fragment-threshold through wpa-psk

fragment-threshold

To set the size at which packets are fragmented, use the **fr agment-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

bytes	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.

Command 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
show running-config	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.

Command 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.
ssid	Specifies the SSID and enters SSID configuration mode.

information-element ssidl

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.

Command 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.

Command 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
show running-config	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

optional	(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.

Command 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

interface	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.

Command 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.

Command 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

vlan-id	The VLAN identification number. Valid range is from 1 to 4094; do not enter leading zeros.
vlan-range	A VLAN range. For example, 1 - 3.
vlan-combination	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 s**ervice-policy type performance-monitor inline**command.

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
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	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.

Command 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

Command 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

ip-address	IP address of the access point or router.
key	Specifies a key.
shared-key	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.

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

Command 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
show running-config	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

rfc1042	Specifies the RFC1042 SNAP encapsulation.
dot1h	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.

Command 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
show running-config	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

milliwatt	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.
maximum	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.

Command 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
show running-config	Displays configuration information.

power local

To configure the access point radio power level, use the **power**local 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

cck	Sets Complimentary Code Keying (CCK) power levels.
ofdm	Sets Orthogonal Frequency Division Multiplexing (OFDM) power levels.
milliwatt	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.
maximum	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.

Release	Modification
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.
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.

Command 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
show running-config	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.

Command 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
show running-config	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.

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

seconds	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.

Command 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
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	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

threshold bytes	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.
retries number	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.

Command 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

interface	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.

Command 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-18.0ic-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                Statistics
   Count Quota Max Count Quota         txed  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
Firstep 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
show interfaces dot11Radio Statistics	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

mac-address	(Optional) MAC address (in xxxx.xxxx.xxxx format).
ap-number *ap-number*	(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.

Command 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
clear dot11 aaa authentication mac-authen filter-cache	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

client	(Optional) Displays all client devices associated with the access point.
repeater	(Optional) Displays all repeater devices associated with the access point.
statistics	(Optional) Displays access point association statistics for the radio interface.
mac-address	(Optional) MAC address (in xxxx.xxxx.xxxx format).
ap-number *ap-number*	(Optional) Specifies an access point number. The range is from 1 to 500.
bss-only	(Optional) Displays only the basic service set clients that are directly associated with the access point.
all-client	(Optional) Displays the status of all clients associated with the access point.
cckm-statistics	(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.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Command 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 1 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	Displays the state of the device. If the station/ wireless client is associated, the following states are displayed: • EAP-Assoc • MAC-Assoc • Assoc If the station/wireless client is not associated, the actual states are displayed: • Auth_notAssoc • Wait ReAuth • BLOCK • IAPP_get • AAA_Auth • AAA_ReAuth • Drv_Add_InProg

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.

Command 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 2 show dot11 associations Field Descriptions

Field	Description
Frequency	Displays the frequency of the radio channel., in mega hertz (MHz).
Carrier Busy	Display levels of radio activity on each channel.

Related Commands

Command	Description
dot11 carrier busy	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.

Command 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 decrpyt 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 decrpyt 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
clear dot11 statistics	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.

Command 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
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 (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 header CRC:                 0 /   0
CCK illegal rate:            0 /   0    CCK illegal service:            0 /   0
CCK restart:              4710 /   8    Misc errors:                    0 /   0
RATE 1.0 Mbps
Rx Packets:             277857 / 394    Tx Packets:                   0 /   0
Rx Bytes:             38460765 /54811    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
Interface Dot11Radio0/0/1 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx Bytes:           597052 /3618    Host Tx Bytes:             642705 /4371
Unicasts Rx:                335 /   0    Unicasts Tx:                  16 /   0
Unicasts to host:           335 /   0    Unicasts by host:             16 /   0
Broadcasts Rx:            10193 /  81    Broadcasts Tx:              6872 /  47
Beacons Rx:                4414 /  27    Beacons Tx:                 6872 /  47
Prob Req Rx:               5779 /  54    Prob Resp Tx:                 12 /   0
Broadcasts to host:        4414 /  27    Broadcasts by host:         6872 /  47
Multicasts Rx:                0 /   0    Multicasts Tx:                 6 /   0
Multicasts to host:           0 /   0    Multicasts by host:            6 /   0
Mgmt Packets Rx:          10195 /  81    Mgmt Packets Tx:            6874 /  47
RTS received:                 0 /   0    RTS transmitted:               0 /   0
Duplicate frames:             0 /   0    CTS not received:              0 /   0
CRC errors:                  14 /   0    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 (749/0)
Tx underrun:                  0 /   0    Error panic:                   0 /   0
Radar detect:                 0 /   0    Abort:                         0 /   0
Tx override Rx:               0 /   0
OFDM timing:                749 /   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:                 0 /   0
CCK timing:                   0 /   0    CCK header CRC:                0 /   0
CCK illegal rate:             0 /   0    CCK illegal service:           0 /   0
CCK restart:                  0 /   0    Misc errors:                   0 /   0
RATE 6.0 Mbps
Rx Packets:                4448 /  32    Tx Packets:                   0 /   0
Rx Bytes:                611446 /4416    Tx Bytes:                     0 /   0
RTS Retries:                  0 /   0    Data Retries:                 0 /   0
RATE 54.0 Mbps
Rx Packets:                 333 /   0    Tx Packets:                   3 /   0
Rx Bytes:                17010 /   0    Tx Bytes:                   273 /   0
RTS Retries:                  0 /   0    Data Retries:                 0 /   0
```

Related Commands

Command	Description
clear dot11 statistics	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

vlan-name	(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.

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
dot11 vlan-name	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

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

Command 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
show interfaces dot11Radio statistics	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

interface	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.

Command 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

interface	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.

Command 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
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 lsmpi

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

show platform software infrastructure lsmpi driver

Syntax Description

driver	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 **driver** 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.

Command Examples

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

```
Router# show platform software infrastructure lsmpi 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 rtry : 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 3 show platform software infrastructure lsmpi 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
show platform hardware slot	Displays information about the processor in a chassis slot.
show platform hardware qfp interface	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.

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

data-rates	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. 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. The client must support the basic rate you select or it cannot associate to the access point.
default	Sets data rates to the default settings. This option is supported on 5-GHz radios and 802.11g, 2.4-GHz radios only.
ofdm-throughput	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. 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. This option is supported on 802.11g, 2.4-GHz radios only.
range	Sets the data rate for best radio range. On the 2.4-GHz radio, this selection configures the 1.0 data rate to basic and the other data rates to supported. On the 5-GHz radio, this selection configures the 6.0 data rate to basic and the other data rates to supported.

throughput	(Optional) Sets the data rate for best throughput. On the 2.4-GHz radio, all data rates are set to basic. On the 5-GHz radio, all data rates are set to basic. 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.

Command 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
show running-config	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 **ssi d 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.

Command 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
authentication open (SSID configuration)	Configures the radio interface (for the specified SSID) to support open authentication.
authentication shared (SSID configuration)	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).
show running-config ssid	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

root	Specifies that the radio interface is a root access point.
access-point	(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.
ap-only	(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.
bridge	(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.
non-root	Specifies that the radio interface is a nonroot access point.
bridge	(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.

Release	Modification
12.2(11)JA	This command was modified to support 5-GHz bridges.
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.

Command 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
distance	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

best-effort	Specifies the best-effort traffic class category.
background	Specifies the background traffic class category.
video	Specifies the video traffic class category.
voice	Specifies the voice traffic class category.
cw-min 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 4 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

Command 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
show running-config	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

username	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
password	User password.
group *group-name*	(Optional) Name of group to which the user will be added.
mac-auth-only	(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.

Release	Modification
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.

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

Command	Description
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	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

vlan-id	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.

Command 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
ssid	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 **country-code code**	Enables 802.11d world mode. When you enter the dot11d option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website.
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.

Command 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
show running-config	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 **hex** or **ascii** 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.

Command 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.