

Use the **show ip proxy-mobile subnet-map** privileged EXEC command to display the proxy Mobile IP subnet map table.

show ip proxy-mobile subnet-map

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display the proxy Mobile IP subnet map table:

```
AP# show ip proxy-mobile subnet-map
```

Related Commands	Command	Description
	clear ip proxy-mobile subnet-map	Clears the proxy Mobile IP subnet map and obtains a new table from the AAP
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show ip proxy-mobile traffic

Use the **show ip proxy-mobile traffic** privileged EXEC command to display all the statistics related to proxy Mobile IP.

show ip proxy-mobile traffic

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display all the proxy Mobile IP statistics:

```
AP# show ip proxy-mobile traffic
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP

show ip proxy-mobile visitor

Use the **show ip proxy-mobile visitor** privileged EXEC command to display the visiting proxy Mobile IP nodes.

show ip proxy-mobile visitor

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to display about visiting proxy Mobile IP nodes:

```
AP# show ip proxy-mobile visitor
```

Related Commands	Command	Description
	ip proxy-mobile	Enables proxy Mobile IP on the access point
	show ip proxy-mobile	Displays information about proxy Mobile IP
	show ip proxy-mobile detail	Displays proxy Mobile IP statistics, the subnet map table, and all the security associations

show led flash

Use the **show led flash** privileged EXEC command to display the LED flashing status.

show led flash

Syntax Description This command has no arguments or keywords.

Defaults This command has no defaults.

Command Modes Privileged EXEC

Release	Modification
12.2(4)JA	This command was introduced.

Examples This example shows how to display the LED flashing status:

```
AP# show led flash
```

Command	Description
led flash	Enables or disables LED flashing

speed

Use the **speed** configuration interface command to configure the data rates supported by the access point radios. An individual data rate can be set only to a basic or a non-basic setting, not both.

2.4-GHz Radio (dot11radio0)

```
speed
  { [1.0] [2.0] [5.5] [11.0]
    [basic-1.0] [basic-2.0] [basic-5.5] [basic-11.0] |
    range |
    throughput }
```

5-GHz Radio (dot11radio1)

```
speed
  { [6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0]
    [basic-6.0] [basic-9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0]
    [basic-54.0] |
    range |
    throughput |
    default }
```

Syntax Description

For the 2.4-GHz radio: [1.0] [2.0] [5.5] [11.0]	(Optional) Sets the access point to allow packets to use the non-basic settings. The access point transmits only unicast packets at these rates; multicast packets are sent at one of the data rates set to a basic setting.
For the 5-GHz radio: [6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0]	Note At least one of the access point's data rates must be set to a basic setting.
For the 2.4-GHz radio: [basic-1.0] [basic-2.0] [basic-5.5] [basic-11.0]	(Optional) Sets the access point to require the use of the specified data rates for all packets, both unicast and multicast. At least one of the access point's data rates must be set to a basic setting.
For the 5-GHz radio: [basic-6.0] [basic-9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0]	Note The client must support the basic rate you select or it cannot associate with the access point.
range	(Optional) Sets the data rate for best radio range. On the 2.4-GHz radio, this selection configures the 1.0 data rate to basic and the other data rates to supported. On the 5-GHz radio, this selection configures the 6.0 data rate to basic and the other data rates to supported.
throughput	(Optional) Sets the data rate for best throughput. On the 2.4-GHz radio, all four data rates are set to basic. On the 5-GHz radio, all data rates are set to basic.
default	(Optional) Sets data rates to the default settings.
	Note This command is supported on the 5-GHz radio only. It is not available for the 2.4-GHz radio.

Defaults

On the 2.4-GHz radio, all data rates are set to basic by default. On the 5-GHz radio, data rates 6.0, 12.0 and 24.0 are set to basic by default, and the other data rates are supported.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Examples

This example shows how to set the radio data rates for best throughput:

```
AP(config-if)# speed throughput
```

This example shows how to set the radio data rates support a low-speed client device while still supporting higher-speed client devices:

```
AP(config-if)# speed basic-1.0 2.0 5.5 11.0
```

Related Commands

Command	Description
show running-config	Displays the current access point operation configuration

ssid

Use the **ssid** configuration interface command to specify the radio service set identifier (SSID) and to enter into the ssid configuration mode. Use the **no** form of the command to remove an SSID.

[no] ssid *ssid-string*

Syntax Description	<i>ssid-string</i>	Specifies the SSID name for the radio, expressed as a case-sensitive alphanumeric string from 1 to 32 characters.
---------------------------	--------------------	---

Defaults The factory default SSID is tsunami.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced

Usage Guidelines Use this command to specify a unique SSID for your wireless network. Several access points on a network, or subnetwork, can share a SSID. The **no** form of the command removes the SSID, which inhibits clients that use that SSID from associating with the access point.

Examples This example shows how to set the radio SSID to Ivory-AP25:

```
AP(config-if)# ssid Ivory-AP25
```

This example shows how to remove the SSID named Ivory-AP25 and all its configuration settings:

```
AP(config-if)# no ssid Ivory-AP25
```

Related Commands	Command	Description
	authentication open (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support open authentication
	authentication shared (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support shared authentication
	authentication network-eap (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support network-EAP authentication
	guest-mode (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support guest mode
	ip proxy-mobile (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support proxy Mobile IP

Command	Description
max-associations (ssid configuration mode)	Configures the maximum number of associations supported by the radio interface (for the specified SSID)
show running-config	Displays the current access point operating configuration
vlan (ssid configuration mode)	Configures the radio interface (for the specified SSID) to support a specific Ethernet virtual LAN (VLAN)

station-role

Use the **station-role** configuration interface command to set the role of the radio interface. Use the **no** form of the command to reset the parameter to the default value.

```
[no] station-role
      {repeater | root [fallback {shutdown | repeater}]}
```

Syntax Description		
repeater		Specifies that the access point is configured for repeater operation. Repeater operation indicates the access point is not connected to a wired LAN and must associate to a root access point that is connected to the wired LAN.
root		Specifies that the access point is configured for root mode operation and connected to a wired LAN. This parameter also specifies that the access point should attempt to continue access point operation when the primary Ethernet interface is not functional.
fallback shutdown		(Optional) Specifies that the access point should shutdown when the primary Ethernet interface is not functional.
fallback repeater		(Optional) Specifies that the access point should operate in repeater mode when the primary Ethernet interface is not functional.

Defaults Operates as a root access point by default.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Examples This example shows how to configure the access point for root operation and shutdown when Ethernet is not functional:

```
AP(config-if)# station-role root fallback shutdown
```

This example shows how to configure the access point for repeater operation:

```
AP(config-if)# station-role repeater
```

This example shows how to reset the access point to root operation:

```
AP(config-if)# no station-role
```

Related Commands	Command	Description
	show running-config	Displays the current access point operating configuraion

traffic-class

Use the **traffic-class** configuration interface mode command to configure the radio interface quality-of-service (QoS) traffic class parameters for each of the eight traffic types. Use the **no** form of the command to reset a specific traffic class to the default values.

```
[no] traffic-class 0-7
      cw-min 0-10
      cw-max 0-10
      fixed-slot 0-20
```

Syntax Description	traffic-class 0-7	Specifies the traffic class number (0 to 7)
	cw-min 0-10	Specifies the minimum value (0 to 10) for the contention window
	cw-max 0-10	Specifies the maximum value (0 to 10) for the contention window
	fixed-slot 0-20	Specifies the fixed slot backoff interval value (0 to 20)

Defaults No traffic class support is provided by default.

Command Modes Configuration interface

Command History	Release	Modification
	12.2(4)JA	This command was introduced.

Usage Guidelines Use this command to control the backoff parameters for each class of traffic. Backoff parameters control how the radio accesses the airwaves. The **cw-min** and **cw-max** arguments specify the collision window as a power of 2. For example, if the value is set to 3, the contention window is 0 to 7 backoff slots (2 to the power 3 minus 1). The **fixed-slot** arguments specify the number of backoff slots that are counted before the random backoff counter starts to count down.

Examples This example shows how to configure traffic class 6 for contention windows and fixed slot backoff values. Each time the backoff for class 6 is started, the backoff logic waits a minimum of the 802.11 SIFS time plus 2 backoff slots. Then it begins counting down the 0 to 15 backoff slots in the contention window.

```
AP(config-if)# traffic-class 6 cw-min 4 cw-max 10 fixed-slot 2
```

This example shows how to disable traffic class support:

```
AP(config-if)# no traffic-class
```

vlan (ssid configuration mode)

Use the **vlan** ssid configuration mode command to configure the radio interface (for the specified SSID) to support a specific Ethernet virtual LAN (VLAN). Use the **no** form of the command to reset the parameter to the default value.

[no] **vlan** *vlan-id*

Syntax Description	<i>vlan-id</i>	Specifies the virtual Ethernet LAN identification number for the SSID
Defaults	This command has no defaults.	
Command Modes	SSID configuration interface	
Command History	Release	Modification
	12.2(4)JA	This command was introduced.
Examples	<p>This example shows how to configure the VLAN that uses the radio SSID (wireless LAN):</p> <pre>AP(config-if-ssid)# vlan 2</pre> <p>This example shows how to reset the VLAN parameter to default values:</p> <pre>AP(config-if-ssid)# no vlan</pre>	
Related Commands	Command	Description
	ssid	Specifies the SSID and enters the ssid configuration mode

world-mode

Use the **world-mode** configuration interface mode command to enable access point world mode operation. Use the **no** form of the command to disable world mode operation.

[no] world-mode



Note

This command is not supported on the 5-GHz radio interface (dot11radio1).

Syntax Description

This command has no arguments or keywords.

Defaults

World mode is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Usage Guidelines

With world mode enabled, the access point advertises the local settings, such as allowed frequencies and transmitter power levels. Clients with this capability then passively detect and adopt the advertised world settings, and then actively scan for the best access point.

Examples

This example shows how to enable world mode operation:

```
AP(config-if)# world-mode
```

This example shows how to disable world mode operation:

```
AP(config-if)# no world-mode
```

Related Commands

Command	Description
show running-config	Displays the current access point operating configuration

world-mode



List of Supported Cisco IOS Commands

This appendix lists the Cisco IOS commands that the access point supports. Cisco IOS commands that are not in this list have not been tested on access points and might not be supported.

Commands related to wireless LANs are described in [Chapter 2, “Cisco IOS Commands for Access Points,”](#) and appear in blue in this list. You can click those commands to browse to a description of the command. You can find descriptions and usage instructions for the rest of the commands in this list in the *Cisco IOS Release 12.2 Master Indexes*. Click this URL to browse to the master indexes:

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

A

aaa accounting
aaa accounting update
aaa authentication login
aaa group server
aaa new-model
access-class



Note The **access-class** command is supported only on access points that have a console port.

access-list
[accounting \(ssid configuration mode\)](#)
[antenna](#)
archive download-sw
archive upload
arp
[authentication network-eap \(ssid configuration mode\)](#)
[authentication open \(ssid configuration mode\)](#)
[authentication shared \(ssid configuration mode\)](#)

B

[beacon](#)
boot
bridge
bridge-group
bridge-group block-unknown-source
bridge-group input-address-list
bridge-group input-pattern-list
bridge-group input-type-list
bridge-group output-address-list
bridge-group output-pattern-list
bridge-group output-type-list
bridge-group subscriber-loop-control
bridge-group spanning-disabled
bridge-group source-learning
bridge-group unicast-flooding
[bridge-group port-protected](#)
[broadcast-key](#)

C

cd
cdp enable
cdp holdtime
cdp run
cdp timer
[channel](#)
[class-map](#)
clear access-list counters
clear cdp counters
clear cdp table
[clear dot11 client](#)
[clear dot11 hold-list](#)
[clear dot11 statistics](#)
[clear iapp rogue-ap-list](#)
[clear iapp statistics](#)
[clear ip proxy-mobile traffic](#)

[clear ip proxy-mobile subnet-map](#)
clear logging
clear vlan
clock timezone
clock summer-time
configure terminal
copy

D

databits



Note The **databits** command is supported only on access points that have a console port.

debug cdp adjacency
debug cdp events
debug cdp packets
[debug dot11](#)
[debug dot11 aaa](#)
[debug dot11 dot11radio](#)
[debug iapp](#)
debug interface fastethernet
debug ip http authentication
debug ip http ssi
debug ip http tokens
debug ip http transactions
debug ip http url
[debug ip proxy-mobile](#)
debug vlan packets
delete
description
dir
disable
disconnect
[dot11 dot11radio antenna-alignment](#)
[dot11 dot11radio linktest](#)
[dot11 dot11radio meter](#)
[dot11 extension aironet](#)

[dot11 holdoff-time](#)
[dot11 igmp snooping-helper](#)
[dot11 network-map](#)
[dot11 phone](#)
[dot1x client-timeout](#)
[dot1x reauth-period](#)
 duplex

E

enable
 encapsulation dot1q
 encryption
[encryption key](#)
[encryption mode wep](#)
 end
 erase
 exception flash
 exception core-file
 exception dump
 exception memory
 exec-timeout



Note The **exec-timeout** command is supported only on access points that have a console port.

exit

F

[fair-queue](#)
 format
[fragment-threshold](#)
 full-duplex

G

[guest-mode \(ssid configuration mode\)](#)

H

half-duplex
help
hold-queue
holdoff-time
hostname

I

[iapp standby mac-address](#)
[iapp standby poll-frequency](#)
[iapp standby timeout](#)
[infrastructure-client](#)
[infrastructure-ssid \(ssid configuration mode\)](#)
interface
[interface dot11radio](#)
interface fastethernet
interface virtual-dot11Radio
ip access-group
ip access-list
ip address
ip address dhcp
ip default-gateway
ip dhcp-server
ip domain-lookup
ip http authentication
ip http help-path
ip http path
ip http port
ip http server
ip name-server
[ip proxy-mobile](#)
[ip proxy-mobile \(ssid configuration mode\)](#)
[ip proxy-mobile aap](#)
ip proxy-mobile aap sync
[ip proxy-mobile enable](#)
[ip proxy-mobile pause](#)

ip proxy-mobile register

[ip proxy-mobile secure](#)

ip telnet

L

[l2-filter bridge-group-acl](#)

[led flash](#)

length



Note The **length** command is supported only on access points that have a console port.

line

logging

[logging buffered](#)

logging console

logging history

logging history size

logging facility

logging monitor

logging on

logging rate-limit

logging trap

login

logout

M

[match \(class-map configuration\)](#)

[max-associations \(ssid configuration mode\)](#)

monitor



Note The **monitor** command is supported only on access points that have a console port.

more

N

ntp

P

[packet retries](#)

[parent](#)

[parent timeout](#)

parity



Note The **parity** command is supported only on access points that have a console port.

[payload-encapsulation](#)

ping

policy-map

[power client maximum](#)

[power local](#)

[preamble-short](#)

privilege



Note The **privilege** command is supported only on access points that have a console port.

pwd

R

radius-server attribute

radius-server deadtime

radius-server retransmit

radius-server timeout

radius-server vsa send accounting

reload

[rts](#)

S

service-policy output
service sequence-number
service timestamps
session-timeout



Note The **session-timeout** command is supported only on access points that have a console port.

show access-lists
show bridge
show bridge group
show buffers
show cdp
show cdp entry
show cdp interface
show cdp neighbors
show cdp traffic
show clock
[show controllers dot11radio](#)
show controllers fastethernet
show debugging
show dhcp server
[show dot11 associations](#)
[show dot11 network-map](#)
[show dot11 statistics client-traffic](#)
show file information
show file systems
show flash
show history
show hosts
show html users
[show iapp rogue-ap-list](#)
[show iapp standby-params](#)
[show iapp statistics](#)
[show interfaces dot11radio](#)
[show interfaces dot11radio aaa](#)
[show interfaces dot11radio statistics](#)

show interfaces fastethernet
show ip access-list
show ip proxy-mobile
show ip proxy-mobile aaa requests
show ip proxy-mobile agent
show ip proxy-mobile detail
show ip proxy-mobile node
show ip proxy-mobile registration
show ip proxy-mobile subnet-map
show ip proxy-mobile traffic
show ip proxy-mobile visitor
show led flash
show line
show logging
show memory
show privilege
show processes
show queueing
show radius
show registry
show running-config
show sessions
show smf
show snmp
show snmp engineID
show snmp group
show snmp user
show stacks
show startup-config
show subsys
show tech-support
show terminal
show users
show version
show vlan
shutdown
snmp ifindex
snmp-server

snmp-server chassis-id
 snmp-server community
 snmp-server contact
 snmp-server enable traps
 snmp-server group
 snmp-server host
 snmp-server location
 snmp-server system-shutdown
 snmp-server user
 snmp-server view
 snmp trap link-status
[speed](#) (radio configuration interface)
 speed (serial line interface)




Note The **speed** (serial line interface) command is supported only on access points that have a console port.

[ssid](#)
[station-role](#)
 stopbit



Note The **stop bit** command is supported only on access points that have a console port.

T

terminal
 terminal-type

Note The **terminal-type** command is supported only on access points that have a console port.

 test fastethernet
 test led
 timeout (serial line interface)



Note The **timeout** (serial line interface) command is supported only on access points that have a console port.

[traffic-class](#)

U

undebg
username

V

verify
[vlan \(ssid configuration mode\)](#)

W

width



Note The **terminal-type** command is supported only on access points that have a console port.

[world-mode](#)



A

- accounting command [2-1](#)
- antenna receive command [2-3](#)
- audience [vii](#)
- authentication network-eap command [2-4](#)
- authentication open command [2-5](#)
- authentication shared command [2-7](#)

B

- beacon command [2-8](#)
- bridge-group command [2-9](#)
- broadcast-key command [2-10](#)

C

- caution, description [viii](#)
- channel command [2-11](#)
- channels, supported by regulatory domains [2-12](#)
- class map
 - command [2-14](#)
 - creating [2-14](#)
 - defining the match criteria [2-63](#)
- clear dot11 aaa client command [2-16](#)
- clear dot11 hold-list command [2-17](#)
- clear dot11 statistics command [2-18](#)
- clear iapp rogue-ap-list command [2-19](#)
- clear iapp statistics command [2-20](#)
- clear ip proxy-mobile command [2-21](#)
- clear ip proxy-mobile subnet-mask command [2-22](#)
- command modes defined [1-1](#)

conventions

- command [viii](#)
- publication [viii](#)
- text [viii](#)

D

- debug dot11 aaa command [2-24](#)
- debug dot11 command [2-23](#)
- debug dot11 dot11radio command [2-25](#)
- debug iapp command [2-27](#)
- debug ip proxy-mobile command [2-28](#)
- documentation related [ix](#)
- document conventions [viii](#)
- dot11 dot11radio antenna-alignment command [2-30](#)
- dot11 dot11radio link target command [2-31](#)
- dot11 dot11radio meter command [2-33](#)
- dot11 extension aironet command [2-34](#)
- dot11 igmp snooping-helper command [2-36](#)
- dot11 network-map command [2-37](#)
- dot11 phone command [2-38](#)
- dot1x client-timeout command [2-39](#)
- dot1x reauth-period command [2-40](#)

E

- encryption command [2-41, 2-43](#)

F

fragment-threshold command [2-44](#)
frequencies [2-11, 2-12](#)

G

global configuration mode [1-2, 1-3](#)
guest-mode command [2-45](#)

H

holdoff-time command [2-35](#)

I

iapp standby mac-address command [2-46](#)
iapp standby poll-frequency command [2-47](#)
iapp standby timeout command [2-48](#)
infrastructure-client command [2-49](#)
infrastructure-ssid command [2-50](#)
interface configuration mode [1-2, 1-3](#)
interface dot11radio command [2-51](#)
ip proxy-mobile command [2-52, 2-54](#)
ip proxy-mobile enable command [2-57](#)
ip proxy-mobile pause command [2-58](#)
ip proxy-mobile primary-aap command [2-56](#)
ip proxy-mobile secure command [2-59](#)

L

led flash command [2-61](#)
logging buffered command [2-62](#)

M

manual
audience [vii](#)

organization of [viii](#)
purpose of [vii](#)
match (class-map configuration) command [2-63](#)
match command [2-63](#)
max-associations command [2-65](#)
modes, commands [1-1](#)

N

note, description [viii](#)

P

packet retries command [2-66](#)
parent command [2-67, 2-68](#)
payload-encapsulation command [2-69](#)
power client maximum command [2-70](#)
power local command [2-72](#)
preamble-short command [2-73](#)
privileged EXEC mode [1-2](#)
publications, related [ix](#)

Q

QoS class map
creating [2-14](#)
defining the match criteria [2-63](#)

R

regulatory domains [2-11](#)
rts command [2-74](#)

S

show controllers dot11radio command [2-75](#)
show dot11 network-map command [2-77](#)
show dot11radio associations command [2-76](#)

show dot 11 statistics client-traffic command [2-78](#)
show iapp rogue-ap-list command [2-79](#)
show iapp standby-parms command [2-81](#)
show iapp statistics command [2-82](#)
show int dot11radio command [2-84](#)
show interfaces dot11radio command [2-83](#)
show interfaces dot11radio statistics command [2-85](#)
show ip proxy-mobile aaa requests command [2-87](#)
show ip proxy-mobile agent command [2-88](#)
show ip proxy-mobile command [2-86](#)
show ip proxy-mobile detail command [2-89](#)
show ip proxy-mobile node command [2-90](#)
show ip proxy-mobile registration command [2-91](#)
show ip proxy-mobile subnet-map command [2-92](#)
show ip proxy-mobile traffic command [2-93](#)
show ip proxy-mobile visitor command [2-94](#)
show led flash [2-95](#)
speed command [2-96](#)
ssid command [2-98](#)
station-role command [2-100](#)

T

traffic-class command [2-101](#)

U

user EXEC mode [1-2](#)

V

vlan command [2-102](#)

W

warnings [viii](#)

world-mode command [2-103](#)

