Cipher Suites and WEP

This module describes how to configure the cipher suites required for using Wireless Protected Access (WPA) and Cisco Centralized Key Management (CCKM); Wired Equivalent Privacy (WEP); and WEP features including Advanced Encryption Standard (AES), Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation.

This document contains the following sections:

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 frequency and listen to the signal, any wireless networking device within range of a wireless device, such as an access point, can receive the radio transmissions of a wireless device. WEP is the first line of defense against intruders, and we recommend that you use full encryption on your wireless network.

WEP encryption scrambles the data transmitted between wireless devices to keep the communication private. Wireless devices and their wireless client devices use the same WEP key to encrypt and decrypt data. WEP keys encrypt both unicast and multicast messages. (Unicast messages are addressed to one device on the network. Multicast messages are addressed to multiple devices on the network.)

Extensible Authentication Protocol (EAP) authentication, also known as 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 the *Authentication Types for Wireless Devices* module 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).

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cipher suites that contain TKIP provide the best security for your wireless LAN. 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*, Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (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 (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm that was originally designed to provide wireless LAN with the same level of privacy that is available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with little effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP. TKIP 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 of packet source and destination
  - An extension of IV space, to limit the need for rekeying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique which is 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 wireless device to generate the best possible random group key and to update all key-management-capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates.

Note Client devices that are using static WEP cannot use the wireless device when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices that are using 802.1x 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 wireless device.

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 3
- Enabling Cipher Suites and WEP, page 5
- Enabling and Disabling Broadcast Key Rotation, page 6

Creating WEP Keys

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

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

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface.
Step 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** {*40* | *128*} *encryption-key* [**0** | **7**] [**transmit-key**]	Defines a Wired Equivalent Privacy (WEP) key used for data encryption on the wireless LAN or on a specific VLAN. • (Optional) Select the VLAN for which you want to create a key. • Set the key slot where this WEP key resides. Up to 16 VLANs can be assigned. You can assign up to 4 WEP keys for each VLAN. • Set the size of the key, either 40-bit or 128-bit. The 40-bit keys contain 10 hexadecimal digits; the 128-bit keys contain 26 hexadecimal digits. • (Optional) Specify a static encryption key. For example, **11aa33bb55** for a 40-bit key. • (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. Using features such as authenticated key management or broadcast key rotation can restrict WEP key configurations. See the "WEP Key Restrictions" section on page 4 for a list of features that restrict WEP keys.
Step 4	**end**	Returns to privileged EXEC mode.

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

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

WEP Key Restrictions

Table 1 lists WEP key restrictions for various security configurations.

Table 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 slots 1 and 4.
Static WEP with MIC or CMIC	The associated wireless devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both the wireless device and the clients.
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys. Client devices using static WEP cannot use the wireless device 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 wireless device.

Example WEP Key Setup

Table 2 shows an example WEP key setup that would work for the wireless device and an associated wireless client devices.

Table 2 WEP Key Setup Example

Key Slot	Wireless Device		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 wireless device WEP key 1 is selected as the transmit key, associated device WEP key 1 must have the same contents. Associated device WEP key 4 is set, but because it is not set as the transmit key, WEP key 4 does not need to be set at all on the wireless device.

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

Enabling Cipher Suites and WEP

To enable a cipher suite, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface.
Step 3	**encryption** [**vlan** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	Enables a cipher suite containing the WEP protection you require. Table 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. If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher. 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 a wireless device are capable of key management. When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an service set identifier (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.
Step 4	**end**	Returns to privileged EXEC mode.

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

WEP, TKIP, and MIC are disabled by default.

This example configures a cipher suite for VLAN 22 that enables CKIP (unsupported), CMIC (unsupported), and 128-bit WEP:

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

Matching Cipher Suites with WPA and CCKM

If you configure your wireless device to use WPA or CCKM 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 WPA and CCKM.

Table 3 Cipher Suites Compatible with WPA and CCKM

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

Note When you configure 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 WPA or CCKM key management enabled.

Enabling and Disabling Broadcast Key Rotation

Broadcast key rotation is disabled by default.

Note Client devices that are using static WEP cannot exchange data with a wireless device 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 wireless device.

To enable broadcast key rotation, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** *radio-interface*	Enters interface configuration mode for the radio interface.

	Command	Purpose
Step 3	**broadcast-key change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	Configures the time interval between rotations of the broadcast encryption key. • Enter the number of seconds between rotations 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 wireless device changes and distributes the WPA group key. – Membership termination—the wireless device generates and distributes a new group key when any authenticated client device disassociates from the wireless device. 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 wireless device 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 wireless device.
Step 4	**end**	Returns to privileged EXEC mode.

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:

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.