Wireless LAN Commands

accounting (SSID configuration mode)

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

receive	Specifies the antenna that the access point uses to receive radio signals.
transmit	Specifies the antenna that the access point uses to transmit radio signals.
diversity	Specifies the antenna with the best signal. Default value.
left	Specifies to use the left antenna only.
right	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 c**onfiguration 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

wpa	Specifies Wi-Fi Protected Access (WPA) authenticated key management for the service set identifier (SSID).
cckm	Specifies Cisco Centralized Key Management (CCKM) authenticated key management for the SSID.
optional	(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 802.1*x*-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 ciphers	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

list-name	The list name for EAP authentication. List name can be from 1 to 31 characters in length.
mac-address *list-name*	(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.
authentication open (SSID configuration mode)	Specifies open authentication.
authentication shared (SSID configuration mode)	Specifies shared-key authentication.

authentication open (SSID configuration mode)

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

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 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 configuration mode)	Specifies shared key authentication.
ssid	Specifies the SSID and enters SSID configuration mode.

authentication shared (SSID configuration mode)

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.
authentication open (SSID configuration mode)	Specifies open authentication.
authentication network-eap	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

period *microseconds*	Specifies the beacon time in Kilomicroseconds (Kms). Kms is a unit of measurement in software terms. K = 1024, m = 10-6, and s = seconds, so Kms = 0.001024 seconds, 1.024 milliseconds, or 1024 microseconds. Range is from 20 to 4000 microseconds. Default is 100.
dtim-period *period-count*	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

count	Number of failed passwords that triggers a lockout. Range is from 1 to 4294967295.
time	Specifies the time, in seconds, to block the account.
seconds	Number of seconds that the lockout should last. Range is from 1 to 4294967295.
infinite	Specifies the lockout is indefinite.

Defaults

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 Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
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.

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

Command	Description
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.

Command	Description
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.
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.

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.
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 802.1*x* 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

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

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
show controllers dot11Radio	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

mac-address	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
show dot11 associations	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

dot11Radio *interface*	Specifies a radio interface.
mac-address	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
show interfaces dot11Radio statistics	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

statistics	Clears the display of statistical information.
user	Unblocks the locked username specified.
username	Locked username.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
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.

Examples

The following example shows how to unblock the locked username “user1”:

```
Router# clear radius local-server user user1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
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 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.

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 Descriptionn

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

Usage Guidelines

Use this command to display debugging information about radio functions.

Examples

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

```
Router# debug dot11 events
```

Related Commands

Command	Description
debug dot11 aaa	Enables debugging of dot11 AAA operations.
debug dot11 dot11radio	Enables radio debug options.

debug dot11 aaa

To enable debugging of dot11 authentication, authorization, and accounting (AAA) operations, use the **debug dot11 aaa** 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 Descriptionn

accounting	Provides information about 802.11 AAA accounting packets.
authenticator	Provides information about MAC and Extensible Authentication Protocol (EAP) authentication packets. Use the following options to activate authenticator debugging: • **all**—Activates debugging for all authenticator packets • **dispatcher**—Activates debugging for authentication request handler packets • **mac-authen**—Activates debugging for MAC authentication packets • **process**—Activates debugging for authenticator process packets • **rxdata**—Activates debugging for EAP over LAN (EAPOL) packets from client devices • **state-machine**—Activates debugging for authenticator state-machine packets • **txdata**—Activates debugging for EAPOL packets sent to client devices
dispatcher	Provides information about 802.11 AAA dispatcher (interface between association and manager) packets.
manager	Provides information about the AAA manager. Use these options to activate AAA manager debugging: • **all**—Activates all AAA manager debugging • **dispatcher**—Activates debug information for AAA manager-authenticator dispatch traffic • **keys**—Activates debug information for AAA manager key processing • **rxdata**—Activates debugging for AAA manager packets received from client devices • **state-machine**—Activates debugging for AAA manager state-machine packets • **supplicant**—Activates debugging for Light Extensible Authentication Protocol (LEAP) supplicant packets • **txdata**—Activates debugging for AAA manager packets sent to client devices.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.2(15)JA	This command was modified to include the **accounting**, **authenticator**, **dispatcher**, and **manager** debugging options.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

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
debug dot11	Enables debugging of radio functions.
debug dot11 dot11radio	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

interface	The radio interface. The 2.4-GHz radio is 0. The 5-GHz radio is 1.
accept-radio-firmware	Configures the access point to disable checking the radio firmware version.
dfs simulate	Configures the access point to simulate radar generation as part of Dynamic Frequency Selection (DFS).
channel	(Optional) Radio channel to move to. Range is from 24 to 161.
monitor	Enables RF monitor mode. Use these options to turn on monitor modes: • **ack**—Displays ACK packets. ACK packets acknowledge receipt of a signal, information, or packet. • **address**—Displays packets to or from the specified IP address • **beacon**—Displays beacon packets • **crc**—Displays packets with CRC errors • **lines**—Specifies a print line count • **plcp**—Displays Physical Layer Control Protocol (PLCP) packets • **print**—Enables RF monitor printing mode • **probe**—Displays probe packets • **store**—Enables RF monitor storage mode
print	Enables packet printing. Use these options to turn on packet printing: • **hex**—Prints entire packets without formatting • **if**—Prints the in and out interfaces for packets • **iv**—Prints the packet Wired Equivalent Privacy (WEP) IV • **lines**—Prints the line count for the trace • **mic**—Prints the Cisco Message Integrity Check (MIC) • **plcp**—Displays the PLCP • **printf**—Prints using printf instead of buginf • **raw**—Prints without formatting data • **shortadr**—Prints MAC addresses in short form

stop-on-failure	Configures the access point to not restart when the radio driver fails.
trace	Enables trace mode. Use these options to turn on trace modes: • **off**—Turns off traces • **print**—Enables trace printing • **store**—Enables trace storage

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.

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
debug dot11	Enables debugging of radio functions.
debug dot11 aaa	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

client	Displays error messages about failed client authentications.
error	Displays error messages about the local authentication server.
packets	Displays the content of the RADIUS packets that are sent and received.

Defaults

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.

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
clear radius local-server	Clears the statistics display or unblocks a user.
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.

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

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

Defaults

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 in 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 cannnot 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.

Defaults

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

Command Modes

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
station-role	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 athentication 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

timeout *seconds*	(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
clear dot11 aaa authentication mac-authen filter-cache	Clears MAC addresses from the MAC authentication cache.
show dot11 aaa authentication mac-authen filter-cache	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

draft10	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
dot1x default	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: `0007.85b3.5f4a`
ietf	Specifies the Internet Engineering Task Force (IETF) format for MAC addresses in CSID attributes. The IETF format looks like this example: `00-07-85-b3-5f-4a`
unformatted	Specifies no formatting for MAC addresses in CSID attributes. An unformatted MAC address looks like this example: `000785b35f4a`

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
debug dot11 aaa	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.
default *seconds*	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 *seconds* argument is a value from 1 to 100000.
maximum *seconds*	Specifies the maximum activity timeout, in seconds, allowed for a device regardless of the refresh rate proposed by a device when it associates. The *seconds* argument is a value from 1 to 100000.
client-station	Specifies a client station.
repeater	Specifies a repeater.
unknown	Specifies unknown (non-Cisco Aironet) device class.
workgroup-bridge	Specifies a workgroup bridge.

Command Default

Table 1 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
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
debug dot11 aaa	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
show running-config	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

seconds	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
show running-config	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

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

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 an the area code on the access point:

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

Related Commands

Command	Description
snmp-server location	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.

Defaults

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
class-map	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 **dot11qos 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 Qo parameters apply to the radio cells.
local	(Optional) Specifies the QoS parameters are for local use only.

Defaults

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.

Defaults

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

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

Defaults

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
clear dot11 statistics	Resets statistic information for a specific radio interface or a particular client with a specified MAC address.
debug dot11	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

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

Defaults

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
show dot11 vlan-name	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

seconds	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** form of this command.

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

no dot1x reauth-period

Syntax Description

seconds	The number of seconds for the reauthentication period. Range is from 1 to 65555.
server	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
show interfaces dot11Radio	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. A total of four encryption keys can be configured for each VLAN. **Note** 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 Table 2 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.
encryption-key	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 802.1*x* authentication, you do not need to configure static WEP keys.

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

Table 2 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
show running-config	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

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.
aes-ccm	Specifies that Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Code Protocol (AES-CCMP) is included in the cipher suite.
tkip	Specifies that Temporal Key Integrity Protocol (TKIP) is included in the cipher suite. **Note** If you enable a cipher suite with two elements, such as TKIP and 128-bit wired equivalent privacy (WEP), the second cipher becomes the group cipher.
wep128	(Optional) Specifies that 128-bit WEP is included in the cipher suite.
wep40	(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. Table 3 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	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40
WPA	• encryption mode ciphers aes-ccm • encryption mode ciphers aes-ccm wep128 • encryption mode ciphers aes-ccm wep40 • encryption mode ciphers aes-ccm tkip • encryption mode ciphers aes-ccm tkip wep128 • encryption mode ciphers aes-ccm tkip wep40 • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

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
encryption mode wep	Configures the access point for WEP encryption.
authentication open (SSID configuration mode)	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 ciphers** 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
encryption mode ciphers	Enables a cipher suite.