Cisco IOS Commands for Access Points and Bridges

This chapter lists and describes Cisco IOS commands in Cisco IOS Release 12.3(4)JA that you use to configure and manage your access point, bridge, and wireless LAN. The commands are listed alphabetically. Refer to Appendix A, "List of Supported Cisco IOS Commands," for a complete list of Cisco IOS commands supported by access points and bridges.

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

list-name	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:

```
AP(config-if-ssid)# accounting radius1
```

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**
{**gain** *gain* |
{**receive** | **transmit** {**diversity** | **left** | **right**}}}

Syntax Description

gain *gain*	Specifies the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. If necessary, you can use a decimal in the value, such as 1.5. **Note** This setting does not affect the behavior of the wireless device; it only informs the WLSE on your network of the device's antenna gain.
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
```

This example shows how to enter an antenna gain setting:

```
AP(config-if)# antenna gain 1.5
```

Related Commands

Command	Description
power local	Configures the radio power level
show running-config	Displays the current access point operating configuration

authentication (local server configuration mode)

Use the **authentication** local server configuration command to specify the authentication types that are allowed on the local authenticator. By default, a local authenticator access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices. You use the **no** form of the authentication command to limit the local authenticator to one or more authentication types.

[**no**] **authentication** [**eapfast**] [**leap**] [**mac**]

Note This command is not supported on bridges.

Syntax Description

eapfast	Specifies that the local authenticator performs EAP-FAST authentication for client devices.
leap	Specifies that the local authenticator performs LEAP authentication for client devices.
mac	Specifies that the local authenticator performs MAC-address authentication for client devices.

Defaults

By default, a local authenticator access point performs LEAP, EAP-FAST, and MAC-based authentication. To limit the local authenticator to one or two authentication types, use the **no** form of the command to disable unwanted authentication types.

Command Modes

Local server configuration mode

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to limit the local authenticator to perform only LEAP authentications for client devices:

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

Related Commands

Command	Description
group (local server configuration mode)	Creates a user group on the local authenticator and enters user group configuration mode
nas (local server configuration mode)	Adds an access point to the list of NAS access points on the local authenticator

Command	Description
radius-server local	Enables the access point as a local authenticator and enters local server configuration mode
show running-config	Displays the current access point operating configuration

authentication client

Use the **authentication client** configuration interface command to configure a LEAP username and password that the access point uses when authenticating to the network as a repeater.

authentication client username *username* **password** *password*

Syntax Description

username	Specifies the repeater's LEAP username
password	Specifies the repeater's LEAP password

Defaults

This command has no defaults.

Command Modes

SSID configuration interface

Command History

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

Examples

This example shows how to configure the LEAP username and password that the repeater uses to authenticate to the network:

```
AP(config-if-ssid)# authentication client username ap-north password buckeye
```

Related Commands

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

authentication key-management

Use the **authentication key-management** SSID configuration mode command to configure the radio interface (for the specified SSID) to support authenticated key management. Cisco Centralized Key Management (CCKM) and Wi-Fi Protected Access (WPA) are the key management types supported on the access point.

authentication key-management { [**wpa**] [**cckm**] } [**optional**]

Note This command is not supported on bridges.

Syntax Description

wpa	Specifies WPA authenticated key management for the SSID
cckm	Specifies CCKM authenticated key management for the SSID
optional	Specifies that client devices that do not support authenticated key management can use the SSID

Defaults

This command has no defaults.

Command Modes

SSID configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.2(13)JA	This command was modified to allow you to enable both WPA and CCKM for an SSID.

Usage Guidelines

Use this command to enable authenticated key management for client devices.

- To enable authenticated key management, you must enable a cipher suite using the **encryption mode ciphers** command.
- To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must use the **wpa-psk** command to configure a pre-shared key for the SSID.
- When you enable both WPA and CCKM for an SSID, you must enter **wpa** first and **cckm** second in the command. Any WPA client can attempt to authenticate, but only CCKM voice clients can attempt to authenticate. Only 802.11b and 802.11g radios support WPA and CCKM simultaneously.
- To enable both WPA and CCKM, you must set the encryption mode to a cipher suite that includes TKIP.

Examples

This example shows how to enable both WPA and CCKM for an SSID:

```
AP(config-if-ssid)# authentication key-management wpa cckm
```

Related Commands

Command	Description
encryption mode ciphers	Specifies a cipher suite
ssid	Specifies the SSID and enters SSID configuration mode
wpa-psk	Specifies a pre-shared key for an SSID

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*]

Note The **mac-address** option is not supported on bridges.

Syntax Description

list-name	Specifies the list name for EAP authentication
mac-address *list-name*	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.

Note Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.

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 EAP authentication or MAC address authentication. Use the **no** form of the command to disable open authentication for the SSID.

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

Note The **mac-address** and **alternate** options are not supported on bridges.

Syntax Description

eap *list-name*	Specifies the list name for EAP authentication
optional	Specifies that client devices using either open or EAP authentication can associate and become authenticated. This setting is used mainly by service providers that require special client accessibility.
mac-address *list-name*	Specifies the list name for MAC authentication
alternate	Specifies the use of either EAP authentication or MAC address 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 MAC address or EAP authentication. Otherwise, the client must pass both authentications. Use the **optional** keyword to allow client devices using either open or EAP authentication to associate and become authenticated. 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 network-eap (SSID configuration mode)	Specifies network EAP authentication
dot11 ssid	Creates an SSID and enters 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*]

Note The **mac-address** option is not supported on bridges.

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

Command	Description
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 *Kms*	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.
dtim-period *count*	Specifies the number of DTIM beacon periods to wait before delivering multicast packets. **Note** The **dtim-period** option is not supported on bridges.

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

boot buffersize

To modify the buffer size used to load configuration files, use the **boot buffersize** global configuration command. Use the **no** form of the command to return to the default setting.

[**no**] **boot buffersize** *bytes*

Syntax Description

bytes	Specifies the size of the buffer to be used. Enter a value from 4 KB to 512 KB.

Defaults

The default buffer size for loading configuration files is 32 KB.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Usage Guidelines

Increase the boot buffer size if your configuration file size exceeds 512 KB.

Examples

This example shows how to set the buffer size to 512 KB:

```
AP(config)# boot buffersize 524288
```

boot ios-break

Use the **boot ios-break** global configuration command to enable an access point or bridge to be reset using a **send break** Telnet command.

After you enter the boot ios-break command, you can connect to the access point console port and press **Ctrl-]** to bring up the Telnet prompt. At the Telnet prompt, enter **send break**. The access point reboots and reloads the image.

[**no**] **boot ios-break**

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to enable an access point or bridge to be reset using a **send break** Telnet command:

```
AP(config)# boot ios-break
```

boot upgrade

Use the **boot upgrade** global interface command to configure access points and bridges to automatically load a configuration and use DHCP options to upgrade system software.

When your access point renews its IP address with a DHCP request, it uses the details configured on the DHCP server to download a specified configuration file from a TFTP server. If a **boot system** command is part of the configuration file and the unit's current software version is different, the access point or bridge image is automatically upgraded to the version in the configuration. The access point or bridge reloads and executes the new image.

[**no**] **boot upgrade**

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to prevent an access point or bridge from automatically loading a configuration and upgrading system software:

```
AP(config)# no boot upgrade
```

bridge aging-time

Use the **bridge aging-time** global configuration command to configure the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated.

bridge *group* **aging-time** *seconds*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group
seconds	Specifies the aging time in seconds

Defaults

The default aging time is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the aging time for bridge group 1:

```
bridge(config)# bridge 1 aging-time 500
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge forward-time	Specifies a forward delay interval on the bridge
bridge hello-time	Specifies the interval between the hello BPDUs
bridge max-age	Specifies the interval that the bridge waits to hear BPDUs from the spanning tree root
bridge priority	Specifies the bridge STP priority

bridge forward-time

Use the **bridge forward-time** global configuration command to configure the forward delay interval on the bridge.

bridge *group* **aging-time** *seconds*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group
seconds	Specifies the forward time in seconds

Defaults

The default forward time is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the forward time for bridge group 2:

```
bridge(config)# bridge 2 forward-time 60
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge aging-time	Specifies the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated
bridge hello-time	Specifies the interval between the hello BPDUs
bridge max-age	Specifies the interval that the bridge waits to hear BPDUs from the spanning tree root
bridge priority	Specifies the bridge STP priority

bridge hello-time

Use the **bridge hello-time** global configuration command to configure the interval between hello bridge protocol data units (BPDUs).

bridge *group* **hello-time** *seconds*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group
seconds	Specifies the hello interval in seconds

Defaults

The default hello time is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the hello time for bridge group 1:

```
bridge(config)# bridge 1 hello-time 15
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge aging-time	Specifies the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated
bridge forward-time	Specifies a forward delay interval on the bridge
bridge max-age	Specifies the interval that the bridge waits to hear BPDUs from the spanning tree root
bridge priority	Specifies the bridge STP priority

bridge max-age

Use the **bridge max-age** global configuration command to configure the interval that the bridge waits to hear BPDUs from the spanning tree root. If the bridge does not hear BPDUs from the spanning tree root within this specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

bridge *group* **max-age** *seconds*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group
seconds	Specifies the max-age interval in seconds (enter a value between 10 and 200 seconds)

Defaults

The default max-age is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the max age for bridge group 1:

```
bridge(config)# bridge 1 max-age 20
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge aging-time	Specifies the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated
bridge forward-time	Specifies a forward delay interval on the bridge
bridge hello-time	Specifies the interval between the hello BPDUs
bridge priority	Specifies the bridge STP priority

bridge priority

Use the **bridge priority** global configuration command to configure the spanning tree priority for the bridge. STP uses the bridge priority to select the spanning tree root. The lower the priority, the more likely it is that the bridge will become the spanning tree root.

The radio and Ethernet interfaces and the native VLAN on the bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

bridge *group* **priority** *priority*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group to be configured
priority	Specifies the STP priority for the bridge

Defaults

The default bridge priority is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the priority for the bridge:

```
bridge(config-if)# bridge 1 priority 900
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge aging-time	Specifies the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated
bridge forward-time	Specifies a forward delay interval on the bridge
bridge hello-time	Specifies the interval between the hello BPDUs
bridge max-age	Specifies the interval that the bridge waits to hear BPDUs from the spanning tree root

bridge protocol ieee

Use the **bridge** *number* **protocol ieee** global configuration command to enable Spanning Tree Protocol (STP) on the bridge. STP is enabled for all interfaces assigned to the bridge group that you specify in the command.

The radio and Ethernet interfaces and the native VLAN on the bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

bridge *number* **protocol ieee** [**suspend**]

Note This command is supported only on bridges.

Syntax Description

number	Specifies the bridge group for which STP is enabled
suspend	Suspends STP on the bridge until you re-enable it.

Defaults

STP is 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 STP for bridge group 1:

```
bridge(config)# bridge 1 protocol ieee
```

Related Commands

Command	Description
bridge aging-time	Specifies the length of time that a dynamic entry can remain in the bridge table from the time the entry is created or last updated
bridge forward-time	Specifies a forward delay interval on the bridge
bridge hello-time	Specifies the interval between the hello BPDUs
bridge max-age	Specifies the interval that the bridge waits to hear BPDUs from the spanning tree root

bridge-group block-unknown-source

Use the **bridge-group block-unknown-source** configuration interface command to block traffic from unknown MAC addresses on a specific interface. Use the **no** form of the command to disable unknown source blocking on a specific interface.

For STP to function properly, **block-unknown-source** must be disabled for interfaces participating in STP.

bridge-group *group* **block-unknown-source**

Syntax Description

group	Specifies the bridge group to be configured

Defaults

When you enable STP on an interface, block unknown source is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to disable block unknown source for bridge group 2:

```
bridge(config-if)# no bridge-group 2 block-unknown-source
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group path-cost

Use the **bridge-group path-cost** configuration interface command to configure the path cost for the bridge Ethernet and radio interfaces. Spanning Tree Protocol (STP) uses the path cost to calculate the shortest distance from the bridge to the spanning tree root.

bridge-group *group* **path-cost** *cost*

Note This command is supported only on bridges.

Syntax Description

group	Specifies the bridge group to be configured
cost	Specifies the path cost for the bridge group

Defaults

The default path cost for the Ethernet interface is 19, and the default path cost for the radio interface is 33.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the path cost for bridge group 2:

```
bridge(config-if)# bridge-group 2 path-cost 25
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group port-protected

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

bridge-group *bridge-group*
port-protected

Syntax Description

bridge-group	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
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group priority

Use the **bridge-group priority** configuration interface command to configure the spanning tree priority for the bridge Ethernet and radio interfaces. Spanning Tree Protocol (STP) uses the interface priority to select the root interface on the bridge.

The radio and Ethernet interfaces and the native VLAN on the bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

bridge-group *group* **priority** *priority*

Syntax Description

group	Specifies the bridge group to be configured
priority	Specifies the STP priority for the bridge group

Defaults

The default priority for both the Ethernet and radio interfaces is 128.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the priority for an interface on bridge group 2:

```
bridge(config-if)# bridge-group 2 priority 150
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group spanning-disabled

Use the **bridge-group spanning-disabled** configuration interface command to disable Spanning Tree Protocol (STP) on a specific interface. Use the **no** form of the command to enable STP on a specific interface.

For STP to function properly, **spanning-disabled** must be disabled for interfaces participating in STP.

bridge-group *group* **spanning-disabled**

Syntax Description

group	Specifies the bridge group to be configured

Defaults

STP is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to disable STP for bridge group 2:

```
bridge(config-if)# bridge-group 2 spanning-disabled
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group subscriber-loop-control

Use the **bridge-group subscriber-loop-control** configuration interface command to enable loop control on virtual circuits associated with a bridge group. Use the **no** form of the command to disable loop control on virtual circuits associated with a bridge group.

For Spanning Tree Protocol (STP) to function properly, **subscriber-loop-control** must be disabled for interfaces participating in STP.

bridge-group *group* **subscriber-loop-control**

Syntax Description

group	Specifies the bridge group to be configured

Defaults

When you enable STP for an interface, subscriber loop control is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to disable subscriber loop control for bridge group 2:

```
bridge(config-if)# no bridge-group 2 subscriber-loop-control
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group unicast-flooding	Enables unicast flooding for a specific interface

bridge-group unicast-flooding

Use the **bridge-group unicast-flooding** configuration interface command to enable unicast flooding for a specific interface. Use the **no** form of the command to disable unicast flooding for a specific interface.

bridge-group *group* **unicast-flooding**

Syntax Description

group	Specifies the bridge group to be configured

Defaults

Unicast flooding is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure unicast flooding for bridge group 2:

```
bridge(config-if)# bridge-group 2 unicast-flooding
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge
bridge-group block-unknown-source	Blocks traffic from unknown MAC addresses on a specific interface
bridge-group path-cost	Specifies the path cost for the bridge Ethernet and radio interfaces
bridge-group port-protected	Enables protected port for public secure mode configuration
bridge-group priority	Specifies the spanning tree priority for the bridge Ethernet and radio interfaces
bridge-group spanning-disabled	Disables STP on a specific interface
bridge-group subscriber-loop-control	Enables loop control on virtual circuits associated with a bridge group

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*]
[**membership-termination**]
[**capability-change**]

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Note This command is not supported on bridges.

Syntax Description

vlan *vlan-id*	(Optional) Specifies the virtual LAN identification value
change *secs*	(Optional) Specifies the amount of time (in seconds) between the rotation of the broadcast encryption key
membership-termination	(Optional) If WPA authenticated key management is enabled, this option specifies that the access point generates and distributes a new group key when any authenticated client device disassociates from the access point. If clients roam frequently among access points, enabling this feature might generate significant overhead.
capability-change	(Optional) If WPA authenticated key management is enabled, this option specifies that the access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to 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 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
```

cca

Use the **cca** configuration interface command to configure the clear channel assessment (CCA) noise floor level for the bridge radio. The value you enter is used as an absolute value of dBm.

cca *number*

Note This command is supported only on bridges.

Syntax Description

number	Specifies the radio noise floor in dBm. Enter a number from –60 to 0. Zero configures the radio to use a received validate frame as the CCA indication.

Defaults

The default CCA level is –62 dBm.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the CCA level for the bridge radio:

```
bridge(config-if)# cca 50
```

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**}

Note This command is disabled on 5-GHz radios that support Dynamic Frequency Selection (DFS). All 5-GHz radios configured at the factory for use in the European Union and Signapore support DFS. Radios configured for use in other regulatory domains do not support DFS.

Syntax Description

number	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.
frequency	Specifies the center frequency for the radio channel. For a list of center frequencies for the 2.4-GHz access point radio, see Table 2-1. For a list of center frequencies for the 5-GHz access point radio, see Table 2-2. For a list of center frequencies for the 5-GHz bridge radio, see Table 2-3. **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 (both 802.11b and 802.11g)

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	–	–

Table 2-1 Channels and Center Frequencies for 2.4-GHz Radios (both 802.11b and 802.11g)

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Japan (-J)	Israel (-I)	China (-C)
13	2472	–	X	X	–	–
14	2484	–	–	X	–	–

Table 2-2 Channels and Center Frequencies for 5-GHz Access Point 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	X	–	–	–
153	5765	X	–	–	–
157	5785	X	–	–	–
161	5805	X	–	–	–

Note All channel sets for the 5-GHz access point 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.

Table 2-3 Channels and Center Frequencies for 5-GHz Bridge Radios

Channel Identifier	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
149	5745	–	–	–	–
153	5765	–	–	–	–

Table 2-3 Channels and Center Frequencies for 5-GHz Bridge Radios

Channel Identifier	Frequency in MHz	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
157	5785	–	–	–	–
161	5805	–	–	–	–

Note All bridge channel sets are restricted to outdoor usage.

Defaults

The default channel setting 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 access point radio.
12.2(11)JA	Parameters were added to support the 5-GHz bridge 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 frequency to the default setting:

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

Related Commands

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

channel-match (LBS configuration mode)

Use the **channel-match** location based services (LBS) configuration mode command to specify that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet. If the channel used by the tag and the channel used by the access point do not match, the access point drops the packet.

[**no**] **channel-match**

Syntax Description

This command has no arguments or keywords.

Defaults

The channel match option is enabled by default.

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to enable the channel match option for an LBS profile:

```
ap(dot11-lbs)# channel-match
```

Related Commands

Command	Description
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
method (LBS configuration mode)	Specifies the location method used in an LBS profile
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

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

name	Specifies the name of the class map

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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 aaa authentication mac-authen filter-cache

Use the **clear dot11 aaa authentication mac-authen filter-cache** privileged EXEC command to clear entries from the MAC authentication cache.

clear dot11 aaa authentication mac-authen filter-cache [*address*]

Syntax Description

address	Specifies a specific MAC address to clear from the cache.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Examples

This example shows how to clear a specific MAC address from the MAC authentication cache:

```
ap# clear dot11 aaa authentication mac-authen filter-cache 7643.798a.87b2
```

Related Commands

Command	Description
dot11 activity-timeout	Enable MAC authentication caching on the access point.
show dot11 aaa authentication mac-authen filter-cache	Display MAC addresses in the MAC authentication cache.

clear dot11 cckm-statistics

Use the **clear dot11 cckm-statistics** privileged EXEC command to reset CCKM statistics.

clear dot11 cckm-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(15)JA	This command was introduced.

Examples

This example shows how to clear CCKM statistics:

```
AP# clear dot11 cckm-statistics
```

Related Commands

Command	Description
show dot11 associations	Displays association information for 802.11 devices

clear dot11 client

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

clear dot11 client {*mac-address*}

Syntax Description

mac-address	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

interface	Specifies a radio interface number
mac-address	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

Note This command is not supported on bridges.

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 wlccp wds

Use the **clear wlccp wds** privileged EXEC command to clear WDS statistics and to remove devices from the WDS database.

clear wlccp wds {[**ap** [*mac-address*]] | [**mn** [*mac-address*]] | **statistics** | **aaa authentication mac-authen filter-cache** [*mac-address*]}

Syntax Description

ap [*mac-address*]	Removes access points from the WDS database. If you specify a MAC address (in the hhhh.hhhh.hhhh format), the command removes the specified device from the WDS database. If you do not specify a MAC address, the command removes all access points from the WDS database.
mn [*mac-address*]	Removes client devices (mobile nodes) from the WDS database. If you specify a MAC address (in the hhhh.hhhh.hhhh format), the command removes that device from the WDS database. If you do not specify a MAC address, the command removes all clients from the WDS database.
statistics	Resets all WDS statistics.
aaa authentication mac-authen filter-cache [*mac-address*]	Removes MAC addresses from the access point's MAC authentication filter cache. If you specify a MAC address (in the hhhh.hhhh.hhhh format), the command removes that device from the filter cache. If you do not specify a MAC address, the command removes all addresses from the cache.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Examples

This example shows how to remove an access point from the WDS database:

```
AP# clear wlccp wds ap 1572.342d.97f4
```

Related Commands

Command	Description
show wlccp	Displays information on devices participating in Cisco Centralized Key Management (CCKM)
wlccp wds aaa authentication mac-authen filter-cache	Enables MAC authentication caching on the access point

concatenation

Use the **concatenation** configuration interface command to enable packet concatenation on the bridge radio. Using concatenation, the bridge combines multiple packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency.

concatenation [*bytes*]

Note This command is supported only on bridges.

Syntax Description

bytes	(Optional) Specifies a maximum size for concatenated packets in bytes. Enter a value from 1600 to 4000.

Defaults

Concatenation is enabled by default, and the default maximum concatenated packet size is 3500.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure concatenation on the bridge radio:

```
bridge(config-if)# concatenation 4000
```

countermeasure tkip hold-time

Use the **countermeasure tkip hold-time** configuration interface command to configure a TKIP MIC failure holdtime. If the access point detects two MIC failures within 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.

countermeasure tkip hold-time *seconds*

Syntax Description

seconds	Specifies the length of the TKIP holdtime in seconds (if the holdtime is 0, TKIP MIC failure hold is disabled)

Defaults

TKIP holdtime is enabled by default, and the default holdtime is 60 seconds.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the TKIP holdtime on the access point radio:

```
ap(config-if)# countermeasure tkip hold-time 120
```

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 activate 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** | **authenticator** | **dispatcher** | **manager** }

Syntax Description

accounting	Activates debugging of 802.11 AAA accounting packets
authenticator { **all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata** }	Activates debugging of MAC and EAP authentication packets. Use these options to activate authenticator debugging: • **all**—activates debugging for all authenticator packets • **dispatcher**—activates debugging for authentication request handler packets • **mac-authen**—activates debugging for MAC authentication packets • **process**—activates debugging for authenticator process packets • **rxdata**—activates debugging for EAPOL packets from client devices • **state-machine**—activates debugging for authenticator state-machine packets • **txdata**—activates debugging for EAPOL packets sent to client devices
dispatcher	Activates debugging of 802.11 AAA dispatcher (interface between Association & Manager) packets
manager { **all** | **dispatcher** | **keys** | **rxdata** | **state-machine** | **supplicant** | **txdata** }	Activates debugging information for the AAA manager. Use these options to activate AAA manager debugging: • **all**—activates all AAA manager debugging • **dispatcher**—activates debug information for AAA manager-authenticator dispatch traffic • **keys**—activates debug information for AAA manager key processing • **rxdata**—activates debugging for AAA manager packets received from client devices • **state-machine**—activates debugging for AAA manager state-machine packets • **supplicant**—activates debugging for LEAP supplicant packets • **txdata**—activates debugging for AAA manager packets sent to client devices

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(15)JA	This command was modified to include the **accounting**, **authenticator**, **dispatcher**, and **manager** debugging options.

Examples

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

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

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* {**accept-radio-firmware** | **monitor** {**ack** | **address** | **beacon** | **crc** | **lines** | **plcp** | **print** | **probe** | **store**} | **print** { **hex** | **if** | **iv** | **lines** | **mic** | **plcp** | **printf** | **raw** | **shortadr** } | **radio_debug** *flag-value* | **stop-on-failure** | **trace** {**off** | **print** | **store**}}

Syntax Description

interface-number	Specifies a radio interface number (the 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1).
accept-radio-firmware	Configures the access point to disable checking the radio firmware version
monitor	Enables RF monitor mode. Use these options to turn on monitor modes: • **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
print	Enables packet printing. Use these options to turn on packet printing: • **hex**—Prints entire packets without formatting • **if**—Prints the in and out interfaces for packets • **iv**—Prints the packet WEP IV • **lines**—Prints the line count for the trace • **mic**—Prints the Cisco MIC • **plcp**—Displays the PLCP • **printf**—Prints using printf instead of buginf • **raw**—Prints without formatting data • **shortadr**—Prints MAC addresses in short form
stop-on-failure	Configures the access point to not restart when the radio driver fails
trace	Enables trace mode. Use these options to turn on trace modes: • **off**—Turns off traces • **print**—Enables trace printing • **store**—Enables trace storage

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 enable packet printing with MAC addresses in short form:

```
AP# debug dot11 dot11radio 0 print shortadr
```

This example shows how to begin monitoring of all packets with CRC errors:

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

This example shows how to stop monitoring of packets with CRC errors:

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

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 dot11 ids

Use the **debug dot11 ids eap** privileged EXEC command to enable debugging for wireless IDS monitoring. Use the **no** form of the command to disable IDS debugging.

[**no**] **debug dot11 ids** {**eap** | **cipher-errors**}

Note This command is not supported on 1400 series bridges.

Syntax Description

eap	Activates debugging of IDS authentication events
cipher-errors	Activates debugging of cipher errors detected by IDS

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to activate wireless IDS debugging for authentication events:

```
AP# debug dot11 ids eap
```

Related Commands

Command	Description
dot11 ids eap attempts	Configures limits on authentication attempts and EAPOL flooding on scanner access points in monitor mode
show debugging	Displays all debug settings and the debug packet headers
show dot11 ids eap	Displays wireless IDS 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 radius local-server

Use the **debug radius local-server** privileged EXEC mode command to control the display of debug messages for the local authenticator.

debug radius local-server {**client** | **eapfast** | **error** | **packets** }

Syntax Description

Command	Description
client	Activates display of error messages related to failed client authentications to the local authenticator
eapfast {**encryption** | **events** | **pac** | **pkts**}	Activates display of messages related to EAP-FAST on the local authenticator. • **encryption**—displays enecryption and decryption of packets sent and received • **events**—displays EAP-FAST events on the local authenticator • **pac**—displays PAC generations and verifications • **pkts**—displays packets received and transmitted from EAP-FAST clients
error	Activates display of error messages related to the local authenticator
packets	Activates display of the content of RADIUS packets sent from and received by the local authenticator

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was first introduced.

Examples

This example shows how to begin debugging for local authenticator errors:

```
AP# debug radius local-server error
```

Related Commands

Command	Description
radius-server local	Enables the access point as a local authenticator
show debugging	Displays all debug settings and the debug packet headers

debug wlccp ap

Use the **debug wlccp ap** privileged EXEC command to enable debugging for devices that interact with the access point that provides wireless domain services (WDS).

debug wlccp ap {**mn** | **rm** [**statistics** | **context** | **packet**] | **state** | **wds-discovery**}

Note This command is not supported on bridges.

Syntax Description

Command	Description
mn	(Optional) Activates display of debug messages related to client devices
rm [**statistics** | **context** | **packet**]	(Optional) Activates display of debug messages related to radio management • **statistics**—shows statistics related to radio management • **context**—shows the radio management contexts • **packet**—shows output related to packet flow
state	(Optional) Activates display of debug messages related to access point authentication to the WDS access point
wds-discovery	(Optional) Activates display of debug messages related to the WDS discovery process

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was first introduced.

Examples

This example shows how to begin debugging for LEAP-enabled client devices participating in Cisco Centralized Key Management (CCKM):

```
AP# debug wlccp ap mn
```

Related Commands

Command	Description
show debugging	Displays all debug settings and the debug packet headers
show wlccp	Displays WLCCP information

debug wlccp packet

Use the **debug wlccp packet** privileged EXEC command to activate display of packets to and from the access point that provides wireless domain services (WDS).

debug wlccp packet

Note This command is not supported on bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was first introduced.

Examples

This example shows how to activate display of packets to and from the WDS access point:

```
AP# debug wlccp packet
```

Related Commands

Command	Description
show debugging	Displays all debug settings and the debug packet headers
show wlccp	Displays WLCCP information

debug wlccp rmlib

Use the **debug wlccp rmlib** privileged EXEC command to activate display of radio management library functions on the access point that provides wireless domain services (WDS).

debug wlccp rmlib

Note This command is not supported on bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)JA	This command was first introduced.

Examples

This example shows how to activate display of radio management library functions on the access point that provides WDS:

```
AP# debug wlccp rmlib
```

Related Commands

Command	Description
show debugging	Displays all debug settings and the debug packet headers
show wlccp	Displays WLCCP information

debug wlccp wds

Use the **debug wlccp wds** privileged EXEC command to activate display of wireless domain services (WDS) debug messages.

debug wlccp wds
aggregator [**packet**]
authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}
nm [**packet** | **loopback**]
state
statistics

Note This command is not supported on bridges.

Syntax Description

Command	Description
aggregator [**packet**]	(Optional) Activates display of debug messages related to radio management. Use the **packet** option to display packets from and to the radio management aggregator.
authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}	(Optional) Use this command and its options to turn on display of WDS debug messages related to authentication. • **all**—Enables all authenticator debugging • **dispatcher**—Enables debugging related to handling authentication requests • **mac-authen**—Enables debugging related to MAC address authentication • **process**—Enables debugging related to authenticator processes • **rxdata**—Enables display of EAPOL packets from clients • **state-machine**—Enables authenticator state-machine debugging • **txdata**—Enables display of EAPOL packets to clients
nm [**packet** | **loopback**]	(Optional) Activates display of debug messages from the wireless network manager (WNM). The **packet** option displays Cisco IOS packets from and to the network manager, and the **loopback** option re-routes packets sent to the WNM to the WDS access point console instead.
state	(Optional) Activates display of state transitions for access points interacting with the WDS access point.
statistics	(Optional) Activates display of WDS statistics.

Defaults

Debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was first introduced.
12.2(13)JA	This command was modified to include the **aggregator** and **nm** options.

Examples

This example shows how to begin debugging for LEAP-enabled client devices participating in Cisco Centralized Key Management (CCKM):

```
AP# debug wlccp ap mn
```

Related Commands

Command	Description
show debugging	Displays all debug settings and the debug packet headers
show wlccp	Displays WLCCP information

dfs band

Use the **dfs band** configuration interface command to prevent the access point from automatically selecting specific groups of 5-GHz channels during dynamic frequency selection (DFS). Use the **no** form of the command to unblock groups of channels.

[**no**] **dfs band** [**1**] [**2**] [**3**] [**4**] **block**

Note This command is supported only on 5-GHz radios configured at the factory for use in the European Union and Signapore.

Syntax Description

[**1**] [**2**] [**3**] [**4**]	Specifies a group of channels to be blocked from auto-selection during DFS. • **1**—Specifies frequencies 5.150 to 5.250 GHz. This group of frequencies is also known as the UNII-1 band. • **2**—Specifies frequencies 5.250 to 5.350 GHz. This group of frequencies is also known as the UNII-2 band. • **3**—Specifies frequencies 5.470 to 5.725 GHz. • **4**—Specifies frequencies 5.725 to 5.825 GHz. This group of frequencies is also known as the UNII-3 band.

Defaults

By default, no channels are blocked from DFS auto-selection.

Command Modes

Configuration interface

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to prevent the access point from selecting frequencies 5.150 to 5.350 GHz during DFS:

```
ap(config-if)# dfs band 1 2 block
```

This example shows how to unblock frequencies 5.150 to 5.350 for DFS:

```
ap(config-if)# no dfs band 1 2 block
```

This example shows how to unblock all frequencies for DFS:

```
ap(config-if)# no dfs band block
```

Usage Guidelines

Some regulatory domains limit the 5-GHz channels that can be used in specific locations; for example, indoors or outdoors. Use the **dfs band** command to comply with the regulations in your regulatory domain.

Related Commands

Command	Description
channel	Specifies the radio frequency on which a radio interface operates

distance

Use the **distance** configuration interface command to specify the distance from a root bridge to the non-root bridge or bridges with which it communicates. The distance setting adjusts the bridge's timeout values to account for the time required for radio signals to travel from bridge to bridge. You do not need to adjust this setting on non-root bridges.

distance *kilometers*

Note This command is supported only on bridges.

Note If more than one non-root bridge communicates with the root bridge, enter the distance from the root bridge to the non-root bridge that is farthest away.

Syntax Description

kilometers	Specifies the bridge distance setting (enter a value from 0 to 99 km)

Defaults

In installation mode, the default distance setting is 99 km. In all other modes, such as root and non-root, the default distance setting is 0 km.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the distance setting for the root bridge radio:

```
bridge(config-if)# distance 40
```

dot11 association mac-list

To specify a MAC address access list used for dot11 association use the **dot11 association mac-list** command.

dot11 association mac-list *number*

Syntax Description

number	Specifies a number (700 to 799) for a 48-bit MAC address access list.

Defaults

No MAC address access list is assigned.

Examples

This example shows the creation of a MAC address access list used to filter one client with a MAC address of 0000.1234.5678.

```
AP(config)# access-list 700 deny 0000.1234.5678 0000.0000.0000
AP(config)# dot11 association mac-list 700
```

Related Commands

Command	Description
show access-list	Displays the configured access-lists.

dot11 aaa authentication attributes service-type login-only

Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only. By default, the access point sends reauthentication requests to the server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point.

dot11 aaa authentication attributes service-type login-only

Syntax Description

This command has no arguments or keywords.

Defaults

The default service-type attribute in reauthentication requests is set to authenticate-only. This command sets the service-type attribute in reauthentication requests to login-only.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Related Commands

Command	Description
dot11 aaa csid	Selects the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes

dot11 aaa authentication mac-authen filter-cache

Use the **dot11 aaa authentication mac-authen filter-cache** global configuration command to enable MAC authentication caching on the access point. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

dot11 aaa authentication mac-authen filter-cache [**timeout** *seconds*]

Syntax Description

timeout *seconds*	Specifies a timeout value for MAC authentications in the cache.

Defaults

MAC authentication caching is disabled by default. When you enable it, the default timeout value is 1800 (30 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Examples

This example shows how to configure MAC authentication caching with a one-hour timeout:

```
ap(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
```

Related Commands

Command	Description
clear dot11 aaa authentication mac-authen filter-cache	Clear MAC addresses from the MAC authentication cache.
show dot11 aaa authentication mac-authen filter-cache	Display MAC addresses in the MAC authentication cache.

dot11 aaa csid

Use the **dot11 aaa csid** global configuration command to select the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets.

dot11 aaa csid { **default** | **ietf** | **unformatted** }

Syntax Description

default	Specifies the default format for MAC addresses in CSID attributes. The default format looks like this example: `0007.85b3.5f4a`
ietf	Specifies the Internet Engineering Task Force (IETF) format for MAC addresses in CSID attributes. The IETF format looks like this example: `00-07-85-b3-5f-4a`
unformatted	Specifies no formatting for MAC addresses in CSID attributes. An unformatted MAC address looks like this example: `000785b35f4a`

Defaults

The default CSID format looks like this example:

`0007.85b3.5f4a`

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Usage Guidelines

You can also use the **wlccp wds aaa csid** command to select the CSID format.

Related Commands

Command	Description
debug dot11 aaa	Begin debugging of dot11 authentication, authorization, and accounting (AAA) operations

dot11 activity-timeout

Use the **dot11 activity-timeout** global configuration command to configure the number of seconds that the access point tracks an inactive device (the number depends on its device class). The access point applies the unknown device class to all non-Cisco Aironet devices.

dot11 activity-timeout { [**client-station** | **repeater** | **bridge** | **workgroup-bridge** | **unknown**] [**default <1 - 100000>**] [**maximum <1 - 100000>**] }

Syntax Description

client-station, repeater, bridge, workgroup-bridge	Specify Cisco Aironet device classes
unknown	Specifies unknown (non-Cisco Aironet) device class
default <1 - 100000>	Specifies the activity timeout value that the access point uses when a device associates and proposes a zero-refresh rate or does not propose a refresh rate
maximum <1 - 100000>	Specifies the maximum activity timeout allowed for a device regardless of the refresh rate proposed by a device when it associates

Defaults

Table 2-4 lists the default activity timeouts for each device class. All values are in seconds.

Table 2-4 Default Activity Timeouts

Device Class	Default Timeout
unknown	60
client-station	1800
repeater	28800
bridge	28800
workgroup-bridge	28800

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to configure default and maximum activity timeouts for all device classes:

```
AP(config)# dot11 activity-timeout default 5000 maximum 24000
```

Usage Guidelines

To set an activity timeout for all device types, set a default or maximum timeout without specifying a device class (for example, enter **dot11 activity-timeout default 5000**). The access point applies the timeout to all device types that are not already configured with a timeout.

Related Commands

Command	Description
dot11 adjacent-ap age-timeout	Specifies the number of hours an inactive entry remains in the list of adjacent access points
show dot11 associations	Display the radio association table, radio association statistics, or association information about wireless devices
show dot11 network-map	Displays the radio network map

dot11 adjacent-ap age-timeout

Use the **dot11 adjacent-ap age-timeout** global configuration command to specify the number of hours an inactive entry remains in the list of adjacent access points.

dot11 adjacent-ap age-timeout *hours*

Note This command is not supported on bridges.

Syntax Description

hours	Specifies the number of hours an inactive entry remains in the list of adjacent access points

Defaults

The default age-timeout is 24 hours.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the timeout setting for inactive entries in the adjacent access point list:

```
AP# dot11 adjacent-ap age-timeout 12
```

Related Commands

Command	Description
show dot11 adjacent-ap	Displays the list of adjacent access points

dot11 antenna-alignment

Use the **dot11 antenna-alignment** privileged EXEC command to activate the antenna-alignment tool for a radio interface. Use this tool to test and align the wireless device's antenna with another remote antenna.

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

Syntax Description

interface-number	Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)
timeout	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 wireless devices, and records the MAC address and signal strength of responses it receives. After the timeout, the radio reassociates with its parent.

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

Examples

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

```
br# 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 arp-cache

Use the **dot11 arp-cache** global configuration command to enable client ARP caching on the access point. ARP caching on the access point reduces the traffic on your wireless LAN and increases client battery life by stopping ARP requests for client devices at the access point. Instead of forwarding ARP requests to client devices, the access point responds to requests on behalf of associated client devices and drops ARP requests that are not directed to clients associated to the access point. When ARP caching is optional, the access point responds on behalf of clients with IP addresses known to the access point but forwards through its radio port any ARP requests addressed to unknown clients. When the access point knows all the IP addresses for associated clients, it drops any ARP requests not directed to its clients. In its beacon, the access point includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

[**no**] **dot11 arp-cache** [**optional**]

Syntax Description

optional	Configures the access point to respond to ARP requests addressed to clients for which the access point knows the IP address but forward through its radio port ARP requests addressed to client devices that the access point does not recognize. When the access point learns all the IP addresses for associated clients, it drops any ARP requests not directed to its clients.

Defaults

ARP caching is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to enable ARP caching:

```
AP(config)# dot11 arp-cache
```

dot11 carrier busy

Use the **dot11 carrier busy** privileged exec command to display levels of radio activity on each channel.

dot11 *interface-number* **carrier busy**

Syntax Description

interface-number	Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Usage Guidelines

During the carrier busy test, the access point or bridge drops all associations with wireless networking devices for about 4 seconds while it conducts the carrier test and then displays the test results.

You can re-display the carrier busy results using the **show dot11 carrier busy** command.

Examples

This example shows how to run the carrier busy test for radio interface 0:

```
AP# dot11 d0 carrier busy
```

This example shows the carrier busy test results:

```
Frequency  Carrier Busy %
---------  --------------
5180             0
5200             2
5220            27
5240             5
5260             1
5280             0
5300             3
5320             2
```

Related Commands

Command	Description
show dot11 carrier busy	Displays the carrier busy test results

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**

Note You cannot disable Cisco Aironet extensions on bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

Cisco Aironet extensions are enabled 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** global configuration command to specify the hold-off time for EAP and MAC address authentication. The holdoff time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point. Use the **no** form of the command to reset the parameter to defaults.

[no] dot11 holdoff-time *seconds*

Syntax Description

seconds	Specifies the hold-off time (1 to 65555 seconds)

Defaults

The default holdoff time is 0 (disabled).

Command Modes

Global configuration

Command History

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

Examples

This example shows how to specify a 2-minute hold-off time:

```
AP(config)# dot11 holdoff-time 120
```

This example shows how reset the hold-off time to defaults:

```
AP(config)# dot11 no holdoff-time
```

Related Commands

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

dot11 ids eap attempts

Use the **dot11 ids eap attempts** global configuration command to configure the number of authentication attempts and the number of seconds of EAPOL flooding that trigger a fault on a scanner access point in monitor mode.

Setting an authentication failure limit protects your network against a denial-of-service attack called *EAPOL flooding*. The 802.1X authentication that takes place between a client and the access point triggers a series of messages between the access point, the authenticator, and an authentication server using EAPOL messaging. The authentication server can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to impact your network.

A scanner access point in monitor mode tracks the rate at which 802.1X clients attempt to authenticate through the access point. If your network is attacked through excessive authentication attempts, the access point generates an alert when the authentication threshold has been exceeded.

[**no**] **dot11 ids eap attempts** *number* **period** *seconds*

Syntax Description

number	Specifies the number of authentication attempts that triggers a fault on a scanner access point in monitor mode
seconds	Specifies the number of seconds of EAPOL flooding that triggers a fault on a scanner access point in monitor mode

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to configure a limit on authentication attempts and on the duration of EAPOL flooding on a scanner access point in monitor mode:

```
ap(config)# dot11 ids eap attempts 10 period 10
```

Related Commands

Command	Description
debug dot11 ids	Enables wireless IDS debugging
show dot11 ids eap	Displays IDS statistics

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 lbs

Use the **dot11 lbs** global configuration command to create a location based services (LBS) profile and to enter LBS configuration mode.

[**no**] **dot11 lbs** *profile-name*

Syntax Description

profile-name	Specifies the name of the LBS profile

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to create an LBS profile and enter LBS configuration mode:

```
ap(config)# dot11 lbs southside
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
method (LBS configuration mode)	Specifies the location method used in an LBS profile
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

dot11 linktest

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

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

Syntax Description

interface-number	Specifies the radio interface number (The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.)
target *mac-address*	(Optional) Specifies the MAC address (in xxxx.xxxx.xxxx format) of the client device
count *packet-number*	(Optional) Specifies the number of packets (1 to 9999) to send to the client device
interval *sec*	(Optional) Specifies the time interval between tests (from 1 to 10000 seconds)
packet-size *size*	(Optional) Specifies the size of each packet (from 1 to 1400 bytes)
rate *value*	(Optional) Specifies a specific link test data rate. • Rates for the 802.11b, 2.4-GHz radio are 1, 2, 5, or 11 Mbps. • Rates for the 802.11g, 2.4-GHz radio are 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 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.
12.2(8)JA	Parameters were added to support the 5-GHz access point radio.
12.2(11)JA	Parameters were added to support the 5.8-GHz bridge radio.
12.2(13)JA	Parameters were added to support the 802.11g, 2.4-GHz access point radio.

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.

Note Some client devices, such as non-Cisco wireless clients, wired clients that are connected to a workgroup bridge, or non-Cisco clients connected to a repeater access point, might not respond to link test packets.

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 location isocc

Use the **dot11 location isocc** global configuration command to configure location identifiers that the access point sends with all RADIUS authentication and accounting requests.

dot11 location isocc *ISO-country-code* **cc** *country-code* **ac** *area-code*

Syntax Description

isocc *ISO-country-code*	Specifies the ISO country code that the access point includes in RADIUS authentication and accounting requests
cc *country-code*	Specifies the International Telecommunication Union (ITU) country code that the access point includes in RADIUS authentication and accounting requests
ac *area-code*	Specifies the ITU area code that the access point includes in RADIUS authentication and accounting requests

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Usage Guidelines

You can find a list of ISO and ITU country and area codes at the ISO and ITU websites. Cisco IOS software does not check the validity of the country and area codes that you enter with this command.

Examples

This example shows how to configure the ISO and ITU location codes on the access point:

```
ap(config)# dot11 location isocc us cc 1 ac 408
```

This example shows how the access point adds the SSID used by the client device and how it formats the location-ID string:

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

Related Commands

Command	Description
snmp-server location	Specifies the SNMP system location and the WISPr location-name attribute

dot11 mbssid

Use the **dot11 mbssid** global configuration command to enable multiple basic SSIDs on all access point radio interfaces.

[**no**] **dot11 mbssid**

Note This command is supported only on access points that contain at least one radio interface that supports multiple basic SSIDs. To determine whether a radio supports multiple basic SSIDs, enter the **show controllers** *radio_interface* command. Multiple basic SSIDs are supported if the results include this line:
Number of supported simultaneous BSSID on *radio_interface*: 8

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to enable multiple basic SSIDs on all interfaces that support multiple basic SSIDs:

```
ap(config)# dot11 mbssid
```

Related Commands

Command	Description
mbssid (SSID configuration mode)	Specifies that a BSSID is included in beacons and specifies a DTIM period for the BSSID
show dot11 bssid	Displays configured BSSIDs

dot11 meter

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

dot11 *interface-number* **meter**

Syntax Description

interface-number	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 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

collect-interval	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

This example shows how to generate a radio network map with a collection interval of 30 seconds:

```
ap(config)# dot11 network-map 30
```

You can verify the network map by using the **show dot11 network-map** EXEC command.

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**

Note This command is not supported on bridges.

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
```

dot11 priority-map avvid

Use the **dot11 priority-map avvid** global configuration command to enable or disable Cisco AVVID (Architecture for Voice, Video and Integrated Data) priority mapping. AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks. Use the **no** form of this command to disable AVVID priority mapping.

[**no**] **dot11 priority-map avvid**

Note This command is not supported on bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

AVVID priority mapping is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to stop or disable AVVID priority mapping:

```
AP(config)# no dot11 priority-map avvid
```

This example shows how to enable AVVID priority mapping:

```
AP(config)# dot11 priority-map avvid
```

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

dot11 ssid

Use the **dot11 ssid** global configuration command to create a global SSID. The SSID is inactive until you use the **ssid** configuration interface command to assign the SSID to a specific radio interface.

dot11 ssid *ssid*

In Cisco IOS Release 12.3(4)JA, you can configure SSIDs globally or for a specific radio interface. However, when you create an SSID using the **ssid** configuration interface command, the access point stores the SSID in global configuration mode.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to:

- Create an SSID in global configuration mode
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN
- Assign the SSID to a radio interface

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
```

Related Commands

Command	Description
show running-config ssid	Displays configuration details for SSIDs created in global configuration mode
ssid	Creates an SSID in configuration interface mode or assigns a globally configured SSID to a specific radio interface

dot11 update-group-key

Use the **dot11 update-group-key** privileged EXEC command to trigger an update of the WPA group key. When you enter the command, the access point distributes a new WPA group key to authenticated client devices.

dot11 *interface-number* **update-group-key** [**vlan** *vlan-id*]

Syntax Description

interface-number	Specifies the radio interface number (the 2.4-GHz radio is radio 0; the 5-GHz radio is radio 1)
vlan-id	Specifies the VLAN on which the access point sends out the group key update

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to trigger a group key update on VLAN 2:

```
AP# dot11 d0 update-group-key vlan 2
```

Related Commands

Command	Description
authentication key-management	Configures the radio interface (for a specified SSID) to support authenticated key management

dot11 vlan-name

Use the **dot11 vlan-name** global configuration command to assign a name to a VLAN in addition to its numerical ID.

dot11 vlan-name *name* **vlan** *vlan-id*

Syntax Description

name	Specifies a name to assign to a VLAN ID. The name can contain up to 32 ASCII characters.
vlan-id	Specifies the VLAN ID to which the name is assigned.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Usage Guidelines

Keep these guidelines in mind when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point, so across your network, you can assign the same VLAN name to a different VLAN ID.

Note If clients on your wireless LAN require seamless roaming, Cisco recommends that you assign the same VLAN name to the same VLAN ID across all access points, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point must have an ID, but VLAN names are optional.
- VLAN names can contain up to 32 ASCII characters. However, a VLAN name cannot be a number between 1 and 4095. For example, *vlan4095* is a valid VLAN name, but *4095* is not. The access point reserves the numbers 1 through 4095 for VLAN IDs.

Examples

This example shows how to assign a name to a VLAN:

```
AP(config)# dot11 vlan-name chicago vlan 121
```

You can view VLAN name and ID pairs by using the **show dot11 vlan-name** EXEC command.

Related Commands

Command	Description
show dot11 vlan-name	Displays VLAN name and ID pairs.

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

1-65555	Specifies a number of seconds (1 to 65555)
server	Specifies reauthentication period configured on the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to a client device before termination of the session. The server sends this attribute to the access point when a client performs EAP authentication.

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

duplex

To configure the duplex operation on a wireless device's Ethernet port, use the **duplex** interface configuration command. Use the **no** form of this command to return the system to auto-duplex mode.

[**no**] **duplex** {**auto** | **full** | **half**}

Note Cisco recommends that you use **auto**, the default setting, for both the duplex and speed settings on the Ethernet port.

Syntax Description

auto	Specifies auto-duplex operation. Cisco recommends that you use this setting.
full	Specifies full-duplex operation.
half	Specifies auto-duplex operation.

Defaults

The default duplex setting is **auto**.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the Ethernet port.

When the access point or bridge receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the unit. If the switch port to which the wireless device is connected is not set to **auto**, you can change the wireless device port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if the wireless device receives inline power from a switch, the wireless device reboots.

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

Examples

This example shows how to configure the Ethernet port for auto duplex:

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

Related Commands

Command	Description
speed (Ethernet interface)	Configures the speed setting on the Ethernet port

eapfast authority

Use the **eapfast authority** command to configure an EAP-FAST authority ID (AID) for a local authenticator access point. The EAP-FAST AID identifies the server that authenticates the EAP-FAST client. The local authenticator sends its AID to an authenticating client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new Protected Access Credential (PAC).

[**no**] **eapfast authority** {**id** *identifier* | **info** *string*}

Syntax Description

id *identifier*	Specifies an authority identifier for the local authenticator access point. Enter up to 32 hexadecimal digits for the AID.
info *string*	Specifies an AID information string. The information string is not used during EAP-FAST authentication, but it provides additional information about the local authenticator. Enter up to 32 ASCII characters.

Defaults

The default AID is LOCAL RADIUS SER.

Command Modes

Configuration mode for local authenticators

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to configure an AID for the local authenticator access point:

```
AP(config-radsrv)#eapfast authority id ap1200
```

This example shows how to configure an information string for the AID:

```
AP(config-radsrv)#eapfast authority id AP1200 A+G North
```

Related Commands

Command	Description
radius local-server pac-generate	Generates a PAC file for an EAP-FAST client

eapfast pac expiry

Use the **eapfast pac expiry** global configuration command to set the Protected Access Credential (PAC) expiration time and grace period for a group of EAP-FAST clients associated to a local authenticator access point.

[**no**] **eapfast pac expiry** *days* [**grace** *days*]

Syntax Description

days	Specifies the number of days that the PAC is valid for a group of EAP-FAST clients. Enter a number of days from 1 to 4095.
grace *days*	Specifies the grace period after the PAC expires. The PAC remains valid until the end of the grace period. Enter a number of days from 1 to 4095.

Defaults

The default is infinite days for both the expiration time and the grace period.

Command Modes

Client group configuration mode for local authenticators

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

In this example, PACs for the user group *clerks* expire in 10 days with a grace period of two days:

```
AP(config)#radius-server local
AP(config-radsrv)#group clerks
AP(config-radsrv-group)#eapfast pac expiry 10 grace 2
```

Related Commands

Command	Description
radius local-server pac-generate	Generates a PAC file for an EAP-FAST client

eapfast server-key

Use the **eapfast server-key** command to configure EAP-FAST server keys. The local authenticator uses server keys to encrypt Protected Access Credential (PAC) files that it generates and to decrypt PACs when it is authenticating clients. The server maintains two keys, a primary key and a secondary key, and uses the primary key to encrypt PACs. Periodically, the local authenticator switches keys, making the primary key the secondary and using the secondary key as the primary. If you do not configure server keys, the local authenticator generates keys automatically.

When the local authenticator receives a client PAC, it attempts to decrypt the PAC with the primary key. If decryption fails with the primary key, the authenticator attempts to decrypt the PAC with the secondary key. If decryption fails with the secondary key, the authenticator rejects the PAC as invalid.

[no] eapfast server-key {**primary** {**auto-generate** | [**0** | **7**] *key*} | **secondary** [**0** | **7**] *key*}

Syntax Description

primary {**auto-generate** | [**0** | **7**] *key*	Specifies a primary EAP-FAST server key. Use the **auto-generate** option to configure the local authenticator to generate a primary server key automatically. To configure a specific key, enter the key preceded by **0** or **7**. Keys can contain up to 32 hexadecimal digits. Enter **0** before the key to enter an unencrypted key. Enter **7** before the key to enter an encrypted key.
secondary [**0** | **7**] *key*	Specifies a secondary EAP-FAST server key. Enter the key preceded by **0** or **7**. Keys can contain up to 32 hexadecimal digits. Enter **0** before the key to enter an unencrypted key. Enter **7** before the key to enter an encrypted key.

Defaults

By default, the local authenticator generates server keys automatically.

Command Modes

Configuration mode for local authenticators

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to configure a primary server key for the local authenticator access point:

```
AP(config-radsrv)#eapfast server-key primary 0 2468
```

This example shows how to configure a secondary server key:

```
AP(config-radsrv)#eapfast server-key secondary 0 9753
```

Related Commands

Command	Description
radius local-server pac-generate	Generates a PAC file for an EAP-FAST client

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.

Note You need to configure static WEP keys only if your access point supports client devices that use static WEP. If all the client devices that associate to the access point use key management (WPA, CCKM, or 802.1x authentication) you do not need to configure static WEP keys.

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

Syntax Description

vlan *vlan-id*	Specifies the VLAN number (1 to 4095)
key *1-4*	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.) **Note** If you configure static WEP with MIC or CMIC, the access point and associated client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on the access point and the clients. See Table 2-5 for a list of WEP key restrictions based on your security configuration.
size 40bit	Specifies a 40-bit encryption key
size 128bit	Specifies a 128-bit encryption key
encryption-key	Specifies the value of the encryption key: • 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. Key slot 1 is the default key slot.

Defaults

This command has no defaults.

Command Modes

Configuration interface

Command History

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

Usage Guidelines

Using security features such as authenticated key management can limit WEP key configurations. Table 2-5 lists WEP key restrictions based on your security configuration.

Table 2-5 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	Access point and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both access point and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys

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
```

Related Commands

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

encryption mode ciphers

Use the **encryption mode ciphers** configuration interface command to enable a cipher suite. Cipher suites are sets of encryption algorithms that, like WEP, protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM).

Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode ciphers** command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

Note You can also use the **encryption mode wep** command to set up static WEP. However, you should use **encryption mode wep** only if all clients that associate to the access point are not capable of key management.

encryption [**vlan** *vlan*] **mode ciphers**
{[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]}
{[**wep128** | **wep40**]}

Syntax Description

vlan *vlan*	(Optional) Specifies the VLAN number
aes-ccm	Specifies that AES-CCMP is included in the cipher suite.
ckip[1]	Specifies that ckip is included in the cipher suite.
cmic[1]	Specifies that cmic is included in the cipher suite.
ckip-cmic[1]	Specifies that both ckip and cmic are included in the cipher suite.
tkip	Specifies that TKIP is included in the cipher suite. **Note** If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher.
wep128	Specifies that 128-bit WEP is included in the cipher suite.
wep40	Specifies that 40-bit WEP is included in the cipher suite.

1. You must enable Aironet extensions to use this option in the cipher suite.

Defaults

This command has no defaults.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(15)JA	This command was modified to include support for AES-CCMP.

Usage Guidelines

If you configure your access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 2-6 lists the cipher suites that are compatible with WPA and CCKM.

Table 2-6 Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

Note You must enable Aironet extensions to include CKIP, CMIC, or CKIP-CMIC in a cipher suite. Use the dot11 extension aironet command to enable Aironet extensions.

Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for a complete description of WPA and CCKM and instructions for configuring authenticated key management.

Examples

This example sets up a cipher suite for VLAN 22 that enables CKIP, CMIC, and 128-bit WEP.

```
ap(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
```

Related Commands

Command	Description
encryption mode wep	Configures the access point for WEP encryption
authentication open (SSID configuration mode)	Configures the client authentication type for an SSID, including WPA and CCKM authenticated key management

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.

Note Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode ciphers** command. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

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

Syntax Description

vlan *vlan-id*	(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

exception crashinfo buffersize

To change the size of the buffer used for crashinfo files, use the **exception crashinfo buffersize** command in global configuration mode. To revert to the default buffersize, use the **no** form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

Syntax Description

kilobytes	Sets the size of the buffersize to the specified value within the range of 32 to 100 kilobytes. The default is 32 KB.

Defaults

Crashinfo buffer is 32 KB.

Command Modes

Global config

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Usage Guidelines

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The access point writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

Examples

This example sets the crashinfo buffer to 100 KB:

```
ap(config)# exception crashinfo buffersize 100
```

Related Commands

Command	Description
exception crashinfo file	Enables the creation of a diagnostic file at the time of unexpected system shutdowns.

exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file** command in global configuration mode. To disable the creation of crashinfo files, use the **no** form of this command.

exception crashinfo file *device:filename*

no exception crashinfo file *device:filename*

Syntax Description

device:filename	Specifies the flash device and file name to be used for storing the diagnostic information. The colon is required.

Defaults

Creation of crashinfo files is disabled by default.

Command Modes

Global config

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Usage Guidelines

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The access point writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing). The filename will be *filename_yyyymmdd-hhmmss*, where *y* is year, *m* is month, *d* is date, *h* is hour, and *s* is seconds.

Examples

In this example, the access point creates a crashinfo file called *crashdata* in the default flash memory device if a system crash occurs:

```
ap(config)# exception crashinfo file flash:crashinfo
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.

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

256-2346	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

group (local server configuration mode)

Use the **group** local server configuration mode command to enter user group configuration mode and configure a user group to which you can assign shared settings. In user group configuration mode you can specify settings for the user group such as VLAN and SSID.

group *group*

Note This command is not supported on bridges.

Syntax Description

group	Specifies the name of the user group

Defaults

This command has no defaults.

Command Modes

Local server configuration mode

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to create a user group on the local authenticator:

```
AP(config-radsrv)# group hoosiers
```

Related Commands

Command	Description
nas (local server configuration mode)	Adds an access point to the list of NAS access points on the local authenticator
radius-server local	Enables the access point as a local authenticator and enters local server configuration mode
show running-config	Displays the current access point operating configuration
user (local server configuration mode)	Adds a user to the list of users allowed to authenticate to the local authenticator

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 monitored 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*

Note This command is not supported on bridges.

Syntax Description

mac-address	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 primary-shutdown	Shuts down the radio interface on the monitored access point when the standby access point takes over
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*]

Note This command is not supported on bridges.

Syntax Description

sec	Specifies the standby mode poll frequency in seconds
mac-address	Specifies the MAC address of an access point

Defaults

When you enable hot standby, the default poll frequency is 2 seconds.

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
iapp standby mac-address	Places the access point into standby mode and identifies the MAC address of the active access point
iapp standby primary-shutdown	Shuts down the radio interface on the monitored access point when the standby access point takes over
iapp standby timeout	Specifies the access point standby mode polling timeout value

iapp standby primary-shutdown

Use the **iapp standby primary-shutdown** global configuration command to disable the radio interfaces on the monitored access point when the standby access point becomes active. The standby access point sends a Dumb Device Protocol (DDP) message to disable the radios of the monitored access point when it detects a failure (for example, if the standby unit cannot associate to the monitored access point, or if the standby unit detects a link test failure on any of the monitored interfaces).

[no] iapp standby primary-shutdown

Note This command is not supported on bridges.

Note When the monitored access point receives the message to disable its radios it puts the radio interfaces into the *admin down* state. You must re-enable the radios to bring the radio interfaces back up.

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to enable the primary shutdown feature on a standby access point:

```
AP(config)# iapp standby primary-shutdown
```

Related Commands

Command	Description
iapp standby mac-address	Places the access point into standby mode and identifies the MAC address of the active access point
iapp standby poll-frequency	Specifies the polling interval in standby mode
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

sec	Specifies the standby mode polling timeout in seconds

Defaults

When you enable hot standby, the default standby timeout is 20 seconds.

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
iapp standby mac-address	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
iapp standby primary-shutdown	Shuts down the radio interface on the monitored access point when the standby access point takes over

information-element ssidl (SSID configuration mode)

Use the **information-element ssidl** SSID configuration command to designate an SSID for inclusion in an SSIDL information element (IE) that the access point includes in beacons. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

[**no**] **information-element ssidl** {[**advertisement**] [**wps**]}

Note When multiple basic SSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

Syntax Description

advertisement	Includes the SSID name and capabilities in the access point SSIDL IE.
wps	Sets the WPS capability flag in the SSIDL IE.

Defaults

By default, the access point does not include SSIDL IEs in beacons.

Command Modes

SSID configuration mode

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to designate an SSID for inclusion in the WPS IE:

```
AP(config-if-ssid)# information-element ssidl advertisement wps
```

Related Commands

Command	Description
ssid	Assigns an SSID to a specific interface.

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**

Note Enter this command on an access point or bridge. This command is not supported on devices configured as workgroup bridges.

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 or bridge to another. Use the **no** form of the command to revert to a normal non-infrastructure SSID.

[**no**] **infrastructure-ssid** [**optional**]

Syntax Description

optional	Specifies that both infrastructure and mobile client devices are allowed to associate using 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.

Usage Guidelines

This command controls the SSID that access points and bridges use when associating with one another. A root access point only allows a repeater access point to associate using the infrastructure SSID, and a root bridge only allows a non-root bridge to associate using the infrastructure SSID. Repeater access points and non-root bridges use this SSID to associate with root devices. Configure authentication types and VLANs for an SSID to control the security of access points and bridges.

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 dot11 (LBS configuration mode)

Use the **interface dot11** location based services (LBS) configuration mode command to specify the radio interface on which an LBS profile is enabled. An LBS profile remains inactive until you enter this command.

[no] interface dot11 {**0** | **1**}

Syntax Description

{**0** | **1**}	Specifies the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

Defaults

LBS profiles are disabled by default.

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to specify the radio interface for an LBS profile:

```
ap(dot11-lbs)# interface dot11 0
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
method (LBS configuration mode)	Specifies the location method used in an LBS profile
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

interface dot11radio

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

interface dot11radio *interface-number*

Syntax Description

interface-number	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 redirection

Use the **ip redirection** SSID configuration mode command to enable IP redirection for an SSID. When you configure IP redirection for an SSID, the access point redirects packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address.

You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point to redirect only packets addressed to specific ports, the access point redirects those packets from clients using the SSID and drops all other packets from clients using the SSID.

Note When you perform a ping test from the access point to a client device that is associated using an IP-redirect SSID, the response packets from the client are redirected to the specified IP address and are not received by the access point.

[**no**] **ip redirection** {**host** *ip-address* [**access-group** {*access-list-number* | *access-list-name*} **in**]}

Syntax Description

ip-address	Specifies the IP address to which packets are redirected. If you do not specify an access control list (ACL) which defines TCP or UDP ports for redirection, the access point redirects all packets that it receives from client devices.
access-list-number	Specifies the number of the ACL used for packet redirection.
access-list-name	Specifies the name of the ACL used for packet redirection.
in	Specifies that the ACL is applied to the access point's incoming interface.

Defaults

IP redirection is disabled by default.

Command Modes

SSID configuration mode

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point redirects all packets that it receives from client devices associated to the SSID *zorro*:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid zorro
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

This example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL. When the access point receives packets from client devices associated using the SSID robin, it redirects packets sent to the specified ports and discards all other packets:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid zorro
AP(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
AP(config-if-ssid)# end
```

Related Commands

Command	Description
ssid	Configure an SSID for the access point radio

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

seconds	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

size	Specifies the size of the internal buffer (4096 to 2147483647 bytes)
severity	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

logging snmp-trap

Use the **logging snmp-trap** global configuration command to specify the severity level of syslog messages for which the access point sends SNMP traps.

[**no**] **logging snmp-trap** *severity*

Syntax Description

severity	Specifies the severity levels for which the access point sends SNMP traps. You can enter a range of severity levels--**0** through **7**--or a single severity level. To specify a single severity level, enter **emergencies** (level 0), **alerts** (level 1), **critical** (level 2), **errors** (level 3), **warnings** (level 4), **notifications** (level 5), **informational** (level 6), or **debugging** (level 7).

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Usage Guidelines

For the **logging snmp-trap** command to operate correctly, you must also configure these global configuration commands on the access point:

```
AP(config)# logging history severity
AP(config)# snmp-server enable traps
AP(config)# snmp-server host address syslog
```

Examples

This example shows how to configure the access point to send SNMP traps for all severity levels:

```
AP(config)# logging snmp-trap 0 7
```

This example shows how to configure the access point to send SNMP traps only for warning messages:

```
AP(config)# logging snmp-trap warnings
```

Related Commands

Command	Description
logging buffered	Controls logging of messages to an internal buffer
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 *acl-index-or-name*	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 are100 to 199 and 2000 to 2699.
ip dscp *dscp-list*	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 *precedence-list*	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 *vlan-id*	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 maximun 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

value	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

mbssid

Use the **mbssid** configuration interface command to enable multiple basic SSIDs on an access point radio interface.

[**no**] **mbssid**

Note This command is supported only on radio interfaces that support multiple BSSIDs. To determine whether a radio supports multiple BSSIDs, enter the **show controllers** *radio_interface* command. Multiple BSSIDs are supported if the results include this line:
Number of supported simultaneous BSSID on *radio_interface*: 8

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to enable multiple BSSIDs on a radio interface:

```
ap(config-if)# mbssid
```

To enable multiple BSSIDs on all radio interfaces, use the **dot11 mbssid** global configuration command.

Related Commands

Command	Description
dot11 mbssid	Enables multiple BSSIDs on all radio interfaces that support multiple BSSIDs
mbssid (SSID configuration mode)	Specifies that a BSSID is included in beacons and specifies a DTIM period for the BSSID
show dot11 bssid	Displays configured BSSIDs

mbssid (SSID configuration mode)

Use the **mbssid** SSID configuration mode command to include the SSID name in the beacon and broadcast probe response and to configure the DTIM period for the SSID.

[**no**] **mbssid** [**guest-mode**] [**dtim-period** *period*]

Note This command is supported only on radio interfaces that support multiple basic SSIDs. To determine whether a radio supports multiple basic SSIDs, enter the **show controllers** *radio_interface* command. Multiple basic SSIDs are supported if the results include this line:
Number of supported simultaneous BSSID on *radio_interface*: 8

Syntax Description

guest-mode	Specifies that the SSID is included in beacons.
dtim-period *period*	Specifies the rate at which the device sends a beacon that contains a Delivery Traffic Indicator Message (DTIM). Enter a beacon rate between 1 and 100.

Defaults

Guest mode is disabled by default. The default period is 2, which means that every other beacon contains a DTIM.

Command Modes

SSID configuration interface

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Usage Guidelines

The guest mode and DTIM period configured in this command are applied only when MBSSIDs are enabled on the radio interface.

When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

Note Increasing the DTIM period count delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

If you configure a DTIM period for a BSSID and you also use the **beacon** command to configure a DTIM period for the radio interface, the BSSID DTIM period takes precedence.

Examples

This example shows how to include a BSSID in the beacon:

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

This example shows how to configure a DTIM period for a BSSID:

```
AP(config-if-ssid)# mbssid dtim-period 5
```

This example shows how to include a BSSID in the beacon and to configure a DTIM period:

```
AP(config-if-ssid)# mbssid guest-mode dtim-period 5
```

Related Commands

Command	Description
dot11 mbssid	Enables BSSIDs on all radio interfaces that support multiple BSSIDs
mbssid	Enables BSSIDs on a specific radio interface
show dot11 bssid	Displays configured BSSIDs

method (LBS configuration mode)

Use the **method** location based services (LBS) configuration mode command to specify the location method used in an LBS profile.

method *method*

Syntax Description

method	Specifies the location method used by the access point. In this release, **rssi** (in which the access point measures the location packet's received signal strength indication) is the only option and is also the default.

Defaults

The default location method is RSSI.

Command Modes

LBS configuration mode

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to specify the location method used in the LBS profile:

```
ap(dot11-lbs)# method rssi
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

mobile station

Use the **mobile station** configuration interface command to configure a bridge or a workgroup bridge as a mobile device. When you enable this setting on a device in non-root or workgroup bridge mode, the device scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a bridge configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the bridge does not search for a new association until it loses its current association.

[**no**] **mobile station**

Note This command is supported only on 1100 and 1200 series access points in workgroup bridge mode and on 1300 series access point/bridges in non-root or workgroup bridge mode.

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(15)JA	This command was introduced.
12.3(2)JA	Support added for 1100 series access points in workgroup bridge mode.
12.3(4)JA	Support added for 1200 series access points in workgroup bridge mode.

Usage Guidelines

This command can prevent data loss on a mobile workgroup bridge or bridge by ensuring that the bridge roams to a new parent device before it loses its current association.

Examples

This example shows how to specify that a bridge is a mobile station:

```
BR(config-if)# mobile-station
```

Related Commands

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

mobility network-id

Use the **mobility network-id** SSID configuration mode command to associate an SSID to a Layer 3 mobility network ID. Use the **no** form of the command to disassociate the SSID from the mobility network ID.

[**no**] **mobility network-id** *network-id*

Syntax Description

network-id	Specifies the Layer 3 mobility network identification number for the SSID

Defaults

This command has no defaults.

Command Modes

SSID configuration interface

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Examples

This example shows how to an SSID with a Layer 3 mobility network ID:

```
AP(config-if-ssid)# mobility network-id 7
```

This example shows how to reset the VLAN parameter to default values:

```
AP(config-if-ssid)# no mobility network-id
```

Related Commands

Command	Description
ssid	Specifies the SSID and enters the SSID configuration mode
wlccp authentication-server	Enables Layer 3 mobility on the access point

multicast address (LBS configuration mode)

Use the **multicast address** location based services (LBS) configuration mode command to specify the multicast address that LBS tag devices use when they send LBS packets.

multicast address *mac-address*

Syntax Description

mac-address	Specifies the multicast address that LBS tag devices use when they send LBS packets.

Defaults

The default multicast address is 01:40:96:00:00:10.

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to specify the multicast address used in the LBS profile:

```
ap(dot11-lbs)# multicast address 01.40.96.00.00.10
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
method (LBS configuration mode)	Specifies the location method used in an LBS profile
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

nas (local server configuration mode)

Use the **nas** local server configuration mode command to add an access point to the list of devices that use the local authenticator.

nas *ip-address* **key** *shared-key*

Syntax Description

ip-address	Specifies the IP address of the NAS access point
shared-key	Specifies the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the access points that use the local authenticator.

Defaults

This command has no defaults.

Command Modes

Local server configuration mode

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to add an access point to the list of NAS access points on the local authenticator:

```
AP(config-radsrv)# nas 10.91.6.158 key 110337
```

Related Commands

Command	Description
group (local server configuration mode)	Creates a user group on the local authenticator and enters user group configuration mode
radius-server local	Enables the access point as a local authenticator and enters local server configuration mode
user (local server configuration mode)	Adds a user to the list of users allowed to authenticate to the local server

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

1-128	Specifies the maximum number of retries (1 to 128)

Defaults

The default number of retries is 64.

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

packet-type (LBS configuration mode)

Use the **packet-type** location based services (LBS) configuration mode command to specify the LBS packet type that accepted in an LBS profile.

packet-type {**extended** | **short**}

Syntax Description

extended	Specifies that the access point accepts extended packets from LBS tag devices. An extended packet contains two bytes of LBS information in the frame body. If the packet does not contain those two bytes in the frame body, the access point drops the packet.
short	Specifies that the access point accepts short location packets from LBS tag devices. In short packets, the LBS information is missing from the tag packet's frame body and the packet indicates the tag's transmit channel.

Defaults

The default packet type is extended.

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to specify the packet type used in the LBS profile:

```
ap(dot11-lbs)# packet-type short
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
method (LBS configuration mode)	Specifies the location method used in an LBS profile
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
server-address (LBS configuration mode)	Specifies the IP address of the location server on your network

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

1-4	Specifies the parent root access point number (1 to 4)
mac-address	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 2
```

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 that a repeater tries to associate with a parent access point. Use the **no** form of the command to disable the timeout.

[**no**] **parent timeout** *sec*

Syntax Description

sec	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

Use the **power client** 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 (802.11b)

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

2.4-GHz Radio (802.11g)

[no] power client
{1 | 5 | 10 | 20 | 30 | 50 | 100} | maximum

5-GHz Radio (dot11radio1)

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

AIR-RM21A 5-GHz Radio Module (dot11radio1)

[no] power client
{ -1 | 2 | 5 | 8 | 11 | 14 | 16 | 17 | 20 | maximum }

Note This command is not supported on bridges.

Syntax Description

For the 802.11b, 2.4-GHz radio: **1**, **5**, **20**, **30**, **50**, **100**, **maximum**	Specifies a specific power level in mW or, on the AIR-RM21A 5-GHz radio module, in dBm. 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 802.11g, 2.4-GHz radio: **1**, **5**, **10**, **20**, **30**, **50**, **100**, **maximum**	For a list of maximum power levels allowed in each regulatory domain for the 2.4-GHz radio, see Table 2-7. For a list of maximum power levels allowed in each regulatory domain for the 5-GHz radio, see Table 2-8.
For the 5-GHz radio: **5**, **10**, **20**, **40**, **maximum**	**Note** The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.
If your access point contains an AIR-RM21A 5-GHz radio module, these power options are available (in dBm): **-1, 2, 5, 8, 11, 14, 16, 17, 20, maximum**	

Table 2-7 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

Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11 Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW. Maximum transmit power is limited depending on your regulatory domain.

Table 2-8 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
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 or bridge radio power level. Use the **no** form of the command to reset the parameter to defaults. On the 2.4-GHz, 802.11g radio, you can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices.

2.4-GHz Access Point Radio (802.11b)

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

2.4-GHz Access Point Radio (802.11g)

[**no**] **power local cck** {**1** | **5** | **10** | **20** | **30** | **50** | **100** | **maximum**}

[**no**] **power local ofdm** {**1** | **5** | **10** | **20** | **30** | **maximum**}

5-GHz Access Point Radio

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

AIR-RM21A 5-GHz Access Point Radio Module

[**no**] **power local**
{ **-1** | **2** | **5** | **8** | **11** | **14** | **16** | **17** | **20** | **maximum** }

5.8-GHz Bridge Radio

[**no**] **power local** {**12** | **15** | **18** | **21** | **22** | **23** | **24** | **maximum**}

Note The maximum transmit power for your bridge depends on your regulatory domain. If your bridge is configured at the factory for use in a regulatory domain other than North America or Korea, the transmit power options on your bridge are **16**, **13**, **12**, **10**, **9**, **8**, **7**, and **4** dBm.

Syntax Description

For the 802.11b, 2.4-GHz access point radio:
1, **5**, **20**, **30**, **50**, **100**, or **maximum**

For the 802.11g, 2.4-GHz access point radio:
1, **5**, **10**, **20**, **30**, **50**, **100**, or **maximum**

For the 5-GHz access point radio:
5, **10**, **20**, **40**, or **maximum**

If your access point contains an AIR-RM21A 5-GHz radio module, these power options are available (in dBm):

-1, 2, 5, 8, 11, 14, 16, 17, 20, maximum

For the 5.8-GHz bridge radio:
12, **15**, **18**, **21**, **22**, **23**, **24**, or **maximum**

Specifies access point power setting in mWor, on the AIR-RM21A 5-GHz radio module, in dBm. Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the access point. For a list of maximum power levels allowed in each regulatory domain for the 2.4-GHz access point radio, see Table 2-7. For a list of maximum power levels allowed in each regulatory domain for the 5-GHz access point radio, see Table 2-8.

Specifies bridge power setting in dBm. Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the bridge. For a list of maximum power levels allowed in each regulatory domain for the 5.8-GHz bridge radio, see Table 2-9.

Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11 Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54 Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW. Maximum transmit power is limited depending on your regulatory domain.

Table 2-9 Maximum Power Levels and Antenna Gains for 5.8-GHz Radios

	Maximum Power Settings				
Regulatory Domains	**Orientation**	**9-dBi Omnidirectional Antenna**	**9.5-dBi Sector Antenna**	**22.5-dBi Integrated Antenna**	**28-dBi Dish Antenna**
Americas (-A)	P2P[1]	24 dBm	24 dBm	24 dBm	22 dBm
	P2MP[2]	24 dBm	24 dBm	12[3] dBm[4]	–

1. Point to point.
2. Point to multipoint.
3. A maximum of 13 dBm is allowed, but that setting is not supported by the bridge.
4. On point-to-multipoint links, the remote bridges communicating with the central bridge are allowed to use a maximum power setting of 24 dBm. The central bridge is limited to a maximum power setting of 12 dBm.

Defaults

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

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 access point radio.
12.2(11)JA	Parameters were added to support the 5.8-GHz bridge radio.
12.2(13)JA	Parameters were added to support the 802.11g, 2.4-GHz access point radio.
12.3(2)JA	Parameters were added to support the AIR-RM21A 5-GHz access point radio module.

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	Displays the current access point operating configuration

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 access point 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

radius local-server pac-generate

Use the **radius local-server pac-generate** global configuration command to generate a Protected Access Credential (PAC) for a client device on a local authenticator access point. The local authenticator automatically generates PACs for EAP-FAST clients that request them. However, you might need to generate a PAC manually for some client devices. When you enter the command, the local authenticator generates a PAC file and writes it to the network location that you specify. The user imports the PAC file into the client profile.

radius local-server pac-generate *username filename* [**password** *password*] [**expire** *days*]

Syntax Description

username	Specifies the client username for which the PAC is generated.
filename	Specifies the name for the PAC file. When you enter the PAC file name, enter the full path to which the local authenticator writes the PAC file.
password *password*	Specifies a password used in password protection for the PAC file.
expire *days*	Specifies the number of days until the PAC file expires and is no longer valid.

Defaults

This default password for a PAC file is *test*, and the default expiration time is 1 day.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

In this example, the local authenticator generates a PAC for the username *joe*, password-protects the file with the password *bingo*, sets the PAC to expire in 10 days, and writes the PAC file to the TFTP server at 10.0.0.5:

```
AP# radius local-server pac-generate joe tftp://10.0.0.5/joe.pac password bingo expiry 10
```

Related Commands

Command	Description
radius-server local	Configures an access point as a local or backup authenticator
show running-config	Displays the current access point operating configuration
user (local server configuration mode)	Adds a user to the list of users allowed to authenticate to the local authenticator

radius-server local

Use the **radius-server local** global configuration command to enable the access point as a local or backup authenticator and to enter configuration mode for the local authenticator.

radius-server local

Note This command is not supported on bridges.

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to enable the access point as a local or backup authenticator:

```
AP(config)# radius-server local
```

Related Commands

Command	Description
group (local server configuration mode)	Creates a user group on the local authenticator and enters user group configuration mode
nas (local server configuration mode)	Adds an access point to the list of NAS access points on the local authenticator
show radius local-server statistics	Displays statistics for a local authenticator access point
show running-config	Displays the current access point operating configuration
user (local server configuration mode)	Adds a user to the list of users allowed to authenticate to the local authenticator

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.

Access Points

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

Bridges

[**no**] **rts**
{**threshold** *0-4000* | **retries** *1-128*}

Syntax Description

threshold *0-2347* (*0-4000* on bridges)	Specifies the packet size, in bytes, above which the access point or bridge negotiates an RTS/CTS before sending out the packet.
retries *1-128*	Specifies the number of times the access point or bridge issues an RTS before stopping the attempt to send the packet over the radio.

Defaults

The default **threshold** is 2312 bytes on access points and 4000 bytes on bridges.

The default number of **retries** is 32.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(11)JA	This command was modified to support bridges.

Usage Guidelines

On bridges set up in a point-to-point configuration, set the RTS threshold to 4000 on both the root and non-root bridges. If you have multiple bridges set up in a point-to-multipoint configuration, set the RTS threshold to 4000 on the root bridge and to 0 on the non-root bridges.

Examples

This example shows how to set the RTS threshold on a bridge to 4000 bytes:

```
bridge(config-if)# rts threshold 4000
```

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
```

server-address (LBS configuration mode)

Use the **server-address** LBS configuration mode command to specify the IP address of your location server and the port number on the server to which LBS access points send UDP packets that contain positioning information.

server-address *ip-address* **port** *port-number*

Syntax Description

ip-address	Specifies the IP address of the location server on your network.
port-number	Specifies the port on the location server to which LBS access points send UDP packets that contain positioning information. Enter a port number from 1024 to 65535.

Defaults

This command has no defaults.

Command Modes

LBS configuration mode

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to specify the IP address of your location server and a port on the server:

```
ap(dot11-lbs# server-address 10.91.107.19 port 1024
```

Related Commands

Command	Description
channel-match (LBS configuration mode)	Specifies that the LBS packet sent by an LBS tag must match the radio channel on which the access point receives the packet
dot11 lbs	Creates an LBS profile and enters LBS configuration mode
interface dot11 (LBS configuration mode)	Enables an LBS profile on a radio interface
method (LBS configuration mode)	Specifies the location method used in an LBS profile
multicast address (LBS configuration mode)	Specifies the multicast address that LBS tag devices use when they send LBS packets
packet-type (LBS configuration mode)	Specifies the LBS packet type accepted in an LBS profile

short-slot-time

Use the **short-slot-time** configuration interface command to enable short slot time on the 802.11g, 2.4-GHz radio. Short slot time reduces the slot time from 20 microseconds to 9 microseconds, thereby increasing throughput. The access point uses short slot time only when all clients that are associated to the 802.11g radio can support short slot time.

short-slot-time

Note This command is supported only on 802.11g, 2.4-GHz radios.

Syntax Description

This command has no arguments or keywords.

Defaults

Short slot time is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

This example shows how to enable short slot time:

```
AP(config-if)# short-slot-time
```

Related Commands

Command	Description
wlccp wds priority	Configures an access point as a candidate to provide wireless domain services (WDS)

show controllers dot11radio

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

show controllers dot11radio *interface-number*

Syntax Description

interface-number	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 aaa authentication mac-authen filter-cache

Use the **show dot11 aaa authentication mac-authen filter-cache** privileged EXEC command to display MAC addresses in the MAC authentication cache.

show dot11 aaa authentication mac-authen filter-cache [*address*]

Syntax Description

address	Specifies a specific MAC address in the cache.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Related Commands

Command	Description
clear dot11 aaa authentication mac-authen filter-cache	Clear MAC addresses from the MAC authentication cache.
dot11 activity-timeout	Enable MAC authentication caching.

show dot11 adjacent-ap

Use the **show dot11 adjacent-ap** privileged EXEC command to display the fast, secure roaming list of access points that are adjacent to this access point. The WDS access point builds the adjacent access point list based on data from client devices that support fast, secure roaming. This command works only when you configure your wireless LAN for fast, secure roaming and there are client devices on your wireless LAN that support fast, secure roaming.

show dot11 adjacent-ap

Note This command is not supported on bridges.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to display the adjacent access point list:

```
AP# show dot11 adjacent-ap
```

This example shows a list of adjacent access points:

```
Radio      Address                 Channel      Age(Hours)       SSID

--------   ---------------------- ------------ ---------------- ----------

0          0007.50d5.8759          1            1                tsunami
```

These are descriptions of the list columns:

- Radio—the interface number to which the client is currently associated
- Address—the MAC address of the adjacent access point from which the client device roamed
- Channel—the radio channel used by the adjacent access point
- Age (Hours)—the number of hours since a client roamed from the adjacent access point
- SSID—the SSID the client used to associate to the adjacent access point

Related Commands

Command	Description
dot11 adjacent-ap age-timeout	Specifies the number of hours an inactive entry remains in the adjacent access point list

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** | **cckm-statistics**]

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
H.H.H (mac-address)	(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
cckm-statistics	(Option) Displays fast, secure roaming (CCKM) latency statistics measured at the access point for client devices using CCKM

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 extension aironet	Starts a link test between the access point and a client device

show dot11 bssid

Use the **show dot11 bssid** privileged EXEC command to display the relationship between SSIDs and BSSIDs or MAC addresses.

show dot11 bssid

Syntax Description

This command has no arguments or keywords.

DefaultsDefaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Examples

This example shows how to display a list of BSSIDs and SSIDs:

```
AP# show dot11 bssid
```

This example shows the command output:

```
AP1230#show dot11 bssid
Interface      BSSID         Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  tsunami
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

Related Commands

Command	Description
dot11 mbssid	Enables BSSIDs on all radio interfaces that support multiple BSSIDs
mbssid	Enables BSSIDs on a radio interface
mbssid (SSID configuration mode)	Specifies that a BSSID is included in beacons and specifies a DTIM period for the BSSID

show dot11 carrier busy

Use the **show dot11 carrier busy** privileged EXEC command to display recent carrier busy test results. You can display test results once using this command. After the display, you must use the **dot11 carrier busy** command to run the carrier busy test again.

show dot11 carrier busy

Syntax Description

This command has no arguments or keywords.

DefaultsDefaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to display the carrier busy test results:

```
AP# show dot11 carrier busy
```

This example shows the carrier busy test results:

```
Frequency  Carrier Busy %
---------  --------------
5180             0
5200             2
5220            27
5240             5
5260             1
5280             0
5300             3
5320             2
```

Related Commands

Command	Description
dot11 carrier busy	Runs the carrier busy test

show dot11 ids eap

Use the **show dot11 ids eap** privileged EXEC command to display wireless IDS statistics.

show dot11 ids eap

Syntax Description

This command has no arguments or keywords.

DefaultsDefaults

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 wireless IDS information only if you first enable IDS on a scanner access point in monitor mode.

Examples

This example shows how to display wireless IDS statistics:

```
AP# show dot11 ids eap
```

Related Commands

Command	Description
dot11 ids eap attempts	Configures limits on authentication attempts and EAPOL flooding on scanner access points in monitor mode

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 dot11network-map

Syntax Description

This command has no arguments or keywords.

DefaultsDefaults

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 dot11 vlan-name

Use the **show dot11 vlan-name** privileged EXEC command to display VLAN name and ID pairs configured on the access point. If your access point is not configured with VLAN names or is configured only with VLAN IDs, there is no output for this command.

show dot11 vlan-name [*vlan-name*]

Syntax Description

vlan-name	(Optional) Displays the VLAN name and VLAN ID for a specific VLAN name

Defaults

When you do not specify a VLAN name, this command displays all VLAN name and ID pairs configured on the access point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Examples

This example shows how to display all VLAN name and ID pairs on an access point:

```
AP# show dot11 vlan-name
```

This example shows how to display the VLAN name and ID for a specific VLAN name:

```
AP# show dot11 vlan-name chicago
```

Related Commands

Command	Description
dot11 vlan-name	Assigns a VLAN name to a VLAN.

show environment

Use the **show environment** EXEC command to display information about the temperature of the bridge radio.

show environment

Note This command is supported only on bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to display temperature information for the bridge radio:

```
bridge# show environment
Environmental Statistics
    Environmental status as of 00:10:45 UTC Thu Mar 27 2003
    Data is 3 second(s) old, refresh in 57 second(s)

    Dot11Radio0 temperature measured at 37(C)
```

Related Commands

Command	Description
snmp-server enable traps envmon temperature	Enable an SNMP trap to announce near-out-of-range bridge radio temperature.

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

Note This command is not supported on bridges.

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
```

Related Commands

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

show iapp standby-parms

Use the **show iapp standby-parms** 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-parms

Note This command is not supported on bridges.

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-parms
```

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*

Note The output for this command does not contain CRC errors. To display CRC statistics, use the show interfaces dot11radio statistics command.

Syntax Description

interface-number	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

interface-number	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

interface-number	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 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

Command History

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
```

Related Commands

Command	Description
led flash	Enables or disables LED flashing

show power-injector

Use the **show power-injector** privileged EXEC command to display statistics related to the bridge power injector. Statistics include traffic counts and status for each port on the bridge power injector.

show power-injector

Note This command is supported only on bridges.

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(11)JA	This command was introduced.

Examples

This example shows how to display bridge power injector statistics:

```
bridge# show power-injector
```

show radius local-server statistics

Use the **show radius local-server statistics** privileged EXEC command to view statistics collected by the local authenticator.

show radius local-server 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(11)JA	This command was introduced.

Examples

This example shows how to display statistics from the local authenticator:

```
ap# show radius local-server statistics
```

This example shows local server statistics:

```
ap# show radius local-server statistics
Successes               : 0           Unknown usernames      : 0
Client blocks           : 0           Invalid passwords      : 0
Unknown NAS             : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes               : 0           Unknown usernames      : 0
Client blocks           : 0           Invalid passwords      : 0
Corrupted packet        : 0           Unknown RADIUS message : 0
No username attribute   : 0           Missing auth attribute : 0
Shared key mismatch     : 0           Invalid state attribute: 0
Unknown EAP message     : 0           Unknown EAP auth type  : 0
PAC refresh             : 0           Invalid PAC received   : 0

Username                   Successes  Failures  Blocks
janee                              0         0       0
jazke                              0         0       0
jsmith                             0         0       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists statistics for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include the following:

- Auto provision success—the number of PACs generated automatically
- Auto provision failure—the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh—the number of PACs renewed by clients

- Invalid PAC received—the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use this privileged exec mode command to reset local authenticator statistics to zero:

```
AP# clear radius local-server statistics
```

Related Commands

Command	Description
radius-server local	Configures the access point as a local or backup authenticator

show running-config ssid

Use the **show running-config ssid** privileged EXEC command to view configuration details for SSIDs that are configured globally.

show running-config ssid *ssid*

Syntax Description

ssid	Displays configuration details for a specific SSID.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Related Commands

Command	Description
dot11 ssid	Creates an SSID in global configuration mode
ssid	Creates an SSID for a specific radio interface or assigns a globally configured SSID to a specific interface

show spanning-tree

Use the **show spanning-tree** privileged EXEC command to display information about the spanning tree topology.

show spanning-tree
{*group* | **active** | **blockedports** | **bridge** | **brief** | **inconsistentports** | **interface** *interface* | **root** | **summary**}

Syntax Description

group	Specifies a bridge group from 1 to 255
active	Displays information only on interfaces in the active state
blockedports	Lists blocked ports
bridge	Displays status and information for this bridge
brief	Displays a brief summary of interface information
inconsistentports	Lists inconsistent ports
interface *interface*	Displays information for a specific interface
root	Displays status and configuration information for the spanning tree root
summary	Displays a summary of port states

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 STP information for bridge group 1:

```
bridge# show spanning-tree 1
```

This example shows how to display STP information for the bridge's radio interface:

```
bridge# show spanning-tree interface dot11radio0
```

Related Commands

Command	Description
bridge protocol ieee	Enables STP on the bridge

show wlccp

Use the **show wlccp** privileged EXEC command to display information on devices participating in Cisco Centralized Key Management (CCKM).

show wlccp
ap [**rm** [**context** | **accumulation**]] |
wnm status |
wds [**ap** [**detail** | **mac-address** *mac-address* [**mn-list**]]] |
[**mn** [**detail** | **mac-address** *mac-address*]] | [**statistics**] | [**nm**] |
[**aaa authentication mac-authen filter-cache**]

Note This command is not supported on bridges.

Syntax Description

ap [**rm** [**context**	**accumulation**]]	(Optional) When you enter this option on an access point participating in CCKM, this option displays the MAC address and IP address of the access point providing wireless domain services (WDS), the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator. • **rm**—Use this option to display information on radio measurement contexts or the radio measurement accumulation state.

wnm status	(Optional) This command displays the IP address of the wireless network manager (WNM) and the status of the authentication between the WNM and the WDS access point. Possible statuses include *not authenticated*, *auth in progress*, *authentication fail*, *authenticated*, and *security keys setup*.
wds [**ap** [**detail** | **mac-address** *mac-address* [**mn-list**]]] | [**mn** [**detail** | **mac-address** *mac-address*]] | [**statistics**] | [**nm**] | [**aaa authentication mac-authen filter-cache**]	(Optional) When you enter this option on the access point providing WDS, this option displays cached information about participating access points and client devices. • **ap**—Use this option to display information about access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the **mac-addr** sub-option to display information about a specific access point. Use the **mn-list** sub-option to display all the mobile nodes registered through the access point. • **mn**—Use this option to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the **detail** option to display the client's lifetime (seconds remaining before the client must send a refreshed registration), SSID, and VLAN ID. Use the **mac-address** option to display information about a specific client device. • **statistics**—Use this option to display statistics about devices participating in WDS and CCKM. • **aaa authentication mac-authen filter-cache**—Use this option to display MAC addresses in the MAC authentication cache.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.2(13)JA	This command was modified to include radio measurement options.

Examples

This example shows the command you enter on the access point providing WDS to list all client devices (mobile nodes) participating in CCKM:

```
AP# show wlccp wds mn
```

Related Commands

Command	Description
clear wlccp wds	Resets WDS statistics and removes devices from the WDS database
show dot11 aaa authentication mac-authen filter-cache	Displays MAC addresses in the MAC authentication cache
wlccp wds priority	Configures an access point as a candidate to provide wireless domain services (WDS)

snmp-server enable traps envmon temperature

Use the **snmp-server enable traps envmon temperature** global configuration command to enable an SNMP trap for monitoring bridge radio temperature. This trap is sent out when the bridge radio temperature approaches the limits of its operating range (55° C to –33° C; 131° F to –27.4° F).

snmp-server enable traps envmon temperature

Note This command is supported only on bridges.

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(11)JA	This command was introduced.

Examples

This example shows how to enable the envmon temperature trap:

```
bridge# snmp-server enable traps envmon temperature
```

Related Commands

Command	Description
show environment	Displays current temperature of the bridge radio

snmp-server group

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** global configuration command. To remove a specified SNMP group, use the **no** form of this command.

[**no**] **snmp-server group** [**groupname** {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]

Syntax Description

groupname	(Optional) Specifies the name of the group.
v1	(Optional) The least secure of the possible security models.
v2c	(Optional) The second-least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	(Optional) The most secure of the possible security models.
auth	(Optional) Specifies authentication of a packet without encrypting it.
noauth	(Optional) Specifies no authentication of a packet.
priv	(Optional) Specifies authentication of a packet with encryption.
read	(Optional) The option that allows you to specify a read view.
readview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables a user only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.
writeview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables a user to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view.
notifyview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
access	(Optional) The option that allows you to specify an access list.
access-list	(Optional) A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 2-10 lists the default settings for the SNMP views:

Table 2-10 Default View Settings

Setting	Description
readview	Assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless the user uses the read option to override this state.
writeview	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notifyview	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated will be sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Usage Guidelines

When a community string is configured internally, two groups with the name *public* are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name *public* and a v2c group with the name *public*.

Configuring Notify Views

Although the notifyview option allows you to specify a notify view when configuring an SNMP group, Cisco recommends that you avoid specifying a notify view for these reasons:

- The **snmp-server host** command autogenerates a notify view for the user and adds it to the group associated with that user.
- Modifying the group's notify view affects all users associated with that group.

The *notifyview* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you might need to change the notify view.
- The **snmp-server host** command might have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command or specify the appropriate notify view.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in global configuration mode:

Step	Command	Purpose
Step 1	**snmp-server user**	Configures an SNMP user.
Step 2	**snmp-server group**	Configures an SNMP group without adding a notify view.
Step 3	**snmp-server host**	Autogenerates the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

The following example shows how to enter a plain-text password for the string arizona2 for user John in group Johngroup, type the following command line:

```
snmp-server user John Johngroup v3 auth md5 arizona2
```

When you enter a **show running-config** command, you will not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

The following example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
snmp-server user John Johngroup v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Commands

Command	Description
snmp-server user	Configures a new user for an SNMP group
snmp-server view	Creates or modifies an SNMP view entry

snmp-server location

Use the **snmp-server location** global configuration command to specify the SNMP system location and the location-name attribute recommended by the Wi-Fi Alliance's guidelines for Wireless Internet Service Provider roaming (WISPr).

snmp-server location *location*

Syntax Description

location	Specifies the SNMP system location and the WISPr location-name attribute

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)JA	This command was introduced.

Examples

The *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document recommends that you enter the location name in this format:

hotspot_operator_name,*location*

This example shows how to configure the SNMP system location and the WISPr location-name attribute:

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

Related Commands

Command	Description
dot11 location isocc	Specifies ISO and ITU country and area codes that the access point includes in accounting and authentication requests

snmp-server user

To configure a new user to an SNMP group, use the **snmp-server user** global configuration command. To remove a user from an SNMP group, use the **no** form of the command.

[**no**] **snmp-server user** *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3**}[**encrypted**][**auth** {**md5** | **sha**} *auth-password* [**priv** *des56 priv password*]] [**access** ***access-list***]

Syntax Description

username	The name of the user on the host that connects to the agent.
groupname	(Optional) The name of the group to which the user is associated.
remote	(Optional) Specifies the remote copy of SNMP on the router.
ip-address	(Optional) The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
port	(Optional) A UDP port number that the host uses. The default is 162.
v1	(Optional) The least secure of the possible security models.
v2c	(Optional) The second-least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	(Optional) The most secure of the possible security models.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Initiates an authentication level setting session.
md5	(Optional) The HMAC-MD5-96 authentication level.
sha	(Optional) The HMAC-SHA-96 authentication level.
auth-password	(Optional) A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv	(Optional) The option that initiates a privacy authentication level setting session.
des56	(Optional) The CBC-DES privacy authentication algorithm.
priv password	(Optional) A string (not to exceed 64 characters) that enables the host to encrypt the contents of the message it sends to the agent.
access	(Optional) The option that enables you to specify an access list.
access-list	(Optional) A string (not to exceed 64 characters) that is the name of the access list.

Defaults

Table 2-11 describes default values for the **encrypted** option, passwords and access lists:

Table 2-11 Default Values for snmp-server user Options

Setting	Description
encrypted	Not present by default. Specifies that the **auth** and **priv** passwords are **MD5** digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted by default.
remote users	All users are assumed to be local to this SNMP engine unless you use the **remote** option to specify that they are remote.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the command **snmp-server engineID** with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication/privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Related Commands

Command	Description
snmp-server group	Configures a new SNMP group
snmp-server view	Creates or updates an SNMP view entry

snmp-server view

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified SNMP server view entry, use the **no** form of the command.

[**no**] **snmp-server view** *view-name oid-tree* {**included** | **excluded**}

Syntax Description

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
included | **excluded**	Type of view. You must specify either **included** or **excluded**.

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)JA	This command was introduced.

Usage Guidelines

Other SNMP commands require a view as an argument. You use this command to create a view to be used as arguments for other commands that create records including a view.

When a view is required, you can use one of two standard predefined views instead of defining a view. One predefined view is *everything*, which indicates that the user can see all objects. The other is *restricted*, which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

The first **snmp-server** command that you enter enables both versions of SNMP.

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
snmp-server view phred system included
snmp-server view phred cisco included
```

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

Related Commands

Command	Description
snmp-server group	Creates a new SNMP group
snmp-server user	Configures an SNMP user to a group

speed (Ethernet interface)

Use the **speed** (Ethernet) configuration interface command to configure the clock speed on the Ethernet port.

[no] speed {10 | 100 | auto}

Note Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the Ethernet port.

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
auto	Turns on the Fast Ethernet auto-negotiation capability. The interface automatically operates at 10 or 100 Mbps depending on the speed setting on the switch port to which the device is connected. This is the default setting.

Defaults

The default speed setting is **auto**.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the Ethernet port.

When the access point or bridge receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the unit.

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

Examples

This example shows how to configure the Ethernet port for auto duplex:

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

Related Commands

Command	Description
duplex	Configures the duplex setting for the Ethernet port

speed (radio interface)

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. Use the **no** form of the command to remove one or more data rates from the configuration.

2.4-GHz Access Point Radio (802.11b)

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

2.4-GHz Access Point Radio (802.11g)

speed
{ [**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**]
[**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**]
[**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] |
range |
throughput [**ofdm**] |
default }

Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.

5-GHz Access Point and Bridge Radios

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 802.11b, 2.4-GHz radio: [**1.0**] [**2.0**] [**5.5**] [**11.0**] For the 802.11g, 2.4-GHz radio: [**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] For the 5-GHz radio: [**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**]	(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. **Note** At least one of the access point's data rates must be set to a basic setting.
For the 802.11b, 2.4-GHz radio: [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-11.0**] For the 802.11g, 2.4-GHz radio: [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] 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**]	(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. **Note** The client must support the basic rate you select or it cannot associate to 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.
For the 802.11b, 2.4-GHz radio and the 5-GHz radio: **throughput**	(Optional) Sets the data rate for best throughput. On the 2.4-GHz radio, all data rates are set to basic. On the 5-GHz radio, all data rates are set to basic.
For the 802.11g, 2.4-GHz radio: **throughput** [**ofdm**]	(Optional) On the 802.11g radio, enter **speed throughput ofdm** to set all OFDM rates (6, 9, 12, 18, 24, 36, and 48) to basic (required) and set all the CCK rates (1, 2, 5.5, and 11) to disabled. This setting disables 802.11b protection mechanisms and provides maximum throughput for 802.11g clients. However, it prevents 802.11b clients from associating to the access point.
default	(Optional) Sets data rates to the default settings. **Note** This option is supported on 5-GHz radios and 802.11g, 2.4-GHz radios only. It is not available for 802.11b, 2.4-GHz radios.

Defaults

On the 802.11b, 2.4-GHz radio, all data rates are set to basic by default.

On the 802.11g, 2.4-GHz radio, data rates 1.0, 2.0, 5.5, 6.0, 11.0, 12.0, and 24.0 are set to basic by default, and the other data rates are supported.

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.
12.2(8)JA	Parameters were added to support the 5-GHz access point radio.
12.2(11)JA	Parameters were added to support the 5.8-GHz bridge radio.
12.2(13)JA	Parameters were added to support the 802.11g, 2.4-GHz access point radio.
12.3(2)JA	The **ofdm** parameter was added to the **throughput** option for the 802.11g, 2.4-GHz access point radio.

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
speed ofdm	Specifies the way that the access point advertises supported OFDM data rates in beacons and probe responses

speed ofdm

Use the **speed ofdm** configuration interface command to adjust the way that the access point advertises supported OFDM data rates in beacons and probe responses. Use the **no** form of the command to return to the default setting.

[**no**] **speed ofdm** {**join** | **separate**}

Syntax Description

join	Specifies that supported OFDM data rates appear in both information element (IE) 1 and IE 50. This is the default setting.
separate	Specifies that supported OFDM data rates appear only in IE 50.

Defaults

By default, supported OFDM data rates are listed in beacons and probe responses in both IE 1 and in IE 50.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.3(2)JA	This command was introduced.

Usage Guidelines

By default, access points are configured with the **speed ofdm join** command and advertise supported data rates in ascending order in both IE 1 and in IE 50 in beacons and probe responses:

IE 1: 1, 2, 5.5, 6, 9, 11, 12, 18

IE 50: 24, 36, 48, 54

However, some legacy 802.11b client devices cannot properly interpret the OFDM data rates in IE 1 and either associate at a data rate below 11 Mps or do not associate at all. To improve performance for these clients, you can use the **speed ofdm separate** command to list only 802.11b data rates in IE 1 and OFDM data rates in IE 50:

IE 1: 1, 2, 5.5, 11

IE 50: 6, 9, 12, 18, 24, 36, 48, 54

Examples

This example shows how to configure the access point to advertise only 802.11b data rates in IE 1 in beacons and probe responses:

```
AP(config-if)# speed ofdm separate
```

Related Commands

Command	Description
speed (radio interface)	Configures the supported data rates on access point radio interfaces

ssid

Use the **ssid** interface configuration command to assign a globally configured SSID to a radio interface. Use the **no** form of the command to remove an SSID from a radio interface.

[**no**] **ssid** *ssid-string*

In Cisco IOS Release 12.3(4)JA, you can configure SSIDs globally or for a specific radio interface, but all SSIDs are stored globally. After you use the **dot11 ssid** global interface command to create an SSID, you use the **ssid** command to assign the SSID to a specific interface.

Syntax Description

ssid-string	Specifies the SSID name for the radio, expressed as a case-sensitive alphanumeric stirng from 1 to 32 characters.

Defaults

On access points, the factory default SSID is *tsunami*. On bridges, the default SSID is *autoinstall*.

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 an 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:

- Create an SSID in global configuration mode
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN
- Assign the SSID to a radio interface

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
```

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
dot11 ssid	Creates an SSID in global configuration mode
guest-mode (SSID configuration mode)	Configures the radio interface (for the specified SSID) to support guest mode
max-associations (SSID configuration mode)	Configures the maximun number of associations supported by the radio interface (for the specified SSID)
show running-config ssid	Displays configuration details for SSIDs created in global configuration mode
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.

1100 and 1200 Series Access Points

station-role
{**repeater** | **root** [**fallback** {**shutdown** | **repeater**}] | **scanner** | **workgroup-bridge**}

350 Series Access Points

station-role
{**repeater** | **root** [**fallback** {**shutdown** | **repeater**}] | **scanner**}

1310 Access Points/Bridges

station-role
{**root** [**ap-only** [**fallback** {**shutdown** | **repeater**}]] |
repeater |
non-root [**wireless clients**] |
workgroup-bridge }

1400 Series Bridges

station-role
{**install** | **root** | **non-root**}

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. **Note** This option is not supported on 1400 series bridges.
root	On access points, 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. On bridges, specifies that the bridge operates as the root bridge in a pair or group of bridges.
root ap-only	On 1310 access points/bridges, specifies that the device functions as a root access point. If the Ethernet interface is not functional, the unit attempts to continue access point operation. However, you can specify a fallback mode for the radio. **Note** This option is supported only on 1310 access points/bridges.

scanner	This option is supported only when used with a WLSE device on your network. It specifies that the access point operates as a radio scanner only and does not accept associations from client devices. As a scanner, the access point collects radio data and sends it to the WDS access point on your network. **Note** This option is supported only on access points.
non-root	On 1310 and 1400 series bridges, specifies that the bridge operates as a non-root bridge and must associate to a root bridge. **Note** This option is supported only on 1310 access points/bridges and 1400 series bridges.
non-root wireless clients	(Optional) On 1310 access points/bridges, specifies that the bridge in non-root mode accepts associations from client devices. **Note** This option is supported only on 1310 access points/bridges.
fallback shutdown	(Optional) Specifies that the access point should shutdown when the primary Ethernet interface is not functional. **Note** This option is supported only on access points and on 1310 access points/bridges in access point mode.
fallback repeater	(Optional) Specifies that the access point should operate in repeater mode when the primary Ethernet interface is not functional. **Note** This option is supported only on access points and on 1310 access points/bridges in access point mode.
install	On 1400 series bridges, configures the bridge for installation mode. In installation mode, the bridge flashes its LEDs to indicate received signal strength (RSSI) to assist in antenna alignment. **Note** This option is supported only on 1400 series bridges.
workgroup-bridge	On 1100 and 1200 series access points and on 1310 access points/ bridges, specifies that the device operates in workgroup bridge mode. As a workgroup bridge, the device associates to an access point or bridge as a client and provides a wireless LAN connection for devices connected to its Ethernet port. **Note** This option is supported only on 1100 and 1200 series access points and on 1310 access points/bridges.

Defaults

Access points operate as root access points by default. When set to defaults, Cisco Aironet 1400 Series Wireless Bridges start up in install mode and adopt the root role if they do not associate to another bridge. If a 1400 series bridge associates to another bridge at start-up, it automatically adopts the non-root role. Cisco Aironet 1310 Access Points/Bridges operate as root access points by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(11)JA	This command was modified to support 5-GHz bridges.

Release	Modification
12.2(13)JA	This command was modified to include access point scanner mode and settings for 1300 series bridges.
12.3(2)JA	This command was modified to support workgroup-bridge mode on 1100 series access points.
12.3(4)JA	This command was modified to support workgroup-bridge mode on 1200 series access points and repeater mode on 1310 access points/bridges.

Examples

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

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

This example shows how to reset an access point or bridge to default operation:

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

This example shows how to set a bridge to root operation:

```
bridge(config-if)# station-role root
```

This example shows how to set a 1310 access point/bridge to root access point operation and shutdown when Ethernet is not functional:

```
bridge(config-if)# station-role root ap-only fallback shutdown
```

This example shows how to configure a 1310 access point/bridge as a non-root bridge that accepts associations from client devices:

```
bridge(config-if)# station-role non-root wireless clients
```

Related Commands

Command	Description
show running-config	Displays the current operating configuraion

station-role install

Use the **station-role install** configuration interface command to configure the bridge for installation mode. In installation mode, the bridge flashes the LEDs to indicate received signal strength.

station-role install
[**automatic** | **non-root** | **root**]

Note This command is supported only on 1400 series bridges.

Syntax Description

automatic	(Optional) Specifies that the bridge automatically selects the root or non-root role in install mode when it starts up. If the bridge does not associate to another bridge at start-up, the bridge adopts the root role. If a bridge associates to another bridge at start-up, it adopts the non-root role.
non-root	(Optional) Specifies that bridge starts up in install mode as a non-root bridge.
root	(Optional) Specifies that bridge starts up in install mode as a non-root bridge.

Defaults

When set to defaults, bridges start up in install automatic mode and adopt the root role if they do not associate to another bridge. If a bridge associates to another bridge at start-up, it automatically adopts the non-root role.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to set the bridge to install mode, non-root:

```
bridge(config-if)# station-role install non-root
```

Related Commands

Command	Description
station-role	Configures the bridge for root, non-root, or install mode

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** { **best-effort** | **background** | **video** | **voice** }
cw-min *0-10*
cw-max *0-10*
fixed-slot *0-20*

Syntax Description

best-effort	Specifies the best-effort traffic class category
background	Specifies the background traffic class category
video	Specifies the video traffic class category
voice	Specifies the voice traffic class category
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

When QoS is enabled, the default traffic class settings for access points match the values in Table 2-12, and the default traffic class settings for bridges match the values in Table 2-13.

Table 2-12 Default QoS Radio Traffic Class Definitions for Access Points

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time
Best Effort	5	10	2
Background	6	10	3
Video <100ms Latency	4	8	2
Voice <100ms Latency	2	8	2

Table 2-13 Default QoS Radio Traffic Class Definitions for Bridges

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time
Best Effort	4	10	2
Background	6	10	3
Video <100ms Latency	4	8	2
Voice <100ms Latency	2	8	2

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(13)JA	This command was modified to support four traffic classes (best-effort, background, video, and voice) instead of eight (0–7).

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.

For best performance on your bridge links, adjust the CW-min and CW-max contention window settings according to the values listed in Table 2-14. The default settings, CW-min 3 and CW-max 10, are best for point-to-point links. However, for point-to-multipoint links, you should adjust the settings depending on the number of non-root bridges that associate to the root bridge.

Note If packet concatenation is enabled on the bridge, adjust the CW-min and CW-max settings only for traffic class 0. Concatenation is enabled by default.

Table 2-14 CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links

Setting	Point-to-Point Links	Point-to-Multipoint Links with up to 5 Non-Root Bridges	Point-to-Multipoint Links with up to 10 Non-Root Bridges	Point-to-Multipoint Links with up to 17 Non-Root Bridges
CW-min	3	4	5	6
CW-max	10	10	10	10

Examples

This example shows how to configure the best-effort traffic class for contention windows and fixed slot backoff values. Each time the backoff for best-effort 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 best-effort cw-min 4 cw-max 10 fixed-slot 2
```

This example shows how to disable traffic class support:

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

Related Commands

Command	Description
concatenation (bridges only)	Enables packet concatenation on the bridge radio
show running-config	Displays the current operating configuration

user (local server configuration mode)

Use the **user** local server configuration command to specify the users allowed to authenticate using the local authenticator. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices. The access point performs up to 5 authentications per second.

user *username*
{**password** | **nthash**} *password*
[**group** *group-name*]
[**mac-auth-only**]

Note This command is not supported on bridges.

Syntax Description

username	Specifies the user's username. To add a client device for MAC-based authentication, enter the device's MAC address.
password *password*	Specifies the password assigned to the user. To add a client device for MAC-based authentication, enter the device's MAC address.
nthash *password*	Specifies the NT value of the user's password. If you only know the NT value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits.
group *group-name*	(Optional) Specifies the user group to which the user is assigned
mac-auth-only	(Optional) Specifies that the user is allowed to authenticate using only MAC authentication.

Defaults

This command has no defaults.

Command Modes

Local server configuration mode

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.2(15)JA	This command was modified to support MAC address authentication on the local authenticator.
12.3(2)JA	This command was modified to support EAP-FAST authentication on the local authenticator.

Examples

This example shows how to add a user to the list of clients allowed to authenticate using LEAP on the local authenticator:

```
AP(config-radsrv)# user sam password rover32 group cashiers
```

This example shows how to add a user to the list of clients allowed to authenticate using MAC-based authentication on the local authenticator:

```
AP(config-radsrv)# user 00074218d01b password 00074218d01b group cashiers
```

Related Commands

Command	Description
group (local server configuration mode)	Creates a user group on the local authenticator and enters user group configuration mode
nas (local server configuration mode)	Adds an access point to the list of NAS access points on the local authenticator
radius-server local	Enables the access point as a local authenticator and enters local server configuration mode
show running-config	Displays the current access point operating configuration

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

vlan-id	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

This example shows how to configure the VLAN that uses the radio SSID (wireless LAN):

```
AP(config-if-ssid)# vlan 2
```

This example shows how to reset the VLAN parameter to default values:

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

Related Commands

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

wlccp ap

Use the **wlccp ap** global configuration command to configure an access point to authenticate through the device configured for wireless domain services (WDS) and participate in Cisco Centralized Key Management (CCKM).

wlccp ap username *username* **password** *password*

Note This command is not supported on bridges.

Syntax Description

username *username*	Specifies the username that the access point uses when it authenticates through the device configured for WDS
password *password*	Specifies the password that the access point uses when it authenticates through the device configured for WDS

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the username and password for an access point that will participate in CCKM:

```
AP(config)# wlccp ap username birdman password 8675309
```

Related Commands

Command	Description
wlccp authentication-server	Specifies server lists for 802.1x authentication for client and infrastructure devices participating in CCKM

wlccp authentication-server

Use the **wlccp authentication-server** global configuration command to configure the list of servers to be used for 802.1x authentication for infrastructure devices and client devices enabled for Cisco Centralized Key Management (CCKM).

wlccp authentication-server
client { **any** | **eap** | **leap** | **mac** } *list* |
infrastructure *list*

Note This command is not supported on bridges and 350 series access points.

Syntax Description

client { **any** | **eap** | **leap** | **mac** } *list*	Specifies the server list to be used for 802.1x authentication for client devices. You can specify a server list for a specific 802.1x authentication method, or use the **any** option to specify a list to be used for for all 802.1x authentication methods. • **eap**—usually used with non-Cisco wireless adapters. Any wireless LAN client which uses a value of 0 in the algorithm field in the 802.11 association request frame can use EAP. This authentication-server setting must be used with the **authentication open eap** statement under the SSID configuration for each access point participating in WDS. • **leap**—usually used with Cisco Aironet wireless adapters. Any WLAN client which uses a value of 128 in the algorithm field in the 802.11 association request frame can use LEAP. This authentication-server setting must be used with the **authentication network-eap** statement under the SSID configuration for each access point participating in WDS. • **mac**—used for any RADIUS-based MAC authentication used with WDS. This authentication-server setting must be used with the **authentication open mac** or the **authentication network-eap mac** statement under the SSID configuration for each access point participating in WDS.
infrastructure *list*	Specifies the server list to be used for 802.1x authentication for infrastructure devices, such as other access points

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the server list for LEAP authentication for client devices:

```
AP(config)# wlccp authentication-server client leap leap-list1
```

This example shows how to configure the server list for 802.1x authentication for infrastructure devices participating in CCKM:

```
AP(config)# wlccp authentication-server infrastructure wlan-list1
```

Related Commands

Command	Description
authentication network-eap (SSID configuration mode)	Configures the radio interface (for the specified SSID) to support network-EAP authentication with optional MAC address authentication
authentication open (SSID configuration mode)	Configures the radio interface (for the specified SSID) to support open authentication and optionally MAC address authentication or EAP authentication
wlccp ap	Configures an access point to participate in CCKM
wlccp wds priority	Configures an access point for WDS

wlccp wds aaa authentication mac-authen filter-cache

Use the **wlccp wds aaa authentication mac-authen filter-cache** global configuration command to enable MAC authentication caching on the access point. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

wlccp wds aaa authentication mac-authen filter-cache [**timeout** *seconds*]

Syntax Description

timeout *seconds*	Specifies a timeout value for MAC authentications in the cache.

Defaults

MAC authentication caching is disabled by default. When you enable it, the default timeout value is 1800 (30 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)JA	This command was introduced.

Examples

This example shows how to configure MAC authentication caching with a one-hour timeout:

```
ap(config)# wlccp wds aaa authentication mac-authen filter-cache timeout 3600
```

Related Commands

Command	Description
clear dot11 aaa authentication mac-authen filter-cache	Clear MAC addresses from the MAC authentication cache.
dot11 aaa authentication mac-authen filter-cache	Enable MAC authentication caching on the access point.
show dot11 aaa authentication mac-authen filter-cache	Display MAC addresses in the MAC authentication cache.
show wlccp	Display information on devices participating in Cisco Centralized Key Management (CCKM) and WDS, including addresses in the MAC authentication cache.

wlccp wds priority

Use the **wlccp wds priority** global configuration command to configure an access point to provide Wireless Domain Services (WDS). When configuring Cisco Centralized Key Management (CCKM), you configure one or more access points or switches as candidates to provide WDS. The device with the highest priority provides WDS.

wlccp wds
priority *priority*
interface *interface*

Note This command is not supported on bridges and 350 series access points.

Syntax Description

priority *priority*	Specifies the priority of the access point among devices configured to provide WDS. Enter a priority number from 1 to 255.
interface *interface*	Specifies the interface on which the access point sends out WDS advertisements. For this release, you must use **bvi 1** as the interface for WDS advertisements.

Defaults

This command has no defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS:

```
AP(config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
wlccp ap	Configures an access point to participate in CCKM
wlccp authentication-server	Specifies server lists for 802.1x authentication for client and infrastructure devices participating in CCKM

wlccp wnm ip address

Use the **wlccp wnm ip address** global configuration command to configure the IP address of the wireless network manager (WNM) that performs network management for the wireless LAN to which the access point belongs.

wlccp wnm ip address

Note This command is not supported on bridges.

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(13)JA	This command was introduced.

Examples

This example shows how to configure the IP address of the wireless network manager:

```
AP(config)# wlccp wnm ip address 10.10.0.101
```

Related Commands

Command	Description
wlccp ap	Configures an access point to participate in CCKM
wlccp authentication-server	Specifies server lists for 802.1x authentication for client and infrastructure devices participating in CCKM

workgroup-bridge client-vlan

Use the **workgroup-bridge client-vlan** configuration interface command to assign a VLAN to the devices attached to a workgroup bridge. This command enables VLAN trunking on the workgroup bridge's radio and Ethernet interfaces.

workgroup-bridge client-vlan *vlan-id*

Note This command is supported only on 1100 and 1200 series access points and 1300 series access points/bridges.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no defaults.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)JA	This command was introduced.
12.3(2)JA	This command was modified to support 1100 series access points.

Examples

This example shows how to assign a VLAN to the devices attached to a workgroup bridge:

```
wgb(config-if)# workgroup-bridge client-vlan 17
```

Related Commands

Command	Description
show running-config	Displays the current operating configuration

world-mode

Use the **world-mode** configuration interface mode command to enable access point world mode operation. You can configure the access point to support 802.11d world mode or Cisco legacy world mode. Use the **no** form of the command to disable world mode operation.

[**no**] **world-mode**
dot11d country_code *code* {**both** | **indoor** | **outdoor**} |
legacy

Syntax Description

dot11d country_code *code* {**both** | **indoor** | **outdoor**}	Enables 802.11d world mode. • When you enter the **dot11d** option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is **US**). You can find a list of ISO country codes at the ISO website. • After the country code, you must enter **indoor**, **outdoor**, or **both** to indicate the placement of the access point.
legacy	Enables Cisco legacy world mode.

Defaults

World mode is disabled by default.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(15)JA	This command was modified to support 802.11d world mode.

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. Cisco client devices running firmware version 5.30.17 or later detect whether the access point is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the access point.

Examples

This example shows how to enable 802.11d world mode operation:

```
AP(config-if)# world-mode dot11d country-code TH both
```

This example shows how to disable world mode operation:

```
AP(config-if)# no world-mode dot11d
```

Related Commands

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

wpa-psk

Use the **wpa-psk** SSID interface configuration command to configure a pre-shared key for use in WPA authenticated key management. To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key for the SSID.

wpa-psk { **hex** | **ascii** } [**0** | **7**] *encryption-key*

Note This command is not supported on bridges.

Syntax Description

hex	Specifies entry of the pre-shared key in hexadecimal characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key.
ascii	Specifies ASCII entry of the pre-shared key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.
encryption-key	Specifies the pre-shared key

Defaults

This command has no defaults.

Command Modes

SSID configuration interface

Command History

Release	Modification
12.2(11)JA	This command was introduced.

Examples

This example shows how to configure a WPA pre-shared key for an SSID:

```
AP(config-if-ssid)# wpa-psk ascii shared-secret-key
```

Related Commands

Command	Description
authentication key-management	Specifies authenticated key management for an SSID
encryption mode ciphers	Specifies a cipher suite
ssid	Specifies the SSID and enters SSID configuration mode