



CHAPTER 10

Configuring Cipher Suites and WEP

This chapter describes how to configure the cipher suites required to use WPA and CCKM authenticated key management, Wired Equivalent Privacy (WEP), WEP features including AES, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. This chapter contains these sections:

- [Understanding Cipher Suites and WEP, page 10-2](#)
- [Configuring Cipher Suites and WEP, page 10-3](#)

Understanding Cipher Suites and WEP

This section describes how WEP and cipher suites protect traffic on your wireless LAN.

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 WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the communication between the access point and client devices to keep the communication private. 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.

Extensible Authentication Protocol (EAP) authentication, also called 802.1x authentication, provides dynamic WEP keys to wireless users. 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 to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode cipher** command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

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**

Cisco Aironet 1130 and 1230 series access points support WPA2. Cisco Aironet 1100, 1200, and 1300 series 802.11g radios support WPA2 with a Cisco IOS software upgrade to Release 12.3(2)JA or later.

**Note**

Cisco Aironet 1200 series radio modules having part numbers AIR-RM21A or AIR-RM22A support WPA2 or AES.

**Note**

Cisco 802.11n radios require that either no encryption or AES-CCMP be configured for proper operation.

- 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.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks.
- 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. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC, TKIP, and broadcast key rotation:

- [Creating WEP Keys, page 10-3](#)
- [Enabling Cipher Suites and WEP, page 10-6](#)
- [Enabling and Disabling Broadcast Key Rotation, page 10-7](#)

**Note**

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

Creating 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 <i>vlan-id</i>] key <i>I-4</i> size { 40 128 } <i>encryption-key</i> [0 7] [transmit-key]	Create a WEP key and set up its properties. <ul style="list-style-type: none"> • (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 is encrypted (7) or unencrypted (0). • (Optional) Set this key as the transmit key. The key in slot 1 is the transmit key by default. <p>Note If you configure static WEP with MIC or CMIC, the access point and associated client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on the access point and the clients.</p> <p>Note Using security features such as authenticated key management can limit WEP key configurations. See the “WEP Key Restrictions” section on page 10-5 for a list of features that impact WEP keys.</p>
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 or CMIC	Access point and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both access point and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

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	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
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 and WEP

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio { 0 1 }</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<code>encryption</code> <code>[vlan <i>vlan-id</i>]</code> <code>mode ciphers</code> <code>{[aes-ccm ckip cmic ckip-cmic </code> <code>tkip]} {[wep128 wep40]}</code>	<p>Enable a cipher suite containing the WEP protection you need. Table 10-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure.</p> <ul style="list-style-type: none"> (Optional) Select the VLAN for which you want to enable WEP and WEP features. Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. <p>Note If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher.</p> <p>Note If you configure <code>ckip</code>, <code>cmic</code>, or <code>ckip-cmic</code>, you must also enable Aironet extensions. The command to enable Aironet extensions is <code>dot11 extension aironet</code>.</p> <p>Note You can also use the <code>encryption mode wep</code> command to set up static WEP. However, you should use <code>encryption mode wep</code> only if no clients that associate to the access point are capable of key management. See the <i>Cisco IOS Command Reference for Cisco Access Points and Bridges</i> for a detailed description of the <code>encryption mode wep</code> command.</p> <p>Note When you configure the cipher TKIP (not <code>TKIP + WEP 128</code> or <code>TKIP + WEP 40</code>) 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.</p>
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

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

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

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
ap1200(config-if)# exit
```

Matching Cipher Suites with WPA and 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	<ul style="list-style-type: none"> • 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
WPA	<ul style="list-style-type: none"> • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40



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.

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. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

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 <i>seconds</i> [<i>vlan vlan-id</i>] [membership-termination] [capability-change]	Enable broadcast key rotation. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> – 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. <p>See Chapter 11, “Configuring Authentication Types,” for detailed instructions on enabling authenticated key management.</p>
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
```