CHAPTER 10

Configuring WLAN Authentication and Encryption

This chapter describes how to configure authentication and encryption schemes to protect your WLANs.

Encryption can be achieved using shared keys or individual client keys. Individual client keys are more robust, but need to be managed. Key management can be achieved using cipher suites with Wi-Fi Protected Access (WPA) version 1 or version 2 and Cisco Centralized Key Management (CCKM) authenticated key management.

Encryption robustness can be achieved using Wired Equivalent Privacy (WEP), WEP features including AES, Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and broadcast key rotation. Authentication can be achieved using shared keys (with WEP), pre-shared keys (with WPA v1 or WPAv2) or individual client authentication with 802.1x/EAP.

Understanding Authentication and Encryption Mechanisms

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's, and any wireless client's, radio transmissions. Also, the access point typically connects to the wired infrastructure. As the access point's radio signal can expand beyond the walls of the facility where the access point is deployed, external users may be provided access to the wired infrastructure through the access point. Therefore WLAN security relies on two major pillars:

- Authenticating the users, to make sure that only valid users are allowed to communicate through the access point.
- Encrypting wireless communications, to make sure that eavesdroppers cannot deciphers signals captured from the access point and clients communications.

On Cisco Aironet access points, SSIDs are mapped directly to the access point radio, or to VLANs configured on the AP radio interface. Encryption is configured at the radio level (if no VLAN is defined on the radio interface), or at the VLAN level (as soon as one or more VLANs are defined on the radio interface). This means that if you enable several SSIDs on a given radio interface or a given VLAN, all these SSIDs must share a common encryption scheme.

Authentication is configured at the SSID level. Each SSID can have a different authentication mechanism. However, as the SSID is mapped to a VLAN (or a radio interface), you need to make sure that the authentication mechanism defined at the SSID level is compatible with the encryption mechanism defined at the VLAN (or the radio) level for that SSID.

Encryption, defined at the radio (or the VLAN) level, can use one of the following schemes:

- No encryption
- Optional Static WEP (with a 40 bit or a 128 bit long key) encryption, both clients supporting WEP and those not supporting encryption are allowed to join the SSID
- Mandatory Static WEP (with a 40 bit or a 128 bit long key) encryption, clients must support static WEP encryption to be allowed to join the SSID
- Cipher 40 bit or 128 bit WEP encryption with key management, allowing for unicast WEP key rotation (if your authentication mechanism is compatible with individual client key determination) and/or broadcast key rotation (if your authentication mechanism is compatible with individual client key determination)
- Cipher TKIP, CKIP, CMIC,CKIP-CMIC, or AES (if your authentication mechanism is compatible with individual client key determination)
- A combination of two or three ciphers (TKIP+WEP, AES+TKIP, AES+TKIP+WEP).
  This type of combination is used when you want to elevate the security level of your SSID, but still support clients that only support a weaker encryption scheme. In that case, clients will use the strongest encryption mechanism allowed by the SSID. Broadcast keys will use the encryption mechanism supported by all clients.
  Among all supported encryption schemes, AES-CCMP is the strongest, followed by TKIP. WEP is considered a weak encryption mechanism and is deprecated by the IEEE 802.11 standard.
  For example, suppose you define an AES+TKIP+WEP encryption. Clients supporting AES will use AES for their unicast key encryption. Clients not supporting AES but supporting TKIP will be allowed to join the cell, and will use TKIP for their unicast key encryption. Clients only supporting WEP will also be allowed to join the cell, and will use WEP for their unicast key encryption. When the cell contains AES, TKIP and WEP clients, the broadcast key will use WEP encryption (because WEP is the only common encryption scheme supported by all clients). When the cell contains AES and TKIP clients, but no WEP client, the broadcast key will use TKIP (the broadcast key encryption

will change to WEP if a WEP client joins the cell). When the cell contains only AES clients, the broadcast key uses AES (and will change to TKIP if TKIP clients join the cell, and to WEP if WEP clients join the cell).

Note Encryption mechanism support is incremental. A client supporting WEP may or may not support TKIP or AES. However, a client supporting TKIP necessarily supports WEP. Similarly, an AES client necessarily supports TKIP and WEP.

You can find more details about each encryption mechanism in the Understanding Encryption Modes section of this chapter.

Encryption is configured at the radio or the VLAN level. Authentication is configured at the SSID level. Authentication can use one or a combination of the following mechanisms:

- Open—No authentication is required to associate to the Access Point.
- Shared key—For using static WEP authentication.
- Network EAP—For using LEAP

Note Both Open and Shared key modes can be combined with other modes, such as EAP/802.1x, where authentication occurs after association to the access point, or with MAC authentication, where authentication occurs during the final phase of the association to the access point.

You can find more details about each authentication mechanism in the "Understanding Authentication Mechanisms" section of this chapter.

Combination of different authentication and encryption mechanisms result in different security schemes for your SSID. The following table summarizes the supported combinations:

SSID Authentication	Interface encryption	Supported security
Open	WEP optional	The AP announces the SSID as Open/Open, without broadcasting explicit support for WEP. However, the AP also accepts client association when client configuration is set to WEP encryption and/or WEP authentication. You must define a WEP key if you want to use this mode with clients using WEP.
Open	WEP mandatory	The AP announces the SSID as supporting WEP. The AP accepts client association when client configuration is set to Open/None, WEP encryption and/or WEP authentication. After the association phase, WEP support is mandatory in order to forward traffic through the access point. You must define a WEP key if you want to use this mode with clients using WEP.
Open with MAC	Any mode supported with Open authentication	Client MAC authentication is added to the final phase of the client association to the AP (see the MAC Address Authentication to the Network, page 11-5 section for more details)

SSID Authentication	Interface encryption	Supported security
Open with EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client association to the AP is followed with 802.1x/EAP authentication (supported EAP modes are LEAP,EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST). During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Open with MAC and EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client MAC authentication is added to the final phase of the client association to the AP. Client association to the AP is followed with 802.1x/EAP authentication. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Open with Optional EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Clients configured for EAP will use individual authentication and encryption with individual keys. Clients with no security configuration can also associate to the AP. This mode is designed as a transition mechanism to stronger security. Broadcast key uses the common security mechanism supported by all clients. When both EAP and Open clients are associated, the broadcast key is not encrypted.
Shared Authentication	WEP Optional	The AP announces the SSID as supporting WEP. The AP only accepts clients configured with WEP authentication. WEP encryption after association is supported, but optional.
Shared Authentication	WEP Mandatory	The AP announces the SSID as supporting WEP. The AP only accepts clients configured with WEP authentication. WEP encryption after association is mandatory.
Shared Authentication with MAC	Any mode supported with Shared authentication	WEP authentication is followed, during the final phase of the association phase, with MAC authentication.
Shared Authentication with EAP	Any mode supported with Shared authentication	WEP authentication is followed with open association to the AP. Association is followed with individual client EAP authentication and individual key generation.

SSID Authentication	Interface encryption	Supported security
Shared Authentication with EAP and MAC	Any mode supported with Shared authentication	WEP authentication is followed, during the final phase of the association phase, with MAC authentication. Association is followed with individual client EAP authentication and individual key generation.
Network EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client association to the AP is followed with Cisco LEAP authentication. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Network EAP with MAC	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client MAC authentication is added to the final phase of the client association to the AP. Client association to the AP is followed with 802.1x/EAP authentication using LEAP. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Web Authentication	Any	Web authentication can be used independently (with no other SSID authentication or encryption), or in combination with any other authentication and encryption scheme.

You can enable Network EAP authentication in combination with Open (with EAP or not, and any combination of MAC, namely Network EAP with or without MAC, with Open with or without EAP, with or without MAC, or with or without EAP and MAC). Network EAP uses LEAP, but requires support for LEAP formatting in the AP announcements. Clients that do not support this specific announcement formatting can use the Open mode (with LEAP or another EAP mechanism). The client will always try to use the most secure authentication mechanism supported through the access point, and the strongest encryption mechanism. However, client access points (in bridge or workgroup bridge mode) will use Network EAP by default, unless you configure the client side specifically to use a stronger authentication mechanism.

When configuring the SSID, using a cipher allows you to manage each client individual key. When configuring the SSID, you can define how this key should be managed. If you configure the interface to use a Cipher, you must also enable key management when configuring the SSID. Key management can be set to none (when using no security or shared key security), mandatory (when using a cipher), or Optional (when using Open with optional EAP or Shared key with optional EAP authentications). Please refer to the Key management sections of this chapter for more details on the different key management modes.

Understanding Encryption Modes

As encryption is defined at the interface (VLAN or radio) level of the access point, and can be common to several SSIDs, encryption is usually configured before the SSID and its authentication mechanism.

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. Because encrypted communication is the first line of defense against attackers, Cisco recommends that you use full encryption on your wireless network.

The original encryption mechanism described by the 802.11 standard is WEP (Wired Equivalent Privacy). WEP encryption scrambles the communication between the access point and client devices to keep the communication private. The 802.11 standard describes what Cisco and some other vendors describe as static WEP. In this mode, WEP keys are defined statically on the client and the AP. Both the access point and client devices use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

WEP is a legacy protocol deprecated by the 802.11 standard. Cisco recommends using a stronger protocol, such as AES/CCMP, whenever possible.

When your SSID authentication mechanism uses Extensible Authentication Protocol (EAP) with 802.1x authentication (and without WPA v1 or WPA v2 support), dynamic WEP keys can be generated for each wireless user. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See Chapter 11, "Configuring Authentication Types," for detailed information on EAP and other authentication types.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite when using WPA, WPA2 or CCKM. When using WEP encryption, you have the choice to set WEP using the WEP encryption command, or the cipher command. When using the WEP encryption command, you can use a static WEP key for authentication and / or encryption. However, you cannot use per user secure authentication (using 802.1x) in this mode. Because cipher suites can provide WEP encryption while also allowing use of individual user authentication and key management, Cisco recommends that you enable WEP by using the encryption mode cipher command in the CLI or by using the cipher drop-down list in the web-browser interface, instead of the WEP encryption command. However, WEP is a protocol deprecated by the IEEE, and Cisco recommends using WEP only when client drivers do not support any stronger security mechanism. The recommended security is AES-CCMP.

These security features protect the data traffic on your wireless LAN:

- AES-CCMP—Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's *FIPS Publication 197*, 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.

Note The 802.11n amendment relies on implementation of either No encryption or AES-CCMP encryption. Therefore, 802.11n radios require that either no encryption or AES-CCMP be configured to provide 802.11n rates support.

- WEP (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
  - A per-packet key mixing function to defeat weak-key attacks
  - A new IV sequencing discipline to detect replay attacks
  - A cryptographic message integrity check (MIC), called *Michael*, to detect forgeries such as bit flipping and altering packet source and destination
  - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. WPA TKIP replaced most CKIP implementations.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks. Cisco CKIP is required to use CMIC.
- Broadcast key rotation (also known as Group Key Update)—Broadcast key rotation allows the access point to generate the best possible random group key and update all key-management capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates. See the "Using WPA Key Management" section on page 11-7 for details on WPA.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Note Encryption is configured at the interface or the VLAN level, and authentication is configured for each SSDI to be supported on the relevant VLAN or interface. Therefore, encryption and authentication combine. See Chapter 11, "Configuring Authentication Types,"for details on how encryption and authentication combinations.

Configuring Encryption Modes

Encryption is configured at the VLAN or radio interface level. Ensure that the encryption mechanism you enable is compatible with the authentication mechanism you plan on using for the SSID, that is mapped to the relevant VLAN or radio interface. For more details on encryption and authentication schemes compatibility, see the Understanding Authentication and Encryption Mechanisms section.

Note WEP, TKIP, MIC and broadcast key rotation are disabled by default.

Creating Static WEP Keys

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

Beginning in privileged EXEC mode, follow these steps to create a WEP key and set the key properties:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**0** | **7**] [**transmit-key**]	Create a WEP key and set up its properties. • (Optional) Select the VLAN for which you want to create a key. • Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN. • Enter the key and set the size of the key, either 40-bit or 128-bit. 40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits. • (Optional) Specify whether the key string you enter in this command is an encrypted string or the plain text key. The plain text key will be encrypted when you press the Enter key. • (Optional) Set this key as the transmit key. The key in slot 1 is the transmit key by default. **Note** If you configure static WEP with MIC (key hash), 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. **Note** Configuration of static WEP with CMIC is not supported. **Note** Using security features such as authenticated key management can limit WEP key configurations. See the "WEP Key Restrictions" section on page 10-9 for a list of features that impact WEP keys.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 3 for VLAN 22 and sets the key as the transmit key:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-if)# end
```

WEP Key Restrictions

Table 10-1 lists WEP key restrictions based on your security configuration.

Table 10-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC	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 **Note** Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Example WEP Key Setup

Table 10-2 shows an example WEP key setup that would work for the access point and an associated device.

Table 10-2 WEP Key Setup Example

Key Slot	Access Point		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	1234567890123456789abcdef	—	1234567890123456789abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba

Table 10-2 WEP Key Setup Example (continued)

Key Slot	Access Point		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

Because the access point's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must have the same contents. WEP key 4 on the other device is set, but because it is not selected as the transmit key, WEP key 4 on the access point does not need to be set at all.

Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client's slot 1 must be selected as the transmit key.

Enabling Cipher Suites

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**encryption [vlan** *vlan-id*] **mode ciphers {aes-ccm | ckip | ckip-cmic | cmic | tkip | wep128 | wep40}**	Enable a cipher suite containing the protection you need. Table 10-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure. • (Optional) Select the VLAN for which you want to enable a cipher type. • Select the cipher options you need. You can select more than one cipher. **Note** If you enable a cipher suite with 2 or 3 elements, each client will use the highest encryption mechanism enabled on the interface and supported by the client. The broadcast key will use the element supported by all clients. See the Understanding Authentication and Encryption Mechanisms section for more details. **Note** If you configure **ckip** you must also enable Aironet extensions. The command to enable Aironet extensions is **dot11 extension aironet**. **Note** You can also use the **encryption mode wep** command to set up static WEP. However, you should use **encryption mode wep** only if no clients that associate to the access point are capable of key management. See the *Cisco IOS Command Reference for Cisco Access Points and Bridges* for a detailed description of the **encryption mode wep** command. **Note** When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management. **Note** You must configure WPA key management as optional in order to configure cipher modes **TKIP + WEP 128** or **TKIP + WEP 40**.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

Matching Cipher Suites with WPA or CCKM

If you configure your access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 10-3 lists the cipher suites that are compatible with WPA and CCKM.

Table 10-3 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 aes
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode ciphers eas **Note** Encryption mode ciphers tkip wep128 and tkip wep-40 can only be used is WPA is configured as optional.

Note If using WPA and CCKM as key management, only tkip and aes ciphers are supported. If using only CCKM as key management, ckip, cmic, ckip-cmic, tkip, wep, and aes ciphers are supported.

Note When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.

For a complete description of WPA and instructions for configuring authenticated key management, see the "Using WPA Key Management" section on page 11-7.

Note Wi-Fi certified access points no longer support WPA/TKIP configuration. TKIP is only allowed in combination with WPA2/AES for backward compatibility to allow older TKIP-only devices to associate. WPA version 1 option has been removed from the authentication key-management wpa cli and configuring TKIP only under this interface is not supported. For more information, see Configuration and CLI Changes in this Release, page 1-4.

Enabling and Disabling Broadcast Key Rotation

Broadcast key rotation is disabled by default.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Beginning in privileged EXEC mode, follow these steps to enable broadcast key rotation:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**broadcast-key change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	Enable broadcast key rotation. • Enter the number of seconds between each rotation of the broadcast key. • (Optional) Enter a VLAN for which you want to enable broadcast key rotation. • (Optional) If you enable WPA authenticated key management, you can enable additional circumstances under which the access point changes and distributes the WPA group key. – Membership termination—the access point generates and distributes a new group key when any authenticated client device disassociates from the access point. This feature protects the privacy of the group key for associated clients. However, it might generate some overhead if clients on your network roam frequently. – Capability change—the access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point. See Chapter 11, "Configuring Authentication Types," for detailed instructions on enabling authenticated key management.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable broadcast key rotation.

This example enables broadcast key rotation on VLAN 22 and sets the rotation interval to 300 seconds:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-if)# end
```