Configuring Encryption Types

This chapter describes how to configure the encryption types required to use WPA authenticated key management, Wired Equivalent Privacy (WEP), AES-CCM, Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. This chapter contains these sections:

Understand Encryption Types

This section describes how encryption types 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 encryption is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

One type ofwireless encryption is Wired Equivalent Privacy (WEP). 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 6, “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). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable encryption 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 AES-CCM 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.
- WEP—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
- 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 6-6 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.

Configure Encryption Types

These sections describe how to configure encryption, such as WEP, AES-CCM, and and broadcast key rotation:

- Creating WEP Keys, page 5-3
- Creating Cipher Suites, page 5-5
- Enabling and Disabling Broadcast Key Rotation, page 5-7

Note All encryption types 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 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 is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
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 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. **Note** Using security features such as authenticated key management can limit WEP key configurations. See the "WEP Key Restrictions" section on page 5-4 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:

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

WEP Key Restrictions

Table 5-1 lists WEP key restrictions based on your security configuration.

Table 5-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
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

Table 5-1 WEP Key Restrictions (continued)

Security Configuration	WEP Key Restriction
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
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 5-2 shows an example WEP key setup that would work for the access point and an associated device:

Table 5-2 WEP Key Setup Example

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

Creating Cipher Suites

Beginning in privileged EXEC mode, follow these steps to create 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** | **tkip**]} {[**wep128** | **wep40**]}	Enable a cipher suite containing the encryption you need. Table 5-3 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 WEP and WEP features. • Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. **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 and AES-CCM (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA 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 a cipher suite.

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

```
router# configure terminal
router(config)# interface dot11radio 0
router(config-if)# encryption vlan 22 mode ciphers aes-ccm wep128
router(config-if)# exit
```

Cipher Suites Compatible with WPA

If you configure your access point to use WPA authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 5-3 lists the cipher suites that are compatible with WPA.

Table 5-3 Cipher Suites Compatible with WPA

Authenticated Key Management Types	Compatible Cipher Suites
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 wep128 wep40 • encryption mode ciphers tkip wep128 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 VLANmust 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.

For a complete description of WPA and instructions for configuring authenticated key management, see the "Using WPA Key Management" section on page 6-6.

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 is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
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 6, "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:

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

Security Type in Universal Client Mode

Security

In universal client mode, the security type must be configured exactly as that of the access point it is associating to. For example, if the access point is configured with AES and TKIP encryption, the universal client must also have AES+TKIP in order for the devices to associate properly.

- TKIP
- AES
- TKIP+AES
- WEP 40-bit
- WEP 128-bit

Universal client configuration

```
!
dot11 ssid test10
   authentication open
   authentication key-management wpa
   wpa-psk ascii 7 11584B5643475D5B5C737B
!
!
interface Dot11Radio0/1/0
 ip address dhcp
 !
 encryption mode ciphers aes-ccm
 !
 ssid test10
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role non-root
!
End
```

The access point is configured with AES+TKIP WPA-PSK encryption. The universal client will display the following system message when there is a mismatch in the encryption types during association between the AP and the universal client:

```
%DOT11-4-CANT_ASSOC: Interface Dot11Radio0/1/0, cannot associate: WPAIE invalid multicast
suite exp=0x0050F204 act=0x0050F202
```

In this example, the universal client would have the multicast suite of 0x0050F204 (for TKIP) but instead received the multicast suite of 0x0050F202 (for AES+ TKIP). Here are the different scenarios:

- If the universal client is configured for AES WPAv2 (encryption mode ciphers aes-ccm), the access point must be configured for AES WPAv2. The universal client will associate with AES encryption.
- If the universal client is configured for TKIP (encryption mode ciphers tkip) The access point must be configured for either 1. TKIP WPA or 2. TKIP+AES. The universal client will associate with TKIP encryption.
- If the universal client is configured for AES+TKIP (encryption mode ciphers tkip aes) The access point must be configured for TKIP+AES. The universal client will associate with AES encryption.
- If the access point is configured for AES WPAv2 WPAv2 (encryption mode ciphers aes-ccm), and the universal client is configured with TKIP+AES (encryption mode ciphers aes-ccm tkip), you will get a system message stating the multicast suite was not found.

```
%DOT11-4-CANT_ASSOC: Interface Dot11Radio0/1/0, cannot associate: WPAIE not found and
required
```

Debugging

To determine if the universal client has associated to the access point, the user can issue the 'show dot11 association all' command for a detailed output of which access point it was associating to and how it has associated to the access point.

The "show dot11 association" command will have the following output:

```
c2801_uc#
c2801_uc#sh dot11 ass all
Address           : 0015.2b06.17d0     Name             : ap
IP Address        : 200.1.1.1          Interface        : Dot11Radio0/1/0
Device            : ap1200-Parent      Software Version : 12.3
CCX Version       : NONE

State             : Assoc              Parent           : Our Parent
SSID              : test10             VLAN             : 0
Hops to Infra     : 0                  Association Id   : 1
Tunnel Address    : 0.0.0.0
Key Mgmt type     : NONE               Encryption       : Off
Current Rate      : 54.0               Capability       : WMM ShortHdr ShortSlot
Supported Rates   : 1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Signal Strength   : -14  dBm           Connected for    : 236 seconds
Signal Quality    : N/A                Activity Timeout : 15 seconds
Power-save        : Off                Last Activity    : 0 seconds ago

Packets Input     : 2449               Packets Output   : 15
Bytes Input       : 451711             Bytes Output     : 4664
Duplicates Rcvd   : 3                  Data Retries     : 1
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0                  MIC Missing      : 0
Packets Redirected: 0                  Redirect Filtered: 0

c2801_uc#
```

Caveats

When the Cisco dot11radio is in the universal client mode and associates to a 3rd party access point, there are some additional caveats. The first is on the "show dot11 association" output. The "Device" area shows a result of "unknown" when associated to a 3rd party access point (non-Cisco). In the example below, a Cisco 876W universal client is associated to a Symbol 4131 Access Point. The "Software Version" and "Name" fields also result in "NONE". This is because the Cisco Aironet messages between Cisco devices carry this information and not between 3rd party and Cisco devices.

Example:

```
c876#sh dot11 assoc

802.11 Client Stations on Dot11Radio0:

SSID [symbol] :

MAC Address    IP address      Device        Name            Parent         State
00a0.f8dc.133a 192.168.1.4     unknown       -               -              Assoc

c876#sh dot11 ass all
Address           : 00a0.f8dc.133a     Name             : NONE
IP Address        : 192.168.1.4        Interface        : Dot11Radio0
Device            : unknown            Software Version : NONE
CCX Version       : NONE

State             : Assoc              Parent           : Our Parent
```

```
SSID              : symbol             VLAN              : 0
Hops to Infra     : -1                 Association Id    : 2
Tunnel Address    : 0.0.0.0
Key Mgmt type     : NONE               Encryption        : WEP
Current Rate      : 11.0               Capability        :
Supported Rates   : 1.0 2.0 5.5 11.0
Signal Strength   : -55  dBm           Connected for     : 39 seconds
Signal Quality    : N/A                Activity Timeout  : 15 seconds
Power-save        : Off                Last Activity     : 13 seconds ago

Packets Input     : 408                Packets Output    : 16
Bytes Input       : 46619              Bytes Output      : 3495
Duplicates Rcvd   : 2                  Data Retries      : 8
Decrypt Failed    : 0                  RTS Retries       : 0
MIC Failed        : 0                  MIC Missing       : 0
Packets Redirected: 0                  Redirect Filtered: 0

c876#
```