



## **Wireless LAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)**

**First Published:** January 11, 2013

**Last Modified:** January 11, 2013

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## CONTENTS

---

### CHAPTER 1

#### accounting (SSID configuration mode) through encryption mode wep 1

- accounting (SSID configuration) 3
- antenna 4
- authentication key-management 6
- authentication network-eap 8
- authentication open (SSID configuration) 10
- authentication shared (SSID configuration) 12
- beacon 14
- block count 15
- broadcast-key 17
- channel 19
- clear dot11 client 21
- clear dot11 hold-list 22
- clear dot11 statistics 23
- clear radius local-server 24
- debug dot11 26
- debug dot11 aaa 28
- debug dot11 dot11radio 31
- debug radius local-server 34
- dfs band block 36
- distance 38
- dot11 aaa authentication mac-authen filter-cache 39
- dot11 aaa dot1x compliance 41
- dot11 aaa csid 42
- dot11 activity-timeout 44
- dot11 extension aironet 46
- dot11 holdoff-time 47
- dot11 igmp snooping-helper 48

dot11 location isocc 49

dot11 mbssid 51

dot11 phone 52

dot11 priority-map avvid 53

dot11 qos class 54

dot11 qos mode wmm 56

dot11 ssid 57

dot11 syslog 59

dot11 vlan-name 60

dot1x client-timeout 62

dot1x reauth-period 63

encryption key 65

encryption mode ciphers 68

encryption mode wep 71

---

## CHAPTER 2

**fragment-threshold through wpa-psk 73**

fragment-threshold 75

guest-mode (SSID configuration) 76

information-element ssid 78

infrastructure client 79

infrastructure-ssid 80

interface dot11Radio 82

l2-filter bridge-group-acl 83

match vlan 84

max-associations (SSID configuration) 86

mbssid 87

nas 88

packet retries 90

payload-encapsulation 91

power client 92

power local 94

preamble-short 96

radius-server local 97

reauthentication time 99

rts 101

[show controllers dot11Radio](#) 102

[show dot11 aaa authentication mac-authen filter-cache](#) 105

[show dot11 associations](#) 106

[show dot11 carrier busy](#) 109

[show dot11 statistics client-traffic](#) 111

[show dot11 statistics interface](#) 112

[show dot11 vlan-name](#) 115

[show interfaces dot11Radio](#) 116

[show interfaces dot11Radio aaa timeout](#) 118

[show interfaces dot11Radio statistics](#) 119

[show platform software infrastructure lsmapi](#) 121

[show radius local-server statistics](#) 124

[speed \(access point radio\)](#) 126

[ssid](#) 129

[station-role](#) 131

[traffic-class](#) 133

[user](#) 135

[vlan \(SSID configuration\)](#) 138

[world-mode](#) 139

[wpa-psk](#) 141





## accounting (SSID configuration mode) through encryption mode wep

---

- [accounting \(SSID configuration\), page 3](#)
- [antenna, page 4](#)
- [authentication key-management, page 6](#)
- [authentication network-eap, page 8](#)
- [authentication open \(SSID configuration\), page 10](#)
- [authentication shared \(SSID configuration\), page 12](#)
- [beacon, page 14](#)
- [block count, page 15](#)
- [broadcast-key, page 17](#)
- [channel, page 19](#)
- [clear dot11 client, page 21](#)
- [clear dot11 hold-list, page 22](#)
- [clear dot11 statistics, page 23](#)
- [clear radius local-server, page 24](#)
- [debug dot11, page 26](#)
- [debug dot11 aaa, page 28](#)
- [debug dot11 dot11radio, page 31](#)
- [debug radius local-server, page 34](#)
- [dfs band block, page 36](#)
- [distance, page 38](#)
- [dot11 aaa authentication mac-authen filter-cache, page 39](#)
- [dot11 aaa dot1x compliance, page 41](#)
- [dot11 aaa csid, page 42](#)

- [dot11 activity-timeout, page 44](#)
- [dot11 extension aironet, page 46](#)
- [dot11 holdoff-time, page 47](#)
- [dot11 igmp snooping-helper, page 48](#)
- [dot11 location isocc, page 49](#)
- [dot11 mbssid, page 51](#)
- [dot11 phone, page 52](#)
- [dot11 priority-map avvid, page 53](#)
- [dot11 qos class, page 54](#)
- [dot11 qos mode wmm, page 56](#)
- [dot11 ssid, page 57](#)
- [dot11 syslog, page 59](#)
- [dot11 vlan-name, page 60](#)
- [dot1x client-timeout, page 62](#)
- [dot1x reauth-period, page 63](#)
- [encryption key, page 65](#)
- [encryption mode ciphers, page 68](#)
- [encryption mode wep, page 71](#)



# accounting (SSID configuration)

To enable RADIUS accounting for the radio interface, use the **accounting** command in SSID interface configuration mode. To disable RADIUS accounting, use the no form of this command.

**accounting list-name**

**no accounting**

## Syntax Description

|           |                                 |
|-----------|---------------------------------|
| list-name | The name of an accounting list. |
|-----------|---------------------------------|

## Command Default

RADIUS accounting for the radio interface is disabled.

## Command Modes

SSID interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

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

## Examples

The following example shows how to enable RADIUS accounting and set the RADIUS server name:

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

This example shows how to disable RADIUS accounting:

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

## Related Commands

| Command        | Description  |
|----------------|--|
| aaa accounting | Creates a method list for accounting.                  |
| ssid           | Specifies the SSID and enters SSID configuration mode. |

# antenna

To configure the radio receive or transmit antenna settings, use the **antenna** command in interface configuration mode. To reset the receive or transmit antenna to its default setting, use the **no** form of this command.

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

**no antenna**

## Syntax Description

|                  |   |
|------------------|---|
| <b>receive</b>   | Specifies the antenna that the access point uses to receive radio signals.  |
| <b>transmit</b>  | Specifies the antenna that the access point uses to transmit radio signals. |
| <b>diversity</b> | Specifies the antenna with the best signal. Default value.                  |
| <b>left</b>      | Specifies to use the left antenna only.                                     |
| <b>right</b>     | Specifies to use the right antenna only.                                    |

## Command Default

The default antenna setting is **diversity**.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

You can select the antenna the wireless device uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- **diversity** --This default setting tells the wireless device to use the antenna that receives the best signal. If the wireless device has two fixed (nonremovable) antennas, you should use this setting for both receive and transmit.
- **left** --If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's left connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the left antenna is on the left.

- **right** --If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's right connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the right antenna is on the right.

The Cisco 850 series routers have only one antenna, and do not support diversity.

### Examples

The following example shows how to specify the right receive option:

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

# authentication key-management

To configure the radio interface to support authenticated key management, use the **authentication key-management command in SSID interface** configuration mode. To disable key management, use the **no** form of this command.

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

**no authentication key-management wpa**

## Syntax Description

|                 |   |
|-----------------|---|
| <b>wpa</b>      | Specifies Wi-Fi Protected Access (WPA) authenticated key management for the service set identifier (SSID).  |
| <b>cckm</b>     | Specifies Cisco Centralized Key Management (CCKM) authenticated key management for the SSID.                |
| <b>optional</b> | (Optional) Specifies that client devices that do not support authenticated key management can use the SSID. |

## Command Default

Key management is disabled.

## Command Modes

SSID interface configuration

## 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. |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.                    |

## 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 preshared 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.

**Note**

CCKM is not supported in this release.

**Examples**

The following example shows how to enable WPA for an SSID:

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

**Related Commands**

| Command                 | Description   |
|-------------------------|---|
| encryption mode cyphers | Enables a cipher suite.   |
| wpa-psk                 | Configures a preshared key for use in WPA authenticated key management. |

## authentication network-eap

To configure the radio interface to support network Extensible Authentication Protocol (EAP) authentication, use the **authentication network-eap** command in SSID interface configuration mode. To disable network EAP authentication, use the no form of this command.

**authentication network-eap** *list-name* [**mac-address** *list-name*]

**no authentication network-eap**

### Syntax Description

|                                     |   |
|-------------------------------------|---|
| <i>list-name</i>                    | The list name for EAP authentication. List name can be from 1 to 31 characters in length. |
| <b>mac-address</b> <i>list-name</i> | (Optional) Specifies the list name for MAC authentication.                                |

### Command Default

Network EAP authentication is disabled.

### Command Modes

SSID interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

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

### Examples

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

```
Router(config-if-ssid)# authentication network-eap list1  
This example shows how to disable network-eap authentication:
```

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

**Related Commands**

| Command   | Description                          |
|---|--------------------------------------|
| aaa authentication login                          | Sets authentication for login.       |
| <b>authentication open (SSID configuration)</b>   | Specifies open authentication.       |
| <b>authentication shared (SSID configuration)</b> | Specifies shared-key authentication. |

## authentication open (SSID configuration)

To configure the radio interface for the specified service set identifier (SSID) to support open authentication, and optionally MAC address authentication or Extensible Authentication Protocol (EAP) authentication, use the **authentication open** command in SSID interface configuration mode. To disable open authentication for the SSID, use the **no** form of this command.

**authentication open** [**mac-address** *list-name*] [**eap** *list-name*]

**no authentication open**

### Syntax Description

|                                     |  |
|-------------------------------------|--|
| <b>mac-address</b> <i>list-name</i> | (Optional) Specifies the list name for MAC authentication. List name can be from 1 to 31 characters in length. |
| <b>eap</b> <i>list-name</i>         | (Optional) Specifies the list name for EAP authentication. List name can be from 1 to 31 characters in length. |

### Command Default

Open authentication is disabled.

### Command Modes

SSID interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

Use this command to authenticate clients using the open method, with optional MAC address or EAP screenings.

To define list names for MAC addresses and EAP, use the **aaa authentication login** command in the *Cisco IOS Security Command Reference*, Release 12.4. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.

### Examples

The following example shows how to enable MAC authentication using a local list:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# username 00123456789a password 00123456789a
Router(config)# username 00123456789a autocommand exit
Router(config)# username 0023456789ab password 0023456789ab
Router(config)# username 0023456789ab autocommand exit
```



```

Router(config)# username 003456789abc password 003456789abc
Router(config)# username 003456789abc autocommand exit
Router(config)# aaa authentication login mac-methods local
Router(config)# interface dot11radio 0
Router(config-if)# ssid sample1
Router(config-if-ssid)# authentication open mac-address mac-methods
Router(config-if-ssid)# end

```

The following example shows how to enable MAC authentication using a RADIUS server:

```

Router# configure terminal
Router(config)# aaa new-model
! Replace BVI1 if routing mode is used
Router(config)# ip radius source-interface BVI1
Router(config)# radius-server attribute 32 include-in-access-req format %h
Router(config)# radius-server host 10.2.0.1 auth-port 1812 acct-port 1813 key cisco
Router(config)# radius-server vsa send accounting
Router(config)# aaa group server radius rad-mac
Router(config)# server 10.2.0.1 auth-port 1812 acct-port 1813
Router(config)# aaa authentication login mac-methods rad-mac
Router(config)# interface dot11radio 0
Router(config-if)# ssid name1
Router(config-if-ssid)# authentication open mac-address mac-methods
Router(config-if-ssid)# end

```

## Related Commands

| Command                                     | Description  |
|---|--|
| aaa authentication login                    | Sets authentication for login.                         |
| authentication network eap                  | Specifies network EAP authentication.                  |
| authentication shared (SSID authentication) | Specifies shared key authentication.                   |
| ssid  | Specifies the SSID and enters SSID configuration mode. |

## authentication shared (SSID configuration)

To configure the radio interface to support shared authentication, use the **authentication shared** command in **SSID interface** configuration mode. To disable shared authentication, use the no form of this command.

**authentication shared** [**mac-address list-name**] [**eap list-name**]

**no authentication shared**

### Syntax Description

|                       |   |
|-----------------------|---|
| mac-address list-name | (Optional) Specifies the list name for MAC authentication. List name can be from 1 to 31 characters in length.                                      |
| eap list-name         | (Optional) Specifies the list name for Extensible Authentication Protocol (EAP) authentication. List name can be from 1 to 31 characters in length. |

### Command Default

The service set identifier (SSID) authentication type is set to shared key.

### Command Modes

SSID interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

Use this command to authenticate clients using the shared method.

You can assign shared key authentication to only one SSID.

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:

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

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

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

**Related Commands**

| Command  | Description                           |
|--|---------------------------------------|
| aaa authentication login                         | Sets authentication for login.        |
| <b>authentication open (SSID authentication)</b> | Specifies open authentication.        |
| <b>authentication network-eap</b>                | Specifies network EAP authentication. |

# beacon

To specify how often the beacon contains a Delivery Traffic Indicator Message (DTIM), use the **beacon** command in interface configuration mode. To reset the beacon interval to the default values, use the **no** form of this command.

**beacon** {*period microseconds* | *dtim-period period-count*}

**no beacon**

## Syntax Description

|  |  |
|--|--|
| <b>period</b> <i>microseconds</i>      | Specifies the beacon time in Kilomicroseconds (Kms). Kms is a unit of measurement in software terms. K = 1024, m = 10 <sup>-6</sup> , and s = seconds, so Kms = 0.001024 seconds, 1.024 milliseconds, or 1024 microseconds. Range is from 20 to 4000 microseconds. Default is 100. |
| <b>dtim-period</b> <i>period-count</i> | Specifies the number of DTIM beacon periods to wait before delivering multicast packets. Range is from 1 to 100. Default is 2.   |

## Command Default

The default **period** is 100 microseconds. The default **dtim-period** is 2 beacon periods.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## 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

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

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

## block count

To lock out group members for a length of time after a set number of incorrect passwords are entered, use the **block count** command in local RADIUS server group configuration mode. To remove the user block after invalid login attempts, use the **no** form of this command.

**block count** *count* **time** {seconds|infinite}

**no block count** *count* **time** {seconds|infinite}

### Syntax Description

|                 |  |
|-----------------|--|
| <i>count</i>    | Number of failed passwords that triggers a lockout. Range is from 1 to 4294967295. |
| <b>time</b>     | Specifies the time to block the account.   |
| <i>seconds</i>  | Number of seconds that the lockout should last. Range is from 1 to 4294967295.     |
| <b>infinite</b> | Specifies the lockout is indefinite.   |

### Command Default

No default behavior or values

### Command Modes

Local RADIUS server group configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
| 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

### Usage Guidelines

If the **infinite** keyword is entered, an administrator must manually unblock the locked username.

### Examples

The following command locks out group members for 120 seconds after three incorrect passwords are entered:

```
Router(config-radsrv-group) #
block count 3 time 120
```

**Related Commands**

| <b>Command</b>                             | <b>Description</b>   |
|--|--|
| <b>clear radius local-server</b>           | Clears the statistics display or unblocks a user.  |
| <b>debug radius local-server</b>           | Displays the debug information for the local server.   |
| <b>group</b>                               | Enters user group configuration mode and configures shared setting for a user group.   |
| <b>nas</b>                                 | Adds an access point or router to the list of devices that use the local authentication server.                                  |
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>                 | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>reauthentication time</b>               | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.  |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.   |
| <b>user</b>                                | Authorizes a user to authenticate using the local authentication server.   |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.  |

## broadcast-key

To configure the time interval between rotations of the broadcast encryption key used for clients, use the **broadcast-key** command in interface configuration mode. To disable broadcast key rotation, use the no form of this command.

**broadcast-key** [*vlan vlan-id*] [*change seconds*] [*membership-termination*] [*capability-change*]  
**no broadcast-key**

### Syntax Description

|                        |  |
|------------------------|--|
| vlan vlan-id           | (Optional) Specifies the virtual LAN (VLAN) identification value. Range is from 1 to 4095.   |
| change seconds         | (Optional) Specifies the amount of time (in seconds) between the rotation of the broadcast encryption key. Range is from 10 to 10000000.   |
| membership-termination | (Optional) If Wi-Fi Protected Access (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 nonkey management (static Wired Equivalent Privacy [WEP]) client disassociates, and it distributes the statically configured WEP key when the first nonkey 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. |

**Command Default** Broadcast key rotation is disabled.

**Command Modes** Interface configuration

### Command History

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

| Release  | Modification   |
|----------|--|
| 12.4(2)T | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

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 Light Extensible Authentication Protocol (LEAP), Extensible Authentication Protocol Transport Layer Security (EAP TLS), or Protected Extensible Authentication Protocol (PEAP), can use the access point.

### Examples

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

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



# channel

To set the radio channel frequency, use the **channel** command in interface configuration mode. To reset the channel frequency to the default value, use the **no** form of this command.

**channel** {*number* | *MHz* | **least-congested**}

**no channel**

## Syntax Description

|                        |  |
|------------------------|--|
| <i>number</i>          | A channel number.<br><br>The valid numbers depend on the channels allowed in your regulatory region and are set during manufacturing.  |
| <i>MHz</i>             | The center frequency, in MHz, for the radio channel.<br><br>The valid frequencies depend on the channels allowed in your regulatory region and are set during manufacturing. |
| <b>least-congested</b> | Enables or disables the scanning for a least busy radio channel to communicate with the client adapter.  |

## Command Default

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

## Command Modes

Interface configuration

## 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.       |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.   |

## Usage Guidelines

For a list of supported channel numbers and center frequencies for the 2.4-GHz and 5-GHz radios, see the Cisco Wireless Router and HWIC Configuration Guide.

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.

## Examples

The following example shows how to set the access point radio to channel 10 with a center frequency of 2457:

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

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

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

This example shows how to reset the frequency to the default setting:

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

## Related Commands

| Command                           | Description   |
|-----------------------------------|---|
| <b>show controller dot11Radio</b> | Displays the radio controller information and status. |

# clear dot11 client

To deauthenticate a radio client with a specified MAC address, use the **clear dot11 client** command in privileged EXEC mode.

**clear dot11 client** *mac-address*

## Syntax Description

|                    |  |
|--------------------|--|
| <i>mac-address</i> | A radio client MAC address (in xxxx.xxxx.xxxx format). |
|--------------------|--|

## Command Modes

Privileged EXEC

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

To deactivate a radio client, the client must be directly associated with the access point, not a repeater.

## Examples

The following example shows how to deauthenticate a specific radio client:

```
Router# clear dot11 client 0040.9645.2196
```

## Related Commands

| Command                        | Description   |
|--------------------------------|---|
| <b>show dot11 associations</b> | Displays the radio association table or radio association statistics. |

# clear dot11 hold-list

To reset the MAC authentication hold list, use the **clear dot11 hold-list** command in privileged EXEC mode.

**clear dot11 hold-list**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows how to clear the hold list of MAC authentications:

```
Router# clear dot11 hold-list
```

## clear dot11 statistics

To reset statistic information for a specific radio interface or a particular client with a specified MAC address, use the **clear dot11 statistics** command in privileged EXEC mode.

**clear dot11 statistics** {**dot11Radio** *interface* | *mac-address*}

### Syntax Description

|                                    |  |
|------------------------------------|--|
| <b>dot11Radio</b> <i>interface</i> | Specifies a radio interface.                     |
| <i>mac-address</i>                 | A client MAC address (in xxxx.xxxx.xxxx format). |

### Command Modes

Privileged EXEC

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Examples

The following example shows how to clear radio statistics for radio interface 0/3/0:

```
Router# clear dot11 statistics dot11Radio 0/3/0
```

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

```
Router# clear dot11 statistics 0040.9631.81cf
```

### Related Commands

| Command                                      | Description                          |
|--|--------------------------------------|
| <b>show interfaces dot11Radio statistics</b> | Displays radio interface statistics. |

# clear radius local-server

To clear the display on the local server or to unblock a locked username, use the **clear radius local-server** command in privileged EXEC mode.

**clear radius local-server** [*statistics*] *user username*

## Syntax Description

|                   |  |
|-------------------|--|
| <b>statistics</b> | Clears the display of statistical information. |
| <b>user</b>       | Unblocks the locked username specified.        |
| <i>username</i>   | Locked username.                               |

## Command Modes

Privileged EXEC

## Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
| 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

## Examples

The following example shows how to unblock the locked username “smith”:

```
Router# clear radius local-server user smith
```

## Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>block count</b>               | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |
| <b>debug radius local-server</b> | Displays the debug information for the local server.   |
| <b>group</b>                     | Enters user group configuration mode and configures shared setting for a user group.                       |
| <b>nas</b>                       | Adds an access point or router to the list of devices that use the local authentication server.            |

| Command                                    | Description  |
|--|--|
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>                 | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>reauthentication time</b>               | Specifies the time after which access points or wireless-aware routers must reauthenticate the members of a group.               |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.   |

# debug dot11

To enable debugging of radio functions, use the **debug dot11** command in privileged EXEC mode. To stop or disable the debug operation, use the **no** form of this command.

**debug dot11** {events| forwarding| mgmt| packets| syslog| virtual-interface}

**no debug dot11** {events| forwarding| mgmt| packets| syslog| virtual-interface}

## Syntax Description

|                          |  |
|--------------------------|--|
| <b>events</b>            | Displays information about all radio-related events.               |
| <b>forwarding</b>        | Displays information about radio-forwarded packets.                |
| <b>mgmt</b>              | Displays information about radio access point management activity. |
| <b>packets</b>           | Displays information about received or transmitted radio packets.  |
| <b>syslog</b>            | Displays information about the radio system log.                   |
| <b>virtual-interface</b> | Displays information about radio virtual interfaces.               |

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC (#)

## Command History

| Release   | Modification  |
|-----------|---|
| 12.2(4)JA | This command was introduced.  |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T.  |
| 12.2SX    | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to display debugging information about radio functions.



## Examples

The following example shows how to enable debugging of all radio-related events:

```
Router# debug dot11 events
```

## Related Commands

| Command                       | Description                                |
|-------------------------------|--|
| <b>debug dot11 aaa</b>        | Enables debugging of dot11 AAA operations. |
| <b>debug dot11 dot11radio</b> | Enables radio debug options.               |

## debug dot11 aaa

To enable debugging of dot11 authentication, authorization, and accounting (AAA) operations, use the **debug dot11 aaac** command in privileged EXEC mode. To disable or stop the debug operation, use the **no** form of this command.

**debug dot11 aaa** {accounting| authenticator {all| dispatcher| mac-authen| process| rxdata| state-machine| txdata}| dispatcher| manager {all| dispatcher| keys| rxdata| state-machine| supplicant| txdata}}

**no debug dot11 aaa** {accounting| authenticator {all| dispatcher| mac-authen| process| rxdata| state-machine| txdata}| dispatcher| manager {all| dispatcher| keys| rxdata| state-machine| supplicant| txdata}}

### Syntax Description

|                      |   |
|----------------------|---|
| <b>accounting</b>    | Provides information about 802.11 AAA accounting packets.   |
| <b>authenticator</b> | <p>Provides information about MAC and Extensible Authentication Protocol (EAP) authentication packets.</p> <p>Use the following options to activate authenticator debugging:</p> <ul style="list-style-type: none"> <li>• all--Activates debugging for all authenticator packets</li> <li>• dispatcher--Activates debugging for authentication request handler packets</li> <li>• mac-authen--Activates debugging for MAC authentication packets</li> <li>• process--Activates debugging for authenticator process packets</li> <li>• rxdata--Activates debugging for EAP over LAN (EAPOL) packets from client devices</li> <li>• state-machine--Activates debugging for authenticator state-machine packets</li> <li>• txdata--Activates debugging for EAPOL packets sent to client devices</li> </ul> |
| <b>dispatcher</b>    | Provides information about 802.11 AAA dispatcher (interface between association and manager) packets.   |

|                |   |
|----------------|---|
| <b>manager</b> | <p>Provides information about the AAA manager. Use these options to activate AAA manager debugging:</p> <ul style="list-style-type: none"> <li>• <b>all</b> --Activates all AAA manager debugging</li> <li>• <b>dispatcher</b> --Activates debug information for AAA manager-authenticator dispatch traffic</li> <li>• <b>keys</b> --Activates debug information for AAA manager key processing</li> <li>• <b>rxdata</b> --Activates debugging for AAA manager packets received from client devices</li> <li>• <b>state-machine</b> --Activates debugging for AAA manager state-machine packets</li> <li>• <b>supplicant</b> --Activates debugging for Light Extensible Authentication Protocol (LEAP) supplicant packets</li> <li>• <b>txdata</b> --Activates debugging for AAA manager packets sent to client devices.</li> </ul> |
|----------------|---|

**Command Default** Debugging is disabled.

**Command Modes** Privileged EXEC (#)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|------------------------|----------------|---|
|                        | 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.  |
|                        | 12.4(2)T       | This command was integrated into Cisco IOS Release 12.4(2)T.  |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines** Use this command to display debugging information about dot11 AAA operations.

**Examples** The following example shows how to activate debugging for 802.11 AAA accounting packets:

```
Router# debug dot11 aaa accounting
```

**Related Commands**

| Command                       | Description                           |
|-------------------------------|---------------------------------------|
| <b>debug dot11</b>            | Enables debugging of radio functions. |
| <b>debug dot11 dot11radio</b> | Enables radio debug options.          |

# debug dot11 dot11radio

To enable radio debug options, use the **debug dot11 dot11radio** command in privileged EXEC mode. To disable debug options, use the **no** form of this command.

**debug dot11 dot11radio interface** {**accept-radio-firmware**| **dfs simulate** [*channel* ]| **monitor** {**ack**| **address**| **beacon**| **crc**| **lines**| **plcp**| **print**| **probe**| **store** }| **print** {**hex**| **if**| **iv**| **lines**| **mic**| **plcp**| **printf**| **raw**| **shortadr** }| **stop-on-failure**| **trace** {**off**| **print**| **store** } }

**no debug dot11 dot11radio interface** {**accept-radio-firmware**| **dfs simulate** [*channel* ]| **monitor** {**ack**| **address**| **beacon**| **crc**| **lines**| **plcp**| **print**| **probe**| **store** }| **print** {**hex**| **if**| **iv**| **lines**| **mic**| **plcp**| **printf**| **raw**| **shortadr** }| **stop-on-failure**| **trace** {**off**| **print**| **store** } }

## Syntax Description

|                              |  |
|------------------------------|--|
| <i>interface</i>             | The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1.   |
| <b>accept-radio-firmware</b> | Configures the access point to disable checking the radio firmware version.  |
| <b>dfs simulate</b>          | Configures the access point to simulate radar generation as part of Dynamic Frequency Selection (DFS).   |
| <i>channel</i>               | (Optional) Radio channel to move to. Range is from 24 to 161.  |
| <b>monitor</b>               | <p>Enables RF monitor mode. Use these options to turn on monitor modes:</p> <ul style="list-style-type: none"> <li>• <b>ack</b> --Displays ACK packets. ACK packets acknowledge receipt of a signal, information, or packet.</li> <li>• <b>address</b> --Displays packets to or from the specified IP address</li> <li>• <b>beacon</b> --Displays beacon packets</li> <li>• <b>crc</b> --Displays packets with CRC errors</li> <li>• <b>lines</b> --Specifies a print line count</li> <li>• <b>plcp</b> --Displays Physical Layer Control Protocol (PLCP) packets</li> <li>• <b>print</b> --Enables RF monitor printing mode</li> <li>• <b>probe</b> --Displays probe packets</li> <li>• <b>store</b> --Enables RF monitor storage mode</li> </ul> |

|                        |  |
|------------------------|--|
| <b>print</b>           | <p>Enables packet printing. Use these options to turn on packet printing:</p> <ul style="list-style-type: none"> <li>• <b>hex</b> --Prints entire packets without formatting</li> <li>• <b>if</b> --Prints the in and out interfaces for packets</li> <li>• <b>iv</b> --Prints the packet Wired Equivalent Privacy (WEP) IV</li> <li>• <b>lines</b> --Prints the line count for the trace</li> <li>• <b>mic</b> --Prints the Cisco Message Integrity Check (MIC)</li> <li>• <b>plcp</b> --Displays the PLCP</li> <li>• <b>printf</b> --Prints using printf instead of buginf</li> <li>• <b>raw</b> --Prints without formatting data</li> <li>• <b>shortadr</b> --Prints MAC addresses in short form</li> </ul> |
| <b>stop-on-failure</b> | Configures the access point to not restart when the radio driver fails.  |
| <b>trace</b>           | <p>Enables trace mode. Use these options to turn on trace modes:</p> <ul style="list-style-type: none"> <li>• <b>off</b> --Turns off traces</li> <li>• <b>print</b> --Enables trace printing</li> <li>• <b>store</b> --Enables trace storage</li> </ul>  |

**Command Default** Debugging is disabled.

**Command Modes** Privileged EXEC (#)

| <b>Command History</b> | <b>Release</b> | <b>Modification</b>   |
|------------------------|----------------|---|
|                        | 12.2(4)JA      | This command was introduced.  |
|                        | 12.4(2)T       | This command was integrated into Cisco IOS Release 12.4(2)T.  |
|                        | 12.2SX         | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

**Usage Guidelines**

Use this command to display debugging information about radio options.

**Examples**

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

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

**Related Commands**

| Command                | Description                                |
|------------------------|--|
| <b>debug dot11</b>     | Enables debugging of radio functions.      |
| <b>debug dot11 aaa</b> | Enables debugging of dot11 AAA operations. |

## debug radius local-server

To control the display of debug messages for the local authentication server, use the **debug radius local-server** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

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

**no debug radius local-server** {client| error| packets}

### Syntax Description

|                |  |
|----------------|--|
| <b>client</b>  | Displays error messages about failed client authentications.           |
| <b>error</b>   | Displays error messages about the local authentication server.         |
| <b>packets</b> | Displays the content of the RADIUS packets that are sent and received. |

### Command Default

No default behavior or values

### Command Modes

Privileged EXEC (#)

### Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on Cisco Aironet Access Point 1200 and Cisco Aironet Access Point 1100.   |
| 12.3(11)T  | This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.                 |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.  |
| 12.2SX     | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

### Usage Guidelines

Use this command to control the display of debug messages for the local authentication server.



## Examples

The following command shows how to display messages regarding failed client authentication:

```
Router# debug radius local-server  
client
```

## Related Commands

| Command                                    | Description  |
|--|--|
| <b>clear radius local-server</b>           | Clears the statistics display or unblocks a user.                        |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.                   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.                     |
| <b>user</b>                                | Authorizes a user to authenticate using the local authentication server. |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.                  |

## dfs band block

To prevent an access point from selecting specific frequencies during Dynamic Frequency Selection (DFS), use the **dfs band block** command in interface configuration mode. To unblock frequencies for DFS, use the **no** form of this command.

**dfs band** *frequency-group* **block**

**no dfs band** *frequency-group* **block**

### Syntax Description

|                        |  |
|------------------------|--|
| <i>frequency-group</i> | The group of frequencies that is blocked from DFS selection. Values for the <i>frequency-group</i> argument are <b>1</b> , <b>2</b> , <b>3</b> , or <b>4</b> . At least one group of frequencies must be specified. Multiple groups are allowed, separated by a space. |
|------------------------|--|

### Command Default

No frequencies are blocked for DFS.

### Command Modes

Interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.4(2)XA | This command was introduced.                                 |
| 12.4(6)T  | This command was integrated into Cisco IOS Release 12.4(6)T. |

### Usage Guidelines

If your regulatory domain limits the channels that you can use in specific locations—for example, indoors or outdoors—use this command to prevent the access point from selecting specific groups of frequencies when DFS is enabled.

At least one group of frequencies must be specified. Multiple groups are allowed.

The *frequency-group* argument can be one or more of the following values:

- 1--Specifies that the block of channels with frequencies 5.150 to 5.250 GHz cannot be used for DFS. This group of frequencies is also known as the UNII-1 band.
- 2--Specifies that the block of channels with frequencies of 5.250 to 5.350 GHz cannot be used for DFS. This group of frequencies is also known as the UNII-2 band.
- 3--Specifies that the block of channels with frequencies of 5.470 to 5.725 GHz cannot be used for DFS.
- 4--Specifies that the block of channels with frequencies of 5.725 to 5.825 GHz cannot be used for DFS. This group of frequencies is also known as the UNII-3 band.

## Examples

The following example shows how to prevent an access point from selecting frequencies 5.150 to 5.350 GHz for DFS:

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

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

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

# distance

To specify the distance from a root bridge to the nonroot bridge or bridges with which it communicates, use the **distance** command in interface configuration mode. To reset the distance to its default value, use the **no** form of this command.

**distance kilometers**

**no distance**

## Syntax Description

|            |   |
|------------|---|
| kilometers | Bridge distance in kilometers (km). Range is 0 to 99. |
|------------|---|

## Command Default

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

Interface configuration

## Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced.                                  |
| 12.4(15)T  | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

This command is used to optimize the radio frequency (RF) propagation distance. It is available only when the role of the radio interface is set to **root bridge**.

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

## Examples

The following example shows how to configure the distance to 40 km for the root bridge radio:

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

## Related Commands

| Command             | Description                           |
|---------------------|---------------------------------------|
| <b>station-role</b> | Sets the role of the radio interface. |

## dot11 aaa authentication mac-authen filter-cache

To enable message authentication code (MAC) address authentication caching on the access point, use the **dot11 aaa authentication mac-authen filter-cache** command in global configuration mode. To disable the MAC authentication, use the **no** form of this command.

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

**no dot11 aaa authentication mac-authen filter-cache**

### Syntax Description

|                               |  |
|-------------------------------|--|
| <b>timeout</b> <i>seconds</i> | (Optional) Specifies a timeout value, in seconds, for MAC authentications in the cache. The range is from 30 to 65555. |
|-------------------------------|--|

### Command Default

MAC authentication caching is disabled by default. When you enable it, the default timeout value is 1800 seconds.

### Command Modes

Global configuration (config)

### Command History

| Release  | Modification  |
|----------|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

### Usage Guidelines

MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to the authentication server. When a client device completes MAC authentication on the authentication server, the access point adds the client's MAC address to the cache.

### Examples

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

```
Router# configure terminal
Router(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
```

### Related Commands

| Command   | Description   |
|---|---|
| <b>clear dot11 aaa authentication mac-authen filter-cache</b> | Clears MAC addresses from the MAC authentication cache. |

| Command  | Description   |
|--|---|
| <b>show dot11 aaa authentication mac-authen filter-cache</b> | Displays MAC addresses in the MAC authentication cache. |

## dot11 aaa dot1x compliance

To authenticate, authorize, and account for 802.1x draft10 compliance of IEEE 802.11 configuration commands, use the **dot11 aaa dot1x compliance** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**dot11 aaa dot1x compliance draft10**

**no dot11 aaa dot1x compliance**

### Syntax Description

|                |   |
|----------------|---|
| <b>draft10</b> | Specifies the draft10, 2001 compliant requirement for IEEE 802.11 configuration commands. |
|----------------|---|

### Command Default

The AAA conditions for IEEE 802.11 configuration commands are not configured.

### Command Modes

Global configuration (config)

### Command History

| Release  | Modification  |
|----------|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

### Examples

The following example shows how to authenticate, authorize, and account for 802.1x draft10 compliance of IEEE 802.11 configuration commands:

```
Router(config)# dot11 aaa dot1x compliance draft10
```

### Related Commands

| Command              | Description   |
|----------------------|---|
| <b>dot1x default</b> | Resets the global 802.1x authentication parameters to their default values as specified in the latest IEEE 802.1x standard. |

## dot11 aaa csid

To set the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets, use the **dot11 aaa csid** command in global configuration mode. To reset the MAC address format to the default value, use the **no** form of this command.

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

**no 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:<br><br>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:<br><br>00-07-85-b3-5f-4a |
| unformatted | Specifies no formatting for MAC addresses in CSID attributes. An unformatted MAC address looks like this example:<br><br>000785b35f4a                               |

### Command Default

The default CSID format looks like the following example:

0007.85b3.5f4a

### Command Modes

Global configuration

### Command History

| Release    | Modification   |
|------------|--|
| 12.2(13)JA | This command was introduced.                                 |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

Use this command to set the format for MAC addresses in Called-Station-ID and Calling-Station-ID attributes in RADIUS packets.



## Examples

The following example shows how to specify the IETF format for MAC addresses in CSID attributes:

```
Router(config)# dot11 aaa csid ietf
```

## Related Commands

| Command                | Description                                |
|------------------------|--|
| <b>debug dot11 aaa</b> | Enables debugging of dot11 AAA operations. |

## dot11 activity-timeout

To set the number of seconds that the access point tracks an inactive device, use the **dot11 activity-timeout** command in global configuration mode. To reset the activity timeout for a device to the default value, use the **no** form of this command.

**dot11 activity-timeout** {**bridge** {**default** *seconds*| **maximum** *seconds*}| **client-station** {**default** *seconds*| **maximum** *seconds*}| **default** *seconds*| **maximum** *seconds*| **repeater** {**default** *seconds*| **maximum** *seconds*}| **unknown** {**default** *seconds*| **maximum** *seconds*}| **workgroup-bridge** {**default** *seconds*| **maximum** *seconds*}}

**no dot11 activity-timeout** {**bridge** {**default** *seconds*| **maximum** *seconds*}| **client-station** {**default** *seconds*| **maximum** *seconds*}| **default** *seconds*| **maximum** *seconds*| **repeater** {**default** *seconds*| **maximum** *seconds*}| **unknown** {**default** *seconds*| **maximum** *seconds*}| **workgroup-bridge** {**default** *seconds*| **maximum** *seconds*}}

### Syntax Description

|                        |   |
|------------------------|---|
| bridge                 | Specifies a bridge.   |
| client-station         | Specifies a client station.   |
| default <i>seconds</i> | Specifies the default activity timeout, in seconds, that the access point uses when a device associates and proposes a zero-refresh rate or does not propose a refresh rate. The <i>seconds</i> argument is a value from 1 to 100000. |
| maximum <i>seconds</i> | Specifies the maximum activity timeout, in seconds, allowed for a device regardless of the refresh rate proposed by a device when it associates. The <i>seconds</i> argument is a value from 1 to 100000.                             |
| repeater               | Specifies a repeater.   |
| unknown                | Specifies unknown (non-Cisco Aironet) device class.   |
| workgroup-bridge       | Specifies a workgroup bridge.   |

### Command Default

The table below lists the default activity timeouts for each device class. All values are in seconds.

**Table 1: Default Activity Timeouts**

| Device Class   | Default Timeout |
|----------------|-----------------|
| bridge         | 28800           |
| client-station | 1800            |
| repeater       | 28800           |

| Device Class     | Default Timeout |
|------------------|-----------------|
| workgroup-bridge | 28800           |
| unknown          | 60              |

**Command Modes** Global configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.2(13)JA | This command was introduced.                                 |
|                 | 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Usage Guidelines** The default and maximum activity timeout values can be configured with one command, however, the default timeout cannot be greater than the maximum timeout. If the default timeout exceeds the maximum timeout, an error message is displayed.

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

The access point applies the unknown device class to all non-Cisco Aironet devices.

**Examples** The following example shows how to configure default and maximum activity timeouts for all device classes:

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

| Related Commands | Command                 | Description  |
|------------------|-------------------------|--|
|                  | <b>debug dot11 aaa</b>  | Enables debugging of dot11 AAA operations.   |
|                  | show dot11 associations | Displays the radio association table, radio association statistics, or association information about wireless devices. |

# dot11 extension aironet

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

**dot11 extension aironet**

**no dot11 extension aironet**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Cisco Aironet extensions are enabled by default.

**Command Modes** Interface configuration

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |
|                 |           |  |

**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 Message Integrity Code (MIC) and key hashing. Disable these extensions for non-Cisco clients that misinterpret the extensions.

**Examples** The following example shows how to enable Cisco Aironet extensions for the radio interface:

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

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

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

## dot11 holdoff-time

To set the hold-off time for Extensible Authentication Protocol (EAP) and MAC address authentication, use the **dot11 holdoff-time** command in global configuration mode. To reset the hold-off time to the default value, use the **no** form of this command.

**dot11 holdoff-time** *seconds*

**no dot11 holdoff-time**

### Syntax Description

|                |  |
|----------------|--|
| <i>seconds</i> | Hold-off time, in seconds. Range is from 1 to 65555. |
|----------------|--|

### Command Default

No hold-off time is set.

### Command Modes

Global configuration

### Command History

| Release    | Modification   |
|------------|--|
| 12.2(13)JA | This command was introduced.                                 |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

The hold-off time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point.

### Examples

The following example shows how specify a 2-minute hold-off time:

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

### Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

## dot11 igmp snooping-helper

To begin sending Internet Group Management Protocol (IGMP) query requests when a new client associates with an access point, use the **dot11 igmp snooping-helper** command in global configuration mode. To disable the IGMP query requests, use the **no** form of this command.

**dot11 igmp snooping-helper**

**no dot11 igmp snooping-helper**

**Syntax Description** This command has no arguments or keywords.

**Command Default** IGMP query requests are disabled.

**Command Modes** Global configuration (config)

| Command History | Release  | Modification  |
|-----------------|----------|---|
|                 | 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

**Examples** The following example shows how to enable IGMP query requests:

```
Router# configure terminal
Router(config)# dot11 igmp snooping-helper
```

| Related Commands | Command                 | Description  |
|------------------|-------------------------|--|
|                  | show dot11 associations | Displays the radio association table and radio association statistics. |

## dot11 location isocc

To configure the location identifiers that an access point includes in RADIUS authentication and accounting requests, use the **dot11 location isocc** command in global configuration mode. To remove the location identifiers in the accounting requests, use the **no** form of this command.

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

**no dot11 location isocc**

### Syntax Description

|                                      |   |
|--------------------------------------|---|
| <b>isocc</b> <i>ISO-country-code</i> | Specifies the ISO country code that the access point includes in RADIUS authentication and accounting requests.   |
| <b>cc</b> <i>country-code</i>        | Specifies the International Telecommunication Union (ITU) country code that the access point includes in RADIUS authentication and accounting requests. |
| <b>ac</b> <i>area-code</i>           | Specifies the ITU area code that the access point includes in RADIUS authentication and accounting requests.  |

### Command Default

The ISO and ITU location codes on the access point are not configured.

### Command Modes

Global configuration (config)

### Command History

| Release  | Modification  |
|----------|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

### 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 the **dot11 location isocc** command.

### Examples

The following example shows how to configure the ISO and ITU location codes and the area code on the access point:

```
Router# configure terminal
Router(config)# dot11 location isocc us cc 1 ac 408
```

**Related Commands**

| Command                     | Description  |
|-----------------------------|--|
| <b>snmp-server location</b> | Specifies the SNMP system location and the WISP location-name attribute. |



# dot11 mbssid

To enable multiple Basic Service Set Identifiers (SSIDs) on all access point radio interfaces, use the `dot11 mbssid` command in global configuration mode.

**dot11 mbssid**

**no dot11 mbssid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No multiple basic SSIDs are enabled.

**Command Modes** Global configuration

| Command History | Release   | Modification  |
|-----------------|-----------|---|
|                 | 12.3(4)JA | This command was introduced.                                  |
|                 | 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

**Usage Guidelines** 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 display includes this line:

Number of supported simultaneous BSSID on radio-interface: 8

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

```
Router(config)# dot11 mbssid
```

| Related Commands | Command          | Description  |
|------------------|------------------|--|
|                  | mbssid           | Enables multiple basic SSIDs on an access point radio interface. |
|                  | show dot11 bssid | Displays configured basic SSIDs.                                 |

# dot11 phone

To enable IEEE 802.11 compliance phone support, use the **dot11 phone** command in global configuration mode. To disable the IEEE 802.11 phone, use the **no** form of this command.

**dot11 phone**

**no dot11 phone**

**Syntax Description** This command has no arguments or keywords.

**Command Default** IEEE 802.11 compliance phone support is disabled.

**Command Modes** Global configuration

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**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** The following example shows how to enable IEEE 802.11 phone support:

```
Router(config)# dot11 phone
```

## dot11 priority-map avvid

To enable Cisco Architecture for Voice, Video, and Integrated Data (AVVID) priority mapping, use the **dot11 priority-map avvid** command in global configuration mode. To disable AVVID priority mapping, use the **no** form of this command.

**dot11 priority-map avvid**

**no dot11 priority-map avvid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** AVVID priority mapping is enabled.

**Command Modes** Global configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.2(13)JA | This command was introduced.                                 |
|                 | 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |
|                 |            |  |

**Usage Guidelines** 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.

This command is not supported on bridges.

**Examples** The following example shows how to stop or disable AVVID priority mapping:

Router(config)# **no dot11 priority-map avvid**

| Related Commands | Command          | Description  |
|------------------|------------------|--|
|                  | <b>class-map</b> | Creates a class map to be used for matching packets to the class whose name you specify. |

## dot11 qos class

To configure quality of service (QoS) class parameters for a radio interface, use the `dot11 qos class` command in interface configuration mode. To disable the QoS parameters, use the `no` form of this command.

**dot11 qos class** {background| best-effort| video| voice} [both] [cell] [local]

**no dot11 qos class** {background| best-effort| video| voice}

### Syntax Description

|             |   |
|-------------|---|
| background  | Specifies the QoS traffic is a background process.                |
| best-effort | Specifies the QoS traffic is a best-effort process.               |
| video       | Specifies the QoS traffic is video data.                          |
| voice       | Specifies the QoS traffic is voice data.                          |
| both        | (Optional) Specifies the QoS parameters for local and radio use.  |
| cell        | (Optional) Specifies the QoS parameters apply to the radio cells. |
| local       | (Optional) Specifies the QoS parameters are for local use only.   |

### Command Default

QoS class parameters are disabled.

### Command Modes

Interface configuration mode

### Command History

| Release   | Modification  |
|-----------|---|
| 12.3(8)JA | This command was introduced.                                  |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

### Usage Guidelines

This command is not supported when the access point is operating in repeater mode.

## Examples

This example shows how to specify video traffic support on radio cells:

```
Router(config)# interface dot11radio 0/0/1  
Router(config-if)# dot11 qos class video cell
```

This example shows how to disable video traffic support on radio cells:

```
Router(config-if)# no dot11 qos class video
```

## Related Commands

| Command            | Description           |
|--------------------|-----------------------|
| dot11 qos mode wmm | Enables WMM elements. |

## dot11 qos mode wmm

To enable Wi-Fi Multimedia (WMM) mode, use the `dot11 qos mode wmm` command in interface configuration mode. To disable WMM mode, use the `no` form of this command.

**dot11 qos mode wmm**

**no dot11 qos mode wmm**

**Syntax Description** This command has no arguments or keywords.

**Command Default** WMM mode is enabled by default.

**Command Modes** Interface configuration

| Command History | Release   | Modification  |
|-----------------|-----------|---|
|                 | 12.3(8)JA | This command was introduced.                                  |
|                 | 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |
|                 |           |   |

**Usage Guidelines** When you enable quality of service (QoS), the access point uses WMM mode by default. WMM is designed to improve the user experience for audio, video, and voice applications over a Wi-Fi wireless connection.

**Examples** This example shows how to disable WMM:

```
Router(config)# interface dot11radio 0/0/1
Router(config-if)# no dot11 qos mode wmm
```

| Related Commands | Command         | Description  |
|------------------|-----------------|--|
|                  | dot11 qos class | Configures QoS class parameters for the radio interface. |

# dot11 ssid

To create a global SSID, use the dot11 ssid command in global configuration mode.

**dot11 ssid name**

## Syntax Description

|             |   |
|-------------|---|
| <i>name</i> | The SSID name for the radio, expressed as a case-sensitive alphanumeric string up to 32 characters in length. |
|-------------|---|

## Command Default

No global SSID is enabled.

## Command Modes

Global configuration

## Command History

| Release   | Modification  |
|-----------|---|
| 12.3(2)JA | This command was introduced.                                  |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

The SSID is inactive until you use the ssid command in interface configuration mode to assign the SSID to a specific radio interface.

## 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

```
Router# configure terminal
Router(config)# dot11 ssid sample
Router(config-ssid)# accounting accounting-method-list
Router(config-ssid)# max-associations 15
Router(config-ssid)# vlan 3762
Router(config-ssid)# exit
Router(config)# interface dot11radio 0/0/1
Router(config-if)# ssid sample
```

Related Commands

| Command | Description  |
|---------|--|
| ssid    | Creates an SSID in configuration interface mode or assigns a globally configured SSID to a specific radio interface. |



# dot11 syslog

To enable IEEE 802.11 syslog, use the **dot11 syslog** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**dot11 syslog**

**no dot11 syslog**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Syslog is enabled.

**Command Modes** Global configuration (config)

| Command History | Release  | Modification  |
|-----------------|----------|---|
|                 | 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |

**Examples** The following example shows how to enable IEEE 802.11 syslog:

```
Router# configure terminal
Router(config)# dot11 syslog
```

| Related Commands | Command                       | Description  |
|------------------|-------------------------------|--|
|                  | <b>clear dot11 statistics</b> | Resets statistic information for a specific radio interface or a particular client with a specified MAC address. |
|                  | <b>debug dot11</b>            | Enables debugging of radio functions.  |

## dot11 vlan-name

To assign a name to a VLAN in addition to its numerical ID, use the `dot11 vlan-name` command in global configuration mode. To remove a name from a VLAN, use the `no` form of this command.

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

**no dot11 vlan-name name vlan vlan-id**

### Syntax Description

|                |  |
|----------------|--|
| <b>name</b>    | Name to assign to a VLAN ID. The name can contain up to 32 ASCII characters. |
| <b>vlan-id</b> | VLAN ID to which the name is assigned. Range is from 1 to 4095.              |

### Command Default

No VLAN name is assigned.

### Command Modes

Global configuration

### Command History

| Release   | Modification  |
|-----------|---|
| 12.3(2)JA | This command was introduced.                                  |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

### Usage Guidelines

Remember these guidelines 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 from 1 to 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.

**Note**

In Cisco IOS 12.4(15)T Release, the VLAN name overwrites the VLAN ID, which means that when you configure an SSID or configure encryption you will use the VLAN name and not the VLAN ID.

**Examples**

The following example shows how to assign a name to a VLAN:

```
Router(config)# dot11 vlan-name vlan1 vlan 121
```

**Related Commands**

| Command                     | Description   |
|-----------------------------|---|
| <b>show dot11 vlan-name</b> | Displays VLAN name and ID pairs configured on the access point. |

## dot1x client-timeout

To configure the IEEE 802.1x (dot1x) client timeout value, use the **dot1x client-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**dot1x client-timeout** *seconds*

**no dot1x client-timeout**

### Syntax Description

|                |  |
|----------------|--|
| <i>seconds</i> | A number of seconds for the client timeout. Range is from 1 to 65555. Default is 30. |
|----------------|--|

### Command Default

The default client timeout is 30 seconds.

### Command Modes

Interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

The client timeout value is the length of time, in seconds, the access point waits for a reply from a client attempting to authenticate before the authentication fails.

### Examples

The following example shows how to configure a 60-second dot1x client timeout value:

```
Router(config-if)# dot1x client-timeout 60
```

## dot1x reauth-period

To configure the interval that the access point waits before forcing an authenticated client to reauthenticate, use the **dot1x reauth-period** command in interface configuration mode. To disable reauthentication, use the **no dot1x reauth-period** command.

**dot1x reauth-period** {*seconds*| **server**}

**no dot1x reauth-period**

### Syntax Description

|                |  |
|----------------|--|
| <i>seconds</i> | The number of seconds for the reauthentication period. Range is from 1 to 65555. |
| <b>server</b>  | Specifies the reauthentication period configured on authentication server.       |

### Command Default

Reauthentication is disabled.

### Command Modes

Interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

If you use the **server** 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 Extensible Authentication Protocol (EAP) authentication.

If you configure both MAC address authentication and EAP authentication for a service set identifier (SSID), the server sends the Session-Timeout attribute for both MAC and EAP authentications for a client device. The access point uses the Session-Timeout attribute for the last authentication that the client performs. For example, if a client performs MAC address authentication and then performs EAP authentication, the access point uses the server's Session-Timeout value for the EAP authentication. To avoid confusion on which Session-Timeout attribute is used, configure the same Session-Timeout value on your authentication server for both MAC and EAP authentication.

## Examples

The following example shows how to configure a 2-minute dot1x client-reauthentication period:

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

## Related Commands

| Command                           | Description                        |
|-----------------------------------|------------------------------------|
| <b>show interfaces dot11Radio</b> | Displays radio AAA timeout values. |

## encryption key

To define a Wired Equivalent Privacy (WEP) key used for data encryption on the wireless LAN or on a specific VLAN, use the **encryption key** command in interface configuration mode. To remove a specific encryption key, use the no form of this command.

**encryption** [vlan vlan-id] key number size {40bit| 128bit} [0| 7] *encryption-key* [transmit-key]

**no encryption** [vlan vlan-id] key number size {40bit| 128bit} [0| 7] *encryption-key* [transmit-key]

### Syntax Description

|                       |  |
|-----------------------|--|
| vlan vlan-id          | (Optional) Specifies the VLAN number. Range is from 1 to 4095.   |
| key number            | Specifies the number of the key that is being configured. Range is from 1 to 4.<br><br>A total of four encryption keys can be configured for each VLAN.<br><br><b>Note</b> If you configure static WEP with Message Integrity Code (MIC), 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 the table below 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.  |
| 0                     | (Optional) Specifies an unencrypted key follows.   |
| 7                     | (Optional) Specifies a hidden key follows.   |
| <i>encryption-key</i> | An encryption key. A 40-bit encryption key requires 10 hexadecimal digits. A 128-bit encryption key requires 26 hexadecimal digits.  |
| transmit-key          | (Optional) Specifies the key as the transmit key. Key slot 1 is the default key slot.  |

**Command Default** No WEP key is defined.

**Command Modes** Interface configuration

**Command History**

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Usage Guidelines**

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, such as Wi-Fi Protected Access (WPA) or 802.1x authentication, you do not need to configure static WEP keys.

Using security features such as authenticated key management can limit WEP key configurations.

The table below lists WEP key restrictions based on your security configuration.

**Table 2: WEP Key Restrictions**

| Security Configuration  | WEP Key Restriction  |
|---|--|
| WPA authenticated key management                                      | Cannot configure a WEP key in key slot 1   |
| Light Extensible Authentication Protocol (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 (Temporal Key Integrity Protocol) 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   | 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**

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

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



**Related Commands**

| Command                    | Description                                 |
|----------------------------|---|
| <b>show running-config</b> | Displays current configuration information. |

# encryption mode ciphers

To enable a cipher suite, use the `encryption mode ciphers` command in interface configuration mode. To disable a cipher suite, use the **no** form of this command.

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

**no encryption mode ciphers**

## Syntax Description

|                           |  |
|---------------------------|--|
| <code>vlan vlan-id</code> | (Optional) Specifies a VLAN number or VLAN name. The range for a VLAN number is from 1 to 4095. The VLAN name can be up to 32 ASCII characters in length.  |
| <code>aes-ccm</code>      | Specifies that Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Code Protocol (AES-CCMP) is included in the cipher suite.  |
| <code>tkip</code>         | Specifies that TKIP is included in the cipher suite.<br><b>Note</b> If you enable a cipher suite with two elements, such as Temporal Key Integrity Protocol (TKIP) and 128-bit wired equivalent privacy (WEP), the second cipher becomes the group cipher. |
| <code>wep128</code>       | (Optional) Specifies that 128-bit WEP is included in the cipher suite.   |
| <code>wep40</code>        | (Optional) Specifies that 40-bit WEP is included in the cipher suite.  |

## Command Default

Cipher suites are disabled.

## Command Modes

Interface configuration

## 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.   |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |
| 12.4(15)T  | This command was modified to include support for AES-CCMP.   |

## Usage Guidelines

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).

Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, we recommend that you enable WEP by using the **encryption mode wep** command. Cipher suites that contain Temporal Key Integrity Protocol (TKIP) provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

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

AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

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

**Table 3: Cipher Suites Compatible with WPA and CCKM**

| Authenticated Key Management Types | Compatible Cipher Suites   |
|------------------------------------|--|
| CCKM                               | <ul style="list-style-type: none"> <li>• encryption mode ciphers wep128</li> <li>• encryption mode ciphers wep40</li> <li>• encryption mode ciphers ckip</li> <li>• encryption mode ciphers cmic</li> <li>• encryption mode ciphers ckip-cmic</li> <li>• encryption mode ciphers tkip</li> <li>• encryption mode ciphers tkip wep128</li> <li>• encryption mode ciphers tkip wep40</li> </ul>  |
| WPA                                | <ul style="list-style-type: none"> <li>• encryption mode ciphers aes-ccm</li> <li>• encryption mode ciphers aes-ccm wep128</li> <li>• encryption mode ciphers aes-ccm wep40</li> <li>• encryption mode ciphers aes-ccm tkip</li> <li>• encryption mode ciphers aes-ccm tkip wep128</li> <li>• encryption mode ciphers aes-ccm tkip wep40</li> <li>• encryption mode ciphers tkip</li> <li>• encryption mode ciphers tkip wep128</li> <li>• encryption mode ciphers tkip wep40</li> </ul> |

**Note**

When you configure AES-CCM-only, TKIP-only, or AES-CCM + TKIP cipher TKIP encryption (not including any WEP 40 or WEP 128) on a radio interface or VLAN, every SSID on that radio or VLAN must be set to use the WPA key management. If you configure AES-CCM or TKIP on a radio or VLAN but do not configure key management on the SSIDs, client authentication fails on the SSIDs.

**Note**

CCKM is not supported in this release.

**Examples**

The following example shows how to configure a cipher suite for VLAN 22 that enables TKIP and 40-bit WEP:

```
Router(config-if)# encryption vlan 22 mode ciphers tkip wep40
```

**Related Commands**

| Command                                  | Description   |
|--|---|
| <b>encryption mode wep</b>               | Configures the access point for WEP encryption.                                   |
| authentication mode (SSID configuration) | Configures a radio interface for a specified SSID to support open authentication. |

## encryption mode wep

To enable a specific encryption type that is used to communicate on the wireless LAN (WLAN) or a specific VLAN, use the **encryption mode wep** command in interface configuration mode. To disable encryption features, use the no form of this command.

**encryption** [vlan vlan-id] mode wep {mandatory| optional}

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

### Syntax Description

|              |   |
|--------------|---|
| vlan vlan-id | (Optional) Specifies a VLAN number or VLAN name. The range for a VLAN number is from 1 to 4095. The VLAN name can be up to 32 ASCII characters in length. |
| 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.   |

### Command Default

Encryption features are disabled.

### Command Modes

Interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

When encryption is enabled, all client devices on the wireless LAN or VLAN must support the specified encryption methods to communicate with the access point.

Because cipher suites provide the protection of wired equivalent privacy (WEP) while also allowing use of authenticated key management, we recommend that you enable WEP by using the **encryption mode cyphers** command. Cipher suites that contain Temporal Key Integrity Protocol (TKIP) provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

## Examples

The following example shows how to specify that encryption must be used on VLAN number 1:

```
Router(config-if)# encryption vlan 1 mode wep mandatory
```

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

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

## Related Commands

| Command                        | Description             |
|--------------------------------|-------------------------|
| <b>encryption mode cyphers</b> | Enables a cipher suite. |



## fragment-threshold through wpa-psk

---

- [fragment-threshold](#), page 75
- [guest-mode \(SSID configuration\)](#), page 76
- [information-element ssid](#), page 78
- [infrastructure client](#), page 79
- [infrastructure-ssid](#), page 80
- [interface dot11Radio](#), page 82
- [l2-filter bridge-group-acl](#), page 83
- [match vlan](#), page 84
- [max-associations \(SSID configuration\)](#), page 86
- [mbssid](#), page 87
- [nas](#), page 88
- [packet retries](#), page 90
- [payload-encapsulation](#), page 91
- [power client](#), page 92
- [power local](#), page 94
- [preamble-short](#), page 96
- [radius-server local](#), page 97
- [reauthentication time](#), page 99
- [rts](#), page 101
- [show controllers dot11Radio](#), page 102
- [show dot11 aaa authentication mac-authen filter-cache](#), page 105
- [show dot11 associations](#), page 106
- [show dot11 carrier busy](#), page 109
- [show dot11 statistics client-traffic](#), page 111

- [show dot11 statistics interface](#), page 112
- [show dot11 vlan-name](#), page 115
- [show interfaces dot11Radio](#), page 116
- [show interfaces dot11Radio aaa timeout](#), page 118
- [show interfaces dot11Radio statistics](#), page 119
- [show platform software infrastructure lsmpi](#), page 121
- [show radius local-server statistics](#), page 124
- [speed \(access point radio\)](#), page 126
- [ssid](#), page 129
- [station-role](#), page 131
- [traffic-class](#), page 133
- [user](#), page 135
- [vlan \(SSID configuration\)](#), page 138
- [world-mode](#), page 139
- [wpa-psk](#), page 141



# fragment-threshold

To set the size at which packets are fragmented, use the **fragment-threshold** command in interface configuration mode. To reset the threshold to the default value, use the no form of this command.

**fragment-threshold** *bytes*

**no fragment-threshold**

## Syntax Description

|              |   |
|--------------|---|
| <b>bytes</b> | Specifies the packet fragment threshold size. Range is from 256 to 2346 bytes. Default is 2346. |
|--------------|---|

## Command Default

The default threshold size is 2346 bytes.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows how to set the packet fragment threshold size to 1800 bytes:

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

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

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

## guest-mode (SSID configuration)

To configure the radio interface to support guest mode, use the **guest-mode** command in SSID interface configuration mode. To disable the guest mode, use the **no** form of this command.

**guest-mode**

**no guest-mode**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Guest mode is disabled.

**Command Modes** SSID interface configuration

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Usage Guidelines** The access point can have one guest-mode service set identifier (SSID) or none. 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** The following example shows how to set the wireless LAN (WLAN) into guest mode:

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

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

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

### Related Commands

| Command             | Description  |
|---------------------|--|
| show running-config | Displays configuration information.                    |
| <b>ssid</b>         | Specifies the SSID and enters SSID configuration mode. |



# information-element ssid

To designate a Service Set Identifier (SSID) for inclusion in an SSIDL information element (IE) that the access point includes in its beacons, use the **information-element ssidl** command in **SSID configuration mode**.

**information-element ssidl** [advertisement] [wps]

**no information-element ssidl**

## Syntax Description

|               |  |
|---------------|--|
| advertisement | (Optional) Includes the SSID name and capabilities in the access point SSIDL IE. |
| wps           | (Optional) Sets the WPS capability flag in the SSIDL IE.                         |

## Command Default

By default, the access point does not include SSIDL information elements in its beacons.

## Command Modes

SSID configuration

## Command History

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

## Usage Guidelines

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.

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.

## Examples

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

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

## Related Commands

| Command | Description                              |
|---------|--|
| ssid    | Assigns an SSID to a specific interface. |

# infrastructure client

To enable a virtual interface for a workgroup bridge client, use the **infrastructure client** command in interface configuration mode. To disable the workgroup bridge client virtual interface, use the **no** form of this command.

**infrastructure client**

**no infrastructure client**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The `infrastructure client` feature is disabled.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

Enable the infrastructure client feature to increase the reliability of multicast messages to workgroup bridges. When this feature is enabled, the access point sends directed packets containing the multicasts, which are retried if necessary, to the associated workgroup bridge.

Enable this feature only when necessary because it can greatly increase the load on the radio cell.

## Examples

The following example shows how to configure a virtual interface for a workgroup bridge client:

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

# infrastructure-ssid

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

**infrastructure-ssid [optional]**

**no infrastructure-ssid**

## Syntax Description

|                 |  |
|-----------------|--|
| <b>optional</b> | (Optional) Specifies that both infrastructure and mobile client devices are allowed to associate using the SSID. |
|-----------------|--|

## Command Default

No SSID is reserved for infrastructure associations on the WLAN.

## Command Modes

SSID interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

Use this command to control 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 nonroot bridge to associate using the infrastructure SSID. Repeater access points and nonroot 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

The following example shows how to reserve the specified SSID for infrastructure associations on the wireless LAN:

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

This example shows how to restore the SSID to noninfrastructure associations:

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

**Related Commands**

| Command | Description  |
|---------|--|
| ssid    | Specifies the SSID and enters the SSID configuration mode. |

# interface dot11Radio

To enter interface configuration mode for the radio interface, use the **interface dot11Radio** command in global configuration mode. To exit radio interface configuration mode, use the **no** form of this command.

**interface dot11Radio** *interface*

**no interface dot11Radio**

## Syntax Description

|                  |  |
|------------------|--|
| <i>interface</i> | The radio interface. The 2.4-GHz 802.11b/g radio port is 0. The 5-GHz 802.11a radio port is 1. Default is 0. |
|------------------|--|

## Command Default

The default radio port is 0.

## Command Modes

Global configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows how to place the access point in radio configuration mode:

```
Router(config)# interface dot11Radio 0/3/0
```



## l2-filter bridge-group-acl

To apply a Layer 2 access control list (ACL) filter to bridge group incoming and outgoing packets between the access point and the host (upper layer), use the **l2-filter bridge-group-acl** command in interface configuration mode. To disable the Layer 2 ACL filter, use the **no** form of this command.

**l2-filter bridge-group-acl**

**no l2-filter bridge-group-acl**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No Layer 2 ACL filter is applied.

**Command Modes** Interface configuration

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |
|                 |           |  |

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

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

## match vlan

To define the VLAN match criteria, use the `match vlan` command in class-map configuration or policy inline configuration mode. To remove the match criteria, use the **no** form of this command.

**match vlan** {*vlan-id*| *vlan-range*| *vlan-combination*}

**no match vlan**

### Syntax Description

|                         |  |
|-------------------------|--|
| <i>vlan-id</i>          | The VLAN identification number. Valid range is from 1 to 4094; do not enter leading zeros. |
| <i>vlan-range</i>       | A VLAN range. For example, 1 - 3.  |
| <i>vlan-combination</i> | A combination of VLANs. For example, 1 - 3 5 - 7.  |

### Command Default

No match criterion is configured.

### Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

### Command History

| Release    | Modification   |
|------------|--|
| 12.2(4)JA  | This command was introduced.   |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.   |
| 15.1(3)T   | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.   |

### Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

Use the **match vlan** command 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 the Ether Type/Len field are supported.

#### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **service-policy type performance-monitor inline** command.

## Examples

The following example uses the VLAN ID as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)# match vlan 2
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a VLAN ID of 2 will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match vlan 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command  | Description   |
|--|---|
| <b>class-map</b>                               | Creates a class map to be used for matching packets to a specified class. |
| <b>service-policy type performance-monitor</b> | Associates a Performance Monitor policy with an interface.                |

## max-associations (SSID configuration)

To configure the maximum number of associations supported by the radio interface, use the **max-associations** command in SSID interface configuration mode. To reset the parameter to the default value, use the no form of this command.

**max-associations limit**

**no max-associations**

### Syntax Description

|       |   |
|-------|---|
| limit | Specifies the maximum number of associations supported. Range is from 1 to 255. Default is 255. |
|-------|---|

### Command Default

This default number of supported associations is 255.

### Command Modes

SSID interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Examples

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

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

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

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

### Related Commands

| Command | Description  |
|---------|--|
| ssid    | Specifies the SSID and enters SSID configuration mode. |

# mbssid

To enable multiple basic Service Set Identifiers (SSIDs) on an access point radio interface, use the **mbssid** command in interface configuration mode. To disable the multiple basic SSIDs, use the **no** form of this command.

**mbssid**

**no mbssid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Multiple basic SSIDs are disabled on the access point.

**Command Modes** Interface configuration

| Command History | Release   | Modification  |
|-----------------|-----------|---|
|                 | 12.3(4)JA | This command was introduced.                                  |
|                 | 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |
|                 |           |   |

**Usage Guidelines** 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 display includes the following line:

Number of supported simultaneous BSSID on radio-interface: 8

**Examples** This example shows how to include a basic SSID in the beacon:

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

| Related Commands | Command      | Description  |
|------------------|--------------|--|
|                  | dot11 mbssid | Enables BSSIDs on all radio interfaces that support multiple BSSIDs. |

## nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas** command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command.

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

**no nas** *ip-address* **key** *shared-key*

### Syntax Description

|                   |  |
|-------------------|--|
| <i>ip-address</i> | IP address of the access point or router.  |
| <b>key</b>        | Specifies a key.   |
| <i>shared-key</i> | Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator. |

### Command Default

No default behavior or values

### Command Modes

Local RADIUS server configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
| 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

### Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key named shared256.

```
Router(config-radsrv) # nas 192.168.12.17 key shared256
```

### Related Commands

| Command            | Description  |
|--------------------|--|
| <b>block count</b> | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |

| Command                                    | Description  |
|--|--|
| <b>clear radius local-server</b>           | Clears the statistics display or unblocks a user.  |
| <b>debug radius local-server</b>           | Displays the debug information for the local server.   |
| <b>group</b>                               | Enters user group configuration mode and configures shared setting for a user group.   |
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>                 | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>reauthentication time</b>               | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.  |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.   |
| <b>user</b>                                | Authorizes a user to authenticate using the local authentication server.   |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.  |

# packet retries

To specify the maximum number of attempts to send a packet, use the **packet retries** command in interface configuration mode. To reset the parameter to the default value, use the no form of this command.

**packet retries** *number*

**no packet retries**

## Syntax Description

|        |   |
|--------|---|
| number | Specifies the maximum number of attempts to send a packet. Range is from 1 to 128. Default is 32. |
|--------|---|

## Command Default

The default number of retries is 32.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows how to specify 15 as the maximum number of retries:

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

This example shows how reset the packet retries to the default value:

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |



# payload-encapsulation

To specify the Ethernet encapsulation type used to format Ethernet data packets that are not formatted using IEEE 802.3 headers, use the **payload-encapsulation** command in interface configuration mode. To reset the parameter to the default value, use the no form of this command.

**payload-encapsulation** {**rfc1042**|**dot1h**}

**no payload-encapsulation**

## Syntax Description

|                |   |
|----------------|---|
| <b>rfc1042</b> | Specifies the RFC1042 SNAP encapsulation. |
| <b>dot1h</b>   | Specifies the IEEE 802.1H encapsulation.  |

## Command Default

The default payload encapsulation is **rfc1042** (SNAP).

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

Data packets that are not IEEE 802.3 packets must be reformatted using IEEE 802.1H or RFC1042 encapsulation.

## Examples

The following example shows how to specify the use of IEEE 802.1H encapsulation:

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

This example shows how to reset the parameter to the default value:

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

# power client

To configure the maximum power level that clients should use for IEEE 802.11b/g/a radio transmissions to the access point, use the **power client** command in interface configuration mode. To use the default value of no specified power level, use the **no** form of this command.

**power client** {*milliwatt*| **maximum**}

**no power client**

## Syntax Description

|                  |  |
|------------------|--|
| <i>milliwatt</i> | Power level in milliwatts (mW). For the 802.11a radio, value can be 4, 7, 10, 13, or 16. For the 802.11b/g radio, value can be 7, 10, 13, 15, 17, or 20. |
| <b>maximum</b>   | Specifies the maximum power level.   |

## Command Default

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

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Usage Guidelines

Use the **power client** command to specify the desired transmitter power level for clients. The power setting is transmitted to the client device during association with the access point. 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. Maximum transmit power is regulated by the regulatory agency in the country of operation and is set during manufacture of the access point and client device.

## Examples

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

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

This example shows how to disable power level requests:

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

**Related Commands**

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

# power local

To configure the access point radio power level, use the **powerlocal** command in interface configuration mode. To use the default value of maximum power, use the no form of this command.

## 2.4-GHz Access Point Radio (802.11b/g)

**power local** {cck| ofdm} {milliwatt| maximum}

**no power local**

## 5-GHz Access Point Radio (802.11a)

**power local** {milliwatt| maximum}

**no power local**

### Syntax Description

|                  |  |
|------------------|--|
| <b>cck</b>       | Sets Complimentary Code Keying (CCK) power levels.   |
| <b>ofdm</b>      | Sets Orthogonal Frequency Division Multiplexing (OFDM) power levels.   |
| <i>milliwatt</i> | Power level in milliwatts (mW). For the 802.11b/g radio, value can be 7, 10, 13, 15, 17, or 20. For the 802.11a radio, value can be 4, 7, 10, 13, or 16. |
| <b>maximum</b>   | Specifies the maximum power level.   |

### Command Default

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

### Command Modes

Interface configuration

### 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.  |

| Release  | Modification   |
|----------|--|
| 12.4(2)T | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

Use the **power local** command to specify the local transmit power level. Lower power levels reduce the radio cell size and interference between cells. Maximum transmit power is limited depending on your regulatory domain.

On the 2.4-GHz, 802.11b/g radio, you can set CCK and OFDM power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices.

### Examples

This example shows how to specify a 20-mW transmit power level for one of the 802.11b access point radios:

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

### Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

# preamble-short

To enable short radio preambles, use the **preamble-short** command in interface configuration mode. To restore the default value, use the no form of this command.

**preamble-short**

**no preamble-short**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The default is long preambles.

**Command Modes** Interface configuration

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |
|                 |           |  |

**Usage Guidelines** 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.

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.

This command is not supported on the 5-GHz access point radio interface.

**Examples** The following example shows how to set the radio packet to use a short preamble:

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

This example shows how to set the radio packet to use long preambles:

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

| Related Commands | Command                    | Description                         |
|------------------|----------------------------|-------------------------------------|
|                  | <b>show running-config</b> | Displays configuration information. |

# radius-server local

To enable the access point or wireless-aware router as a local authentication server and to enter into configuration mode for the authenticator, use the **radius-server local** command in global configuration mode. To remove the local RADIUS server configuration from the router or access point, use the **no** form of this command.

**radius-server local**

**no radius-server local**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values

**Command Modes** Global configuration

| Command History | Release     | Modification  |
|-----------------|-------------|---|
|                 | 12.2(11)JA  | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
|                 | 12.3(11)T   | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |
|                 | 12.2(33)SRA | This command was integrated into Cisco IOS release 12.(33)SRA.  |
|                 | 12.2SX      | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.                                 |

**Examples** The following example shows that the access point is being configured to serve as a local authentication server:

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

**Usage Guidelines** This command is not supported on bridges.

**Related Commands**

| Command                                    | Description   |
|--|---|
| <b>block count</b>                         | Configures the parameters for locking out members of a group to help protect against unauthorized attacks.                      |
| <b>clear radius local-server</b>           | Clears the statistics display or unblocks a user.   |
| <b>debug radius local-server</b>           | Displays the debug information for the local server.  |
| <b>group</b>                               | Enters user group configuration mode and configures shared setting for a user group.  |
| <b>nas</b>                                 | Adds an access point or router to the list of devices that use the local authentication server.                                 |
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.  |
| <b>reauthentication time</b>               | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group. |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.  |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.  |
| <b>user</b>                                | Authorizes a user to authenticate using the local authentication server.  |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.   |



## reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time** command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

**reauthentication time** *seconds*

**no reauthentication time** *seconds*

### Syntax Description

|                |   |
|----------------|---|
| <i>seconds</i> | Number of seconds after which reauthentication occurs. Range is from 1 to 4294967295. Default is 0. |
|----------------|---|

### Command Default

0 seconds, which means group members are not required to reauthenticate.

### Command Modes

Local RADIUS server group configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
| 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

### Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
Router(config-radsrv-group) # reauthentication time 30
```

### Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>block count</b>               | Configures the parameters for locking out members of a group to help protect against unauthorized attacks. |
| <b>clear radius local-server</b> | Clears the statistics display or unblocks a user.  |
| <b>debug radius local-server</b> | Displays the debug information for the local server.   |

| Command                                    | Description  |
|--|--|
| <b>group</b>                               | Enters user group configuration mode and configures shared setting for a user group.   |
| <b>nas</b>                                 | Adds an access point or router to the list of devices that use the local authentication server.                                  |
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>                 | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.   |
| <b>user</b>                                | Authorizes a user to authenticate using the local authentication server.   |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.  |

## rts

To set the Request-To-Send (RTS) threshold and the number of retries, use the **rts** command in interface configuration mode. To reset the parameter to the default value, use the no form of this command.

**rts** {**threshold bytes**| **retries number**}

**no rts** {**threshold bytes**| **retries number**}

### Syntax Description

|                        |  |
|------------------------|--|
| <b>threshold bytes</b> | Specifies the packet size, in bytes, above which the access point negotiates an RTS before sending out the packet. Range is from 0 to 2347. Default is 2312.       |
| <b>retries number</b>  | Specifies the number of times the access point issues an RTS before stopping the attempt to send the packet over the radio. Range is from 1 to 128. Default is 32. |

### Command Default

The default **threshold** is 2312 bytes. The default number of **retries** is 32.

### Command Modes

Interface configuration

### Command History

| Release    | Modification   |
|------------|--|
| 12.2(4)JA  | This command was introduced.                                 |
| 12.2(11)JA | This command was modified to support bridges.                |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Examples

The following example shows how to set the RTS retries count to 50:

```
Router(config-if)# rts retries 50
```

# show controllers dot11Radio

To display radio controller status, use the **show controllers dot11Radio** command in privileged EXEC mode.

**show controllers dot11Radio** *interface*

## Syntax Description

|                  |  |
|------------------|--|
| <i>interface</i> | The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1. |
|------------------|--|

## Command Modes

Privileged EXEC

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows sample radio controller status for a 2.4-GHz radio:

```
Router# show controllers dot11Radio 0/0/0
interface Dot11Radio0/0/0
Radio ATHEROS AR5212, Address 000e.9b92.3280, BBlock version 0.01, Software version 3.00.0
Serial number:
Carrier Set: Americas (US )
Current Frequency: 2417 Mhz Channel 2
Allowed Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6) 2442(7) 2447(8) 2452(9)
2457(10) 2462
Current CCK Power: 20 dBm
Allowed CCK Power Levels: 7 10 13 15 17 20
Current OFDM Power: 17 dBm
Allowed OFDM Power Levels: 7 10 13 15 17
ERP settings: short slot time, protection mechanisms.
Neighbors in non-erp mode:
000e.9ba1.c084 000e.d700.9003 000e.3858.be9a 0012.43be.e4f0 000a.f4e2.3338
Current Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
54.0
Allowed Rates: 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: 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
Default Rates: basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
54.0
Radio Management (RM) Configuration: Mode 1 Temp Setting Disabled
Temp Settings: AP Tx Power 0 AP Tx Channel 0 Client Tx Power 0
Rates:
Perm Settings: AP Tx Power 0 AP Tx Channel 0 Client Tx Power 0
Rates:
Priority 0 cw-min 4 cw-max 10 fixed-slot 6
Priority 1 cw-min 4 cw-max 10 fixed-slot 2
Priority 2 cw-min 3 cw-max 4 fixed-slot 1
Priority 3 cw-min 2 cw-max 3 fixed-slot 1
Transmit queues: Active 0 In Progress 0 Waiting 0
```

|   | Queued |       |     | In Progress |       |           | txed | Statistics |         |  |
|---|--------|-------|-----|-------------|-------|-----------|------|------------|---------|--|
|   | Count  | Quota | Max | Count       | Quota | discarded |      | failed     | retried |  |
| 4 | 0      | 0     | 0   | 0           | 0     | 0         | 0    | 0          | 0       |  |
| 3 | 0      | 0     | 0   | 0           | 1     | 331       | 0    | 0          | 0       |  |
| 2 | 0      | 0     | 0   | 0           | 0     | 0         | 0    | 0          | 0       |  |
| 1 | 0      | 0     | 0   | 0           | 0     | 0         | 0    | 0          | 0       |  |
| 0 | 0      | 0     | 0   | 0           | 0     | 0         | 0    | 0          | 0       |  |

Transmitted beacon: 23629  
 BeaconStuck count: 0  
 Noise Immunity level 0  
 Spur Immunity Level 0  
 Firststep Level 0  
 OFDM Weak Signal Detection ON  
 CCK Weak Signal Threshold low  
 Transmit Queue details:  
 Q\_ONESHOTARM\_SC=0x0 Q\_ONESHOTARM\_CC=0x0 Q\_RDYTIMESHDN=0x0  
 Q\_TXE=0x0, Q\_TXD=0x0  
 Queue Number = 0  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x800 Q\_RDYTIMECFG=0x0  
 Queue Number = 1  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x800 Q\_RDYTIMECFG=0x0  
 Queue Number = 2  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x800 Q\_RDYTIMECFG=0x0  
 Queue Number = 3  
 =====  
 Q\_TXDP=0x7521B20 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x800 Q\_RDYTIMECFG=0x0  
 Desc=0x7521B20  
     FirstDesc=0x7521B20, LastDesc=0x7521B20, nextPtr=0x0, StaleFlag=TRUE  
     thisPhysPtr=0x7521B20 frameLength=36 more=0 destIdx=0  
         antModeXmit=0x0  
     bufferLength=32 dataLeng=0 pak=0x63AB6C24 pktType=0 noAck=0  
     dataFailCnt=4 RTSFailCnt=0, Filtered=0,  
         fifoUnderrun=0  
     excessiveRetries=1 pktTransmitOk=0, txAnt=0,  
         finalTSIdx=3  
     ackSigStrength=33 seqNum=3241, done=1  
 Queue Number = 4  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x800 Q\_RDYTIMECFG=0x0  
 Queue Number = 5  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x0 Q\_RDYTIMECFG=0x0  
 Queue Number = 6  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x0 Q\_RDYTIMECFG=0x0  
 Queue Number = 7  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x0 Q\_RDYTIMECFG=0x0  
 Queue Number = 8  
 =====  
 Q\_TXDP=0x0 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x862 Q\_RDYTIMECFG=0x1015800  
 Queue Number = 9  
 Q\_TXDP=0x7521520 Q\_STS=0x0 Q\_CBRCFG=0x0 Q\_MISC=0x8A2 Q\_RDYTIMECFG=0x0  
 Desc=0x7521520  
     FirstDesc=0x7521520, LastDesc=0x7521520, nextPtr=0x0, StaleFlag=FALSE  
     thisPhysPtr=0x7521520 frameLength=133 more=0 destIdx=0  
         antModeXmit=0x0  
     bufferLength=129 dataLeng=0 pak=0x634A4A90 pktType=3 noAck=1  
     dataFailCnt=0 RTSFailCnt=0, Filtered=0,  
         fifoUnderrun=0  
     excessiveRetries=0 pktTransmitOk=1, txAnt=1,  
         finalTSIdx=0  
     ackSigStrength=26 seqNum=3543, done=1  
 MAC Registers  
 === 0x0008: 0x00000004  
 === 0x000C: 0x0751F560  
 === 0x0010: 0x00000000  
 === 0x0014: 0x00000105  
 === 0x0018: 0x00000000  
 .

```

.
.
QCU Registers
=== 0x0800: 0x00000000
=== 0x0804: 0x00000000
=== 0x0808: 0x00000000
=== 0x080C: 0x07521C20
=== 0x0810: 0x00000000
.
.
.
DCU Registers
=== 0x1000: 0x00000001
=== 0x1004: 0x00000002
=== 0x1008: 0x00000004
=== 0x100C: 0x00000008
=== 0x1010: 0x00000010
.
.
.
PCI Registers
=== 0x4000: 0x00000000
=== 0x4004: 0x00000000
=== 0x4008: 0x00000000
=== 0x400C: 0x00000000
=== 0x4010: 0x00000014
.
.
.
Eeprom Registers
=== 0x6000: 0x00000000
=== 0x6004: 0x00000000
=== 0x6008: 0x00000000
=== 0x600C: 0x00000000
=== 0x6010: 0x00000000
PCU Registers
=== 0x8000: 0x929B0E00
=== 0x8004: 0x18818032
=== 0x8008: 0x929B0E00
=== 0x800C: 0x00008032
=== 0x8010: 0x00000000
.
.
.
BB Registers
=== 0x9800: 0x00000007
=== 0x9804: 0x00000000
=== 0x9808: 0x00000000
=== 0x980C: 0xAD848E19
=== 0x9810: 0x7D28E000
.
.
.
Clients:
Vlan 0 Clients 0 PSP 0
  Keys: Transmit 0, 0-40Bits ,
Log Buffer:

```

**Related Commands**

| Command                                      | Description  |
|--|--|
| <b>show interfaces dot11Radio Statistics</b> | Displays status information for the radio interface. |

# show dot11 aaa authentication mac-authen filter-cache

To display MAC addresses in the MAC authentication cache, use the **show dot11 aaa authentication mac-authen filter-cache** command in privileged EXEC mode.

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

## Syntax Description

|                                   |  |
|-----------------------------------|--|
| <i>mac-address</i>                | (Optional) MAC address (in xxxx.xxxx.xxxx format).                       |
| <b>ap-number</b> <i>ap-number</i> | (Optional) Specifies an access point number. The range is from 1 to 500. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release   | Modification   |
|-----------|--|
| 12.4(22)T | This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T. |

## Examples

The following is sample output from the **show dot11 aaa authentication mac-authen filter-cache** command. The fields are self-explanatory.

```
Router# show dot11 aaa authentication mac-authen filter-cache
Address      Age (min)
192.168.100.200  0
```

## Related Commands

| Command   | Description   |
|---|---|
| <b>clear dot11 aaa authentication mac-authen filter-cache</b> | Clears MAC addresses from the MAC authentication cache. |

## show dot11 associations

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

**show dot11 associations** [**client**| **repeater**| **statistics**| *mac-address* [**ap-number** *ap-number*]| **bss-only**| **all-client**| **cckm-statistics** [**ap-number** *ap-number*]]

### Syntax Description

|                                   |   |
|-----------------------------------|---|
| <b>client</b>                     | (Optional) Displays all client devices associated with the access point.  |
| <b>repeater</b>                   | (Optional) Displays all repeater devices associated with the access point.  |
| <b>statistics</b>                 | (Optional) Displays access point association statistics for the radio interface.  |
| <b>mac-address</b>                | (Optional) MAC address (in xxxx.xxxx.xxxx format).  |
| <b>ap-number</b> <i>ap-number</i> | (Optional) Specifies an access point number. The range is from 1 to 500.  |
| <b>bss-only</b>                   | (Optional) Displays only the basic service set clients that are directly associated with the access point.  |
| <b>all-client</b>                 | (Optional) Displays the status of all clients associated with the access point.   |
| <b>cckm-statistics</b>            | (Optional) Displays fast, secure roaming (Cisco Centralized Key Management [CCKM]) latency statistics measured at the access point for client devices using CCKM. |

### Command Default

When optional arguments and keywords 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. |



| Release  | Modification   |
|----------|--|
| 12.4(2)T | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following is sample output from the **show dot11 associations** command, which shows radio association statistics:

```
Router# show dot11 associations
802.11 Client Stations on Dot11Radio0/0/0:
SSID [80211bg] :
MAC Address      IP address      Device      Name      Parent      State
0002.8aad.dde9 100.100.100.10 350-client  CSCOAMERB28158 self      Assoc
Others: (not related to any ssid)
802.11 Client Stations on Dot11Radio0/0/1:
SSID [80211a] :
MAC Address      IP address      Device      Name      Parent      State
0040.96a5.3baf 100.100.100.19 CB21AG/PI21AG CSCOAMERB28158 self      Assoc
Others: (not related to any ssid)
```

The table below describes the significant fields shown in the display.

**Table 4: show dot11 associations Field Descriptions**

| Field       | Description  |
|-------------|--|
| MAC Address | Specifies the MAC address (in xxxx.xxxx.xxxx format) of a parent access point. |
| IP address  | Specifies the IP address of the parent access point.                           |
| Device      | Displays the device ID.  |
| Name        | Displays the name of the device.   |
| Parent      | Specifies the parent access point.   |

| Field | Description  |
|-------|--|
| State | <p>Displays the state of the device. If the station/wireless client is associated, the following states are displayed:</p> <ul style="list-style-type: none"><li>• EAP-Assoc</li><li>• MAC-Assoc</li><li>• Assoc</li></ul> <p>If the station/wireless client is not associated, the actual states are displayed:</p> <ul style="list-style-type: none"><li>• Auth_notAssoc</li><li>• Wait ReAuth</li><li>• BLOCK</li><li>• IAPP_get</li><li>• AAA_Auth</li><li>• AAA_ReAuth</li><li>• Drv_Add_InProg</li></ul> |

**Related Commands**

| Command                | Description   |
|------------------------|---|
| clear dot11 statistics | Resets the statistics for a specified radio interface or client device. |

# show dot11 carrier busy

To display recent carrier busy test results, use the **show dot11 carrier busy** command in user EXEC or privileged EXEC mode.

**show dot11 carrier busy** [**ap-number** *ap-number*]

## Syntax Description

**ap-number** *ap-number*

(Optional) Specifies an access point number. The range is from 1 to 500.

## Command Default

If no arguments or keywords are specified, carrier test results for all access points are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification                 |
|---------|------------------------------|
| 12.3T   | This command was introduced. |

## Usage Guidelines

Use the **show dot11 carrier busy** 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.

## Examples

The following is the sample output from the **show dot11 carrier busy** command:

```
Router# show dot11 carrier busy
Frequency  Carrier Busy %
-----
5180      0
5200      2
5220     27
5240      5
5260      1
5280      0
5300      3
5320      2
```

The table below describes the significant fields shown in the display.

**Table 5: show dot11 associations Field Descriptions**

| Field     | Description  |
|-----------|--|
| Frequency | Displays the frequency of the radio channel., in mega hertz (MHz). |

| Field        | Description                                       |
|--------------|---|
| Carrier Busy | Display levels of radio activity on each channel. |

**Related Commands**

| Command                   | Description                 |
|---------------------------|-----------------------------|
| <b>dot11 carrier busy</b> | Runs the carrier busy test. |

## show dot11 statistics client-traffic

To display radio client traffic statistics, use the **show dot11 statistics client-traffic** command in privileged EXEC mode.

**show dot11 statistics client-traffic**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Examples** The following example shows sample radio client traffic statistics:

```
Router# show dot11 statistics client-traffic
Clients:
2-0040.96a5.3baf pak in 383 bytes in 26070 pak out 3 bytes out 345
    dup 0 decrypt err 0 mic mismatch 0 mic miss 0
    tx retries 0 data retries 0 rts retries 0
    signal strength 58 signal quality N/A
Clients:
4-0002.8aad.dde9 pak in 18 bytes in 2119 pak out 3 bytes out 601
    dup 0 decrypt err 0 mic mismatch 0 mic miss 0
    tx retries 0 data retries 0 rts retries 0
    signal strength 26 signal quality N/A
```

| Related Commands | Command                       | Description   |
|------------------|-------------------------------|---|
|                  | <b>clear dot11 statistics</b> | Resets the statistics for a specified radio interface or client device. |

# show dot11 statistics interface

To display statistics for all dot11Radio interfaces, use the **show dot11 statistics interface** command in privileged EXEC mode.

## show dot11 statistics interface

**Syntax Description** This command has no arguments or keywords.

**Command Default** Statistics for all dot11Radio interfaces are displayed.

**Command Modes** Privileged EXEC

| Command History | Release   | Modification   |
|-----------------|-----------|--|
|                 | 12.2(4)JA | This command was introduced.                                 |
|                 | 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Examples** The following example shows sample statistics for all dot11Radio interfaces:

```
Router# show dot11 statistics interface
Interface Dot11Radio0/0/0 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx Bytes:      37361230 / 53211    Host Tx Bytes:      3607499 / 5221
Unicasts Rx:        586 / 1             Unicasts Tx:        555 / 0
Unicasts to host:   586 / 1             Unicasts by host:   555 / 0
Broadcasts Rx:      557194 / 729         Broadcasts Tx:      34151 / 49
Beacons Rx:         277355 / 393         Beacons Tx:        34083 / 49
Prob Req Rx:        279839 / 336         Prob Resp Tx:       64 / 0
Broadcasts to host: 277355 / 393         Broadcasts by host: 34151 / 49
Multicasts Rx:      0 / 0               Multicasts Tx:      20 / 1
Multicasts to host: 0 / 0               Multicasts by host: 20 / 1
Mgmt Packets Rx:    557673 / 729         Mgmt Packets Tx:    34566 / 49
RTS received:       0 / 0               RTS transmitted:    0 / 0
Duplicate frames:   0 / 0               CTS not received:   0 / 0
CRC errors:         41287 / 54          Unicast Fragments Tx: 0 / 0
WEF errors:         0 / 0               Retries:            0 / 0
Buffer full:        0 / 0               Packets one retry:   0 / 0
Host buffer full:   0 / 0               Packets > 1 retry:   0 / 0
Header CRC errors:  0 / 0               Protocol defers:     0 / 0
Invalid header:     0 / 0               Energy detect defers: 0 / 0
Length invalid:     0 / 0               Jammer detected:     0 / 0
Incomplete fragments: 0 / 0           Packets aged:        0 / 0
Rx Concats:         0 / 0               Tx Concats:         0 / 0
PHY RX ERROR STATISTICS: total/last 5 sec (8129/8)
Tx underrun:        0 / 0               Error panic:         0 / 0
Radar detect:       0 / 0               Abort:               0 / 0
Tx override Rx:     0 / 0
OFDM timing:        2411 / 0             OFDM illegal parity: 0 / 0
OFDM illegal rate:  0 / 0               OFDM illegal length: 0 / 0
OFDM power drop:    0 / 0               OFDM illegal service: 0 / 0
```

```

OFDM restart:                2 / 0
CCK timing:                  1006 / 0
CCK illegal rate:            0 / 0
CCK restart:                 4710 / 8
RATE 1.0 Mbps
Rx Packets:                  277857 / 394
Rx Bytes:                    38460765 / 54811
RTS Retries:                 0 / 0
RATE 2.0 Mbps
Rx Packets:                   4 / 0
Rx Bytes:                    268 / 0
RTS Retries:                 0 / 0
RATE 5.5 Mbps
Rx Packets:                   3 / 0
Rx Bytes:                    813 / 0
RTS Retries:                 0 / 0
RATE 6.0 Mbps
Rx Packets:                   5 / 0
Rx Bytes:                    665 / 0
RTS Retries:                 0 / 0
RATE 11.0 Mbps
Rx Packets:                   72 / 0
Rx Bytes:                    13051 / 0
RTS Retries:                 0 / 0
Interface Dot11Radio0/0/1 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER
Host Rx Bytes:               597052 / 3618
Unicasts Rx:                 335 / 0
Unicasts to host:            335 / 0
Broadcasts Rx:               10193 / 81
Beacons Rx:                  4414 / 27
Prob Req Rx:                 5779 / 54
Broadcasts to host:          4414 / 27
Multicasts Rx:               0 / 0
Multicasts to host:          0 / 0
Mgmt Packets Rx:             10195 / 81
RTS received:                0 / 0
Duplicate frames:            0 / 0
CRC errors:                  14 / 0
WEP errors:                  0 / 0
Buffer full:                 0 / 0
Host buffer full:            0 / 0
Header CRC errors:           0 / 0
Invalid header:              0 / 0
Length invalid:              0 / 0
Incomplete fragments:        0 / 0
Rx Concats:                  0 / 0
PHY RX ERROR STATISTICS: total/last 5 sec (749/0)
Tx underrun:                 0 / 0
Radar detect:                0 / 0
Tx override Rx:              0 / 0
OFDM timing:                 749 / 0
OFDM illegal rate:           0 / 0
OFDM power drop:             0 / 0
OFDM restart:                0 / 0
CCK timing:                  0 / 0
CCK illegal rate:            0 / 0
CCK restart:                 0 / 0
RATE 6.0 Mbps
Rx Packets:                  4448 / 32
Rx Bytes:                    611446 / 4416
RTS Retries:                 0 / 0
RATE 54.0 Mbps
Rx Packets:                   333 / 0
Rx Bytes:                    17010 / 0
RTS Retries:                 0 / 0
TRANSMITTER
Host Tx Bytes:               642705 / 4371
Unicasts Tx:                 16 / 0
Unicasts by host:            16 / 0
Broadcasts Tx:               6872 / 47
Beacons Tx:                  6872 / 47
Prob Resp Tx:                12 / 0
Broadcasts by host:          6872 / 47
Multicasts Tx:               6 / 0
Multicasts by host:          6 / 0
Mgmt Packets Tx:             6874 / 47
RTS transmitted:             0 / 0
CTS not received:            0 / 0
Unicast Fragments Tx:        0 / 0
Retries:                     0 / 0
Packets one retry:           0 / 0
Packets > 1 retry:           0 / 0
Protocol defers:             0 / 0
Energy detect defers:        0 / 0
Jammer detected:             0 / 0
Packets aged:                0 / 0
Tx Concats:                  0 / 0
Error panic:                 0 / 0
Abort:                       0 / 0
OFDM illegal parity:         0 / 0
OFDM illegal length:         0 / 0
OFDM illegal service:        0 / 0
CCK header CRC:              0 / 0
CCK illegal service:         0 / 0
Misc errors:                 0 / 0
Tx Packets:                  0 / 0
Tx Bytes:                    0 / 0
Data Retries:                0 / 0
Tx Packets:                   3 / 0
Tx Bytes:                    273 / 0
Data Retries:                0 / 0

```

**Related Commands**

| Command                       | Description   |
|-------------------------------|---|
| <b>clear dot11 statistics</b> | Resets the statistics for a specified radio interface or client device. |



# show dot11 vlan-name

To display VLAN name and ID pairs configured on an access point, use the **show dot11 vlan-name** command in privileged EXEC mode.

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

## Syntax Description

|                  |   |
|------------------|---|
| <b>vlan-name</b> | (Optional) The ASCII name of a specific VLAN. |
|------------------|---|

## Command Default

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.                                  |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |

## Usage Guidelines

If your access point is not configured with VLAN names or is configured only with VLAN IDs, there is no output for this command.

## Examples

The following example shows how to display the VLAN name and ID for the vlan1 VLAN:

```
Router# show dot11 vlan-name vlan1
```

## Related Commands

| Command                | Description   |
|------------------------|---|
| <b>dot11 vlan-name</b> | Assigns a name to a VLAN in addition to its numerical ID. |

## show interfaces dot11Radio

To display configuration information for a specific dot11Radio interface, use the **show interfaces dot11Radio** command in privileged EXEC mode.

**show interfaces dot11Radio** *interface* [**accounting**|**counters**|**crb**|**dampening**|**description**|**irb**|**mac-accounting**|**mpls-exp**|**precedence**|**pruning**|**rate-limit**|**stats**|**status**|**summary**|**switching**|**switchport**|**trunk**]

### Syntax Description

|                       |   |
|-----------------------|---|
| <i>interface</i>      | The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1.    |
| <b>accounting</b>     | Displays interface accounting information.                            |
| <b>counters</b>       | Displays interface counters.  |
| <b>crb</b>            | Displays interface routing and bridging information.                  |
| <b>dampening</b>      | Displays interface dampening information.                             |
| <b>description</b>    | Displays a description of the interface.                              |
| <b>irb</b>            | Displays interface routing and bridging information.                  |
| <b>mac-accounting</b> | Displays interface mac-accounting information.                        |
| <b>mpls-exp</b>       | Displays interface MPLS experimental accounting information.          |
| <b>precedence</b>     | Displays interface precedence accounting information.                 |
| <b>pruning</b>        | Displays interface trunk VTP pruning information.                     |
| <b>rate-limit</b>     | Displays interface rate limit information.                            |
| <b>stats</b>          | Displays interface packets and octets, in and out, by switching path. |
| <b>status</b>         | Displays interface line status.                                       |
| <b>summary</b>        | Displays an interface summary.  |
| <b>switching</b>      | Displays interface switching information.                             |
| <b>switchport</b>     | Displays interface switchport information.                            |
| <b>trunk</b>          | Displays interface trunk information.                                 |

**Command Modes**

Privileged EXEC

**Command History**

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Examples**

The following is sample output for dot11 radio interface 0:

```

Router# show interfaces dot11Radio 0
Dot11Radio0 is reset, line protocol is down
Hardware is 802.11G Radio, address is 0014.a427.3a00 (bia 0014.a427.3a00)
MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/30 (size/max)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 4 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out

```

**Related Commands**

| Command                                      | Description  |
|--|--|
| <b>show interfaces dot11Radio statistics</b> | Displays status information for the radio interface. |
| show interfaces dot11Radio aaa timeout       | Displays dot11 AAA timeout values.                   |

# show interfaces dot11Radio aaa timeout

To display dot11 authentication, authorization, and accounting (AAA) timeout values, use the **show interfaces dot11Radio aaa timeout** command in privileged EXEC mode.

**show interfaces dot11Radio** *interface* **aaa timeout**

## Syntax Description

|                  |  |
|------------------|--|
| <i>interface</i> | The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1. |
|------------------|--|

## Command Modes

Privileged EXEC

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## Examples

The following example shows sample AAA timeout values for radio interface 0/3/0:

```
Router# show interfaces dot11Radio 0/3/0 aaa timeout
802.1X Parameters (in seconds)
-----
reauth-period          no
client-timeout         120
Mac Authentication Parameters (in seconds)
-----
holdoff-time           0
```

# show interfaces dot11Radio statistics

To display statistics for a specific dot11Radio interface, use the **show interfaces dot11Radio statistics** command in privileged EXEC mode.

## show interfaces dot11Radio interface statistics

### Syntax Description

|                  |  |
|------------------|--|
| <i>interface</i> | The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1. |
|------------------|--|

### Command Modes

Privileged EXEC

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Examples

The following example shows sample statistics for radio interface 0/3/0:

```
Router# show interfaces dot11Radio 0/3/0 statistics
Interface Dot11Radio0/0/0 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx Bytes:      38919896 /56768      Host Tx Bytes:      3752618 /5145
Unicasts Rx:        606 / 1              Unicasts Tx:        562 / 0
Unicasts to host:   606 / 1              Unicasts by host:   562 / 0
Broadcasts Rx:      580376 / 854          Broadcasts Tx:      35522 / 49
Beacons Rx:         288916 / 421          Beacons Tx:         35450 / 49
Prob Req Rx:        291460 / 433          Prob Resp Tx:       64 / 0
Broadcasts to host: 288916 / 421          Broadcasts by host: 35522 / 49
Multicasts Rx:      0 / 0                Multicasts Tx:      27 / 0
Multicasts to host: 0 / 0                Multicasts by host: 27 / 0
Mgmt Packets Rx:    580862 / 854          Mgmt Packets Tx:    35940 / 49
RTS received:       0 / 0                RTS transmitted:    0 / 0
Duplicate frames:   0 / 0                CTS not received:   0 / 0
CRC errors:         42943 / 72            Unicast Fragments Tx: 0 / 0
WEP errors:         0 / 0                Retries:            0 / 0
Buffer full:        0 / 0                Packets one retry:   0 / 0
Host buffer full:   0 / 0                Packets > 1 retry:   0 / 0
Header CRC errors:  0 / 0                Protocol defers:     0 / 0
Invalid header:     0 / 0                Energy detect defers: 0 / 0
Length invalid:     0 / 0                Jammer detected:     0 / 0
Incomplete fragments: 0 / 0              Packets aged:        0 / 0
Rx Concats:         0 / 0                Tx Concats:          0 / 0
PHY RX ERROR STATISTICS: total/last 5 sec ( 8292/ 2)
Tx underrun:        0 / 0                Error panic:         0 / 0
Radar detect:       0 / 0                Abort:               0 / 0
Tx override Rx:     0 / 0
OFDM timing:        2411 / 0              OFDM illegal parity: 0 / 0
OFDM illegal rate:  0 / 0                OFDM illegal length: 0 / 0
OFDM power drop:    0 / 0                OFDM illegal service: 0 / 0
```

## show interfaces dot11Radio statistics

|                   |                  |                      |          |
|-------------------|------------------|----------------------|----------|
| OFDM restart:     | 2 / 0            |                      |          |
| CCK timing:       | 1006 / 0         | CCK header CRC:      | 0 / 0    |
| CCK illegal rate: | 0 / 0            | CCK illegal service: | 0 / 0    |
| CCK restart:      | 4873 / 2         | Misc errors:         | 0 / 0    |
| RATE 1.0 Mbps     |                  |                      |          |
| Rx Packets:       | 289438 / 422     | Tx Packets:          | 0 / 0    |
| Rx Bytes:         | 40066067 / 58480 | Tx Bytes:            | 0 / 0    |
| RTS Retries:      | 0 / 0            | Data Retries:        | 0 / 0    |
| RATE 2.0 Mbps     |                  |                      |          |
| Rx Packets:       | 4 / 0            | Tx Packets:          | 0 / 0    |
| Rx Bytes:         | 268 / 0          | Tx Bytes:            | 0 / 0    |
| RTS Retries:      | 0 / 0            | Data Retries:        | 0 / 0    |
| RATE 5.5 Mbps     |                  |                      |          |
| Rx Packets:       | 3 / 0            | Tx Packets:          | 0 / 0    |
| Rx Bytes:         | 813 / 0          | Tx Bytes:            | 0 / 0    |
| RTS Retries:      | 0 / 0            | Data Retries:        | 0 / 0    |
| RATE 6.0 Mbps     |                  |                      |          |
| Rx Packets:       | 5 / 0            | Tx Packets:          | 0 / 0    |
| Rx Bytes:         | 665 / 0          | Tx Bytes:            | 0 / 0    |
| RTS Retries:      | 0 / 0            | Data Retries:        | 0 / 0    |
| RATE 11.0 Mbps    |                  |                      |          |
| Rx Packets:       | 72 / 0           | Tx Packets:          | 21 / 0   |
| Rx Bytes:         | 13051 / 0        | Tx Bytes:            | 1928 / 0 |
| RTS Retries:      | 0 / 0            | Data Retries:        | 0 / 0    |

# show platform software infrastructure lsmapi

To display the statistics for the Linux Shared Memory Punt Interface (LSMPI) on the router, use the **show platform software infrastructure lsmapi** command in privileged EXEC mode.

**show platform software infrastructure lsmapi driver**

## Syntax Description

|               |  |
|---------------|--|
| <b>driver</b> | Displays the LSMPI driver information. |
|---------------|--|

## Command Modes

Privileged EXEC (#)

## Command History

| Release                  | Modification  |
|--------------------------|---|
| Cisco IOS XE Release 2.6 | This command was introduced.  |
| 15.0(1)S                 | This command was integrated into Cisco IOS Release 15.0(1)S. The <b>driver</b> keyword was added. |

## Usage Guidelines

LSMPI is the virtual interface for the packet transfer between the IOS daemon (IOSd) and Linux kernel on RP through the Linux shared memory. Packets punted from the ESP to the RP are received by the Linux kernel of the RP. The Linux kernel sends those packets to the IOSD process through LSMPI.

## Examples

The following is sample output from the **show platform software infrastructure lsmapi** command:

```
Router# show platform software infrastructure lsmapi driver
```

```
LSMPI Driver stat ver: 1
Packets:
  In: 1736274594
  Out: 1734930746

Rings:
  RX: 2047 free    0    in-use    2048 total
  TX: 2047 free    0    in-use    2048 total
  RXDONE: 2047 free 0    in-use    2048 total
  TXDONE: 2047 free 0    in-use    2048 total

Buffers:
  RX: 2047 free    6147 in-use    8194 total

Reason for RX drops (sticky):
  Ring full      : 202930
  Ring put failed: 0
  No free buffer : 731823
  Receive failed : 0
  Packet too large: 0
  Other inst buf : 0
  Consecutive SOPs: 0
```

```

No SOP or EOP      : 0
EOP but no SOP     : 0
Particle overrun   : 0
Bad particle ins    : 0
Bad buf cond       : 0
DS rd req failed   : 0
HT rd req failed   : 202930
Reason for TX drops (sticky):
Bad packet len     : 0
Bad buf len        : 0
Bad ifindex        : 0
No device          : 0
No skbuff          : 0
Device xmit fail   : 0
Device xmit retry  : 0
Bad u->k xlation    : 0
No extra skbuff    : 0
Consecutive SOPs   : 0
No SOP or EOP      : 0
EOP but no SOP     : 0
Particle overrun   : 0
Other inst buf     : 0
Dual stack:
Registration        : 1
De-registration     : 0
Rx packets          : 1736274594
Rx packets err      : 0
L2 Rx packets       : 0
L3 Rx packets       : 0
Looped packets      : 0
skb nonlinear       : 0
Drv stat:
Rx particles        : 3472549117
Tx particles        : 3469859438
Rx err              : 0
Tx err              : 0
Total Err           : 0

```

The table below describes the significant fields shown in the display.

**Table 6: show platform software infrastructure lsmapi Field Descriptions**

| Field                        | Description  |
|------------------------------|--|
| Field                        | Description  |
| Packets                      | Number of packets handled at the LSMPI driver. "In" indicates the packet count towards the Cisco IOS software, whereas "Out" indicates the packet count from Cisco IOS software. |
| Rings                        | The LSMPI driver and Cisco IOS software maintain rings to send and receive the packets. These counters indicate the current ring statistics.                                     |
| Buffers                      | LSMPI receiving (RX) buffers are managed by the LSMPI. This value indicates the statistics maintained at LSMPI driver.   |
| Reason for RX drops (sticky) | These counters indicate the reasons for the RX flow control.   |



| Field                        | Description  |
|------------------------------|--|
| Reason for TX drops (sticky) | These counters indicate the reason for the transmitting (TX) flow control.                     |
| Dual stack                   | Additional statistics for the packets from the management interface to the Cisco IOS software. |

### Related Commands

| Command                                     | Description   |
|---|---|
| <b>show platform hardware slot</b>          | Displays information about the processor in a chassis slot.           |
| <b>show platform hardware qfp interface</b> | Displays information about an interface in the target flow processor. |

# show radius local-server statistics

To display the statistics for the local authentication server, use the **show radius local-server statistics** command in privileged EXEC mode.

**show radius local-server statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

| Command History | Release    | Modification  |
|-----------------|------------|---|
|                 | 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
|                 | 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

**Examples** The following output displays statistics for the local authentication server.

```
Router# show radius local-server statistics
Successes           : 11262      Unknown usernames   : 0
Client blocks       : 0          Invalid passwords   : 8
Unknown NAS         : 0          Invalid packet from NAS: 0
NAS : 10.0.0.1
Successes           : 11262      Unknown usernames   : 0
Client blocks       : 0          Invalid passwords   : 8
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
Maximum number of configurable users: 50, current user count: 11
Username            Successes  Failures  Blocks
vayu-ap-1           2235      0         0
vayu-ap-2           2235      0         0
vayu-ap-3           2246      0         0
vayu-ap-4           2247      0         0
vayu-ap-5           2247      0         0
vayu-11              3         0         0
vayu-12              5         0         0
vayu-13              5         0         0
vayu-14              30        0         0
vayu-15              3         0         0
scm-test             1         8         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 the **clear radius local-server statistics** command in privileged EXEC mode to reset local authenticator statistics to zero.

### Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>block count</b>               | Configures the parameters for locking out members of a group to help protect against unauthorized attacks.                       |
| <b>clear radius local-server</b> | Clears the statistics display or unblocks a user.  |
| <b>debug radius local-server</b> | Displays the debug information for the local server.   |
| <b>group</b>                     | Enters user group configuration mode and configures shared setting for a user group.   |
| <b>nas</b>                       | Adds an access point or router to the list of devices that use the local authentication server.                                  |
| <b>radius-server host</b>        | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>       | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>reauthentication time</b>     | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.  |
| <b>ssid</b>                      | Specifies up to 20 SSIDs to be used by a user group.   |
| <b>user</b>                      | Authorizes a user to authenticate using the local authentication server.   |
| <b>vlan</b>                      | Specifies a VLAN to be used by members of a user group.  |

## speed (access point radio)

To configure the data rates supported by the access point radio, use the **speed** command in interface configuration mode. To reset the data rates to the default values, use the no form of this command.

**speed** {*data-rates*| **default**| **ofdm-throughput**| **range**| **throughput**}

**no speed**

### Syntax Description

|                        |   |
|------------------------|---|
| <i>data-rates</i>      | <p>The data rates (in megabits per second [Mbps]) the access point uses to transmit unicast packets; multicast packets are sent at one of the basic data rates.</p> <p>The basic data rates set 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.</p> <p>The client must support the basic rate you select or it cannot associate to the access point.</p> |
| <b>default</b>         | <p>Sets data rates to the default settings.</p> <p>This option is supported on 5-GHz radios and 802.11g, 2.4-GHz radios only.</p>   |
| <b>ofdm-throughput</b> | <p>Sets all Orthogonal Frequency Division Multiplex (OFDM) rates (6, 9, 12, 18, 24, 36, and 48) to basic and all (Cisco Centralized Key (CCK) rates (1, 2, 5.5, and 11) to disabled.</p> <p>Disables 802.11b protection mechanisms and provides maximum throughput for 802.11g clients. This setting prevents 802.11b clients from associating to the access point.</p> <p>This option is supported on 802.11g, 2.4-GHz radios only.</p>  |
| <b>range</b>           | <p>Sets the data rate for best radio range.</p> <p>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.</p>  |

|            |   |
|------------|---|
| 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.<br><br>This option is supported on 5-GHz and 802.11b, 2.4-GHz radios only. |
|------------|---|

**Command Default**

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**

Interface configuration

**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. |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.                                       |

**Usage Guidelines**

At least one data rate must be specified. Multiple data rates are allowed.

An individual data rate can be set only to a basic or a nonbasic setting, not both. The basic setting allows transmission at the given rate for all packets, both unicast and multicast. At least one of the wireless device's data rates must be set to a basic setting.

For the 802.11b, 2.4-GHz radio, the *data-rates value can be* 1, 2, 5.5, 11.0, basic-1.0, basic-2.0, basic-5.5, or basic-11.0.

For the 802.11g, 2.4-GHz radio, the *data-rates* value can be 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, or basic-54.0.

The 5-GHz radio supports data rates of 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, or basic-54.0.

Data rates can be specified in any order, and basic rates need not precede nonbasic rates.

## Examples

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

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

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

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

# ssid

To create a service set identifier (SSID) for a radio interface or to assign a globally configured SSID to a radio interface, and enter SSID configuration mode, use the **ssid** command in interface configuration mode. To remove an SSID, use the no form of this command.

**ssid name**

**no ssid**

## Syntax Description

|      |   |
|------|---|
| name | The SSID name for the radio, expressed as a case-sensitive alphanumeric string up to 32 characters. |
|------|---|

## Command Default

On access points, the factory default SSID is tsunami.

## Command Modes

Interface configuration

## Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced                                  |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

## 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. Use the **no** form of this command to remove the SSID, which inhibits clients that use that SSID from associating with the access point.

When you create an SSID in global configuration mode, you can assign or change the SSID attributes in both global configuration and interface configuration modes. However, when you create an SSID in interface configuration mode, you cannot assign or change its attributes in global configuration mode.

## Examples

The following example shows how to create an SSID called Ivory-AP25:

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

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

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

The following 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

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

## Related Commands

| Command   | Description  |
|---|--|
| <b>authentication open (SSID configuration)</b>   | Configures the radio interface (for the specified SSID) to support open authentication.                    |
| <b>authentication shared (SSID configuration)</b> | Configures the radio interface (for the specified SSID) to support shared authentication.                  |
| authentication network eap                        | 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)                   | Configures the radio interface (for the specified SSID) to support guest mode.                             |
| max-associations (SSID configuration)             | Configures the maximum number of associations supported by the radio interface (for the specified SSID).   |
| <b>show running-config ssid</b>                   | Displays configuration details for SSIDs created in global configuration mode.                             |
| user  | Configures the radio interface (for the specified SSID) to support a specific Ethernet virtual LAN (VLAN). |



## station-role

To specify the role of the radio interface, use the **station-role** command in interface configuration mode.

**station-role** {**root** [**access-point**|**ap-only**|**bridge** [**wireless-clients**]]|**non-root** [**bridge**]}

### Syntax Description

|                     |   |
|---------------------|---|
| <b>root</b>         | Specifies that the radio interface is a root access point.  |
| <b>access-point</b> | (Optional) Specifies that the radio interface is configured for root mode operation and is 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. |
| <b>ap-only</b>      | (Optional) Specifies that the device functions only as a root access point. If the Ethernet interface is not functional, the device attempts to continue access point operation. However, you can specify a fallback mode for the radio.  |
| <b>bridge</b>       | (Optional) Specifies that the access point operates as the root bridge in a pair of bridges.  |
| wireless-clients    | (Optional) Specifies that the root bridge accepts associations from client devices.   |
| <b>non-root</b>     | Specifies that the radio interface is a nonroot access point.   |
| <b>bridge</b>       | (Optional) Specifies that the access point operates as a nonroot bridge and must associate to a root bridge.  |

### Command Default

The role of the radio interface is root access point by default.

### Command Modes

Interface configuration

### 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   |
|-----------|--|
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T.   |
| 12.4(15)T | This command was modified to support root and nonroot bridge modes and root bridges with wireless clients. |

### Usage Guidelines

Use the **station-role** command to set the role of the radio interface.

If you set the station role to a root bridge, you can specify the distance from the root bridge to the nonroot bridge or bridges with which it communicates using the **distance** command in interface configuration mode. The **distance** command is supported only on bridges.

### Examples

The following example shows how to configure an access point as a root bridge that accepts associations from client devices:

```
Router(config-if)# station-role root bridge wireless clients
```

### Related Commands

| Command         | Description  |
|-----------------|--|
| <b>distance</b> | Specifies the distance from a root bridge to the nonroot bridge or bridges with which it communicates. |

# traffic-class

To configure the radio interface quality of service (QoS) traffic class parameters for each of the four traffic types, use the **traffic-class** command in interface configuration mode. To reset a specific traffic class to the default value, use the no form of this command.

**traffic-class** {best-effort| background| video| voice} [cw-min min-value| cw-max max-value| fixed-slot backoff-interval]

**no traffic-class**

## Syntax Description

|                             |  |
|-----------------------------|--|
| <b>best-effort</b>          | Specifies the best-effort traffic class category.  |
| <b>background</b>           | Specifies the background traffic class category.   |
| <b>video</b>                | Specifies the video traffic class category.  |
| <b>voice</b>                | Specifies the voice traffic class category.  |
| cw-min min-value            | (Optional) Specifies the minimum value for the contention window. Range is from 0 to 10. |
| cw-max max-value            | (Optional) Specifies the maximum value for the contention window. Range is from 0 to 10. |
| fixed-slot backoff-interval | (Optional) Specifies the fixed slot backoff interval value. Range is from 0 to 20.       |

## Command Default

When QoS is enabled, the default traffic class settings for access points match the values in the table below.

## Command Modes

Interface configuration

## 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). |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T.  |

## 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** keywords 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** keyword specifies the number of backoff slots that are counted before the random backoff counter starts to count down.

**Table 7: 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 <100 ms latency | 4                     | 8                     | 2               |
| Voice <100 ms latency | 2                     | 8                     | 2               |

## Examples

The following 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 two backoff slots. It then begins counting down the 0 to 15 backoff slots in the contention window.

```
Router(config-if)# traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2
```

This example shows how to disable traffic class support:

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

## Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

## user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user** command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

**user** *username* {**password**|**nthash**} *password* [**group** *group-name*|**mac-auth-only**]

**no user** *username* {**password**|**nthash**} *password* [**group** *group-name*|**mac-auth-only**]

### Syntax Description

|                                |  |
|--------------------------------|--|
| <i>username</i>                | Name of the user that is allowed to authenticate using the local authentication server.      |
| <b>password</b>                | Indicates that the user password will be entered.  |
| <b>nthash</b>                  | Indicates that the NT value of the password will be entered.                                 |
| <i>password</i>                | User password.   |
| <b>group</b> <i>group-name</i> | (Optional) Name of group to which the user will be added.                                    |
| <b>mac-auth-only</b>           | (Optional) Specifies that the user is allowed to authenticate using only MAC authentication. |

### Command Default

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

### Command Modes

Local RADIUS server configuration

### Command History

| Release    | Modification  |
|------------|---|
| 12.2(11)JA | This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.   |
| 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.  |
| 12.3(11)T  | This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers. |

**Usage Guidelines**

This command is not supported on bridges.

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

**Examples**

The following example shows that the user named "user1" has been allowed to authenticate using the local authentication server (using the password "userisok"). This user will be added to the group named "team1".

```
Router(config-radsrv)# user user1 password userisok group team1
```

The following 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  |
|--|--|
| <b>block count</b>                         | Configures the parameters for locking out members of a group to help protect against unauthorized attacks.                       |
| <b>clear radius local-server</b>           | Clears the statistics display or unblocks a user.  |
| <b>debug radius local-server</b>           | Displays the debug information for the local server.   |
| <b>group</b>                               | Enters user group configuration mode and configures shared setting for a user group.   |
| <b>nas</b>                                 | Adds an access point or router to the list of devices that use the local authentication server.                                  |
| <b>radius-server host</b>                  | Specifies the remote RADIUS server host.   |
| <b>radius-server local</b>                 | Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator. |
| <b>reauthentication time</b>               | Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.  |
| <b>show radius local-server statistics</b> | Displays statistics for a local network access server.   |
| <b>ssid</b>                                | Specifies up to 20 SSIDs to be used by a user group.   |
| <b>vlan</b>                                | Specifies a VLAN to be used by members of a user group.  |



## vlan (SSID configuration)

To configure the radio interface to support a specific Ethernet VLAN, use the **vlan** command in SSID interface configuration mode. To reset the parameter to the default values, use the no form of this command.

**vlan** *vlan-id*

**no vlan**

### Syntax Description

|                |  |
|----------------|--|
| <i>vlan-id</i> | The virtual Ethernet LAN identification number for the service set identifier (SSID). Range is from 1 to 4095. |
|----------------|--|

### Command Default

No default behavior or values.

### Command Modes

SSID interface configuration

### Command History

| Release   | Modification   |
|-----------|--|
| 12.2(4)JA | This command was introduced.                                 |
| 12.4(2)T  | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Examples

The following example shows how to configure the SSID interface to support a specific VLAN:

```
Router(config-if-ssid)# vlan 2
```

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

```
Router(config-if-ssid)# no vlan
```

### Related Commands

| Command     | Description  |
|-------------|--|
| <b>ssid</b> | Specifies the SSID and enters SSID interface configuration mode. |



## world-mode

To enable access point world mode operation, use the **world-mode** command in interface configuration mode. To disable world mode operation, use the no form of this command.

**world-mode** {**legacy**|**dot11d country-code code**} {**indoor**|**outdoor**|**both**}  
**no world-mode**

### Syntax Description

|                                 |  |
|---------------------------------|--|
| legacy                          | Enables Cisco legacy world mode.   |
| dot11d <b>country-code code</b> | Enables 802.11d world mode.<br><br>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. |
| indoor                          | Specifies the access point is indoors.   |
| outdoor                         | Specifies the access point is outdoors.  |
| both                            | Specifies that access points are both indoors and outdoors.  |

### Command Default

World mode operation is disabled.

### Command Modes

Interface configuration

### 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.     |
| 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

### Usage Guidelines

You can configure the access point to support 802.11d world mode or Cisco legacy world mode.

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.

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

### Examples

The following example shows how to enable 802.11d world mode operation:

```
Router(config-if)# world-mode dot11d country-code TH both
```

### Related Commands

| Command                    | Description                         |
|----------------------------|-------------------------------------|
| <b>show running-config</b> | Displays configuration information. |

## wpa-psk

To configure a preshared key for use in Wi-Fi Protected Access (WPA) authenticated key management, use the `wpa-psk` command in SSID interface configuration mode. To disable a preshared key, use the **no** form of this command.

**wpa-psk** {**hex**|**ascii**} [**0**|**7**] *encryption-key*

**no wpa-psk** {**hex**|**ascii**} [**0**|**7**] *encryption-key*

### Syntax Description

|                |   |
|----------------|---|
| hex            | Specifies entry of the preshared 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 preshared 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. |
| 0              | (Optional) Specifies an unencrypted key follows.  |
| 7              | (Optional) Specifies an encrypted key follows.  |
| encryption-key | Preshared key for either the <b>hex</b> or <b>ascii</b> keyword.  |

**Command Default** Preshared key is disabled.

**Command Modes** SSID interface configuration

| Command History | Release    | Modification   |
|-----------------|------------|--|
|                 | 12.2(11)JA | This command was introduced.                                 |
|                 | 12.4(2)T   | This command was integrated into Cisco IOS Release 12.4(2)T. |

**Usage Guidelines** To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a preshared key for the SSID.

## Examples

The following example shows how to configure a WPA preshared key for an SSID:

```
Router(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 cyphers       | Specifies a cipher suite.                              |
| ssid                          | Specifies the SSID and enters SSID configuration mode. |