



Cipher Suites and WEP

This document describes how to configure Wired Equivalent Privacy (WEP), Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES). This document contains these sections:

- [Understanding Cipher Suites and WEP, page 1](#)
- [Configuring Cipher Suites, page 2](#)

Understanding Cipher Suites and WEP

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 a bridge can receive the bridge's radio transmissions. Because WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

To keep the communication private, WEP encryption scrambles the radio communication between bridges. Communicating bridges 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 provides dynamic WEP keys to wireless devices. 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. By changing frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See "[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 command-line interface (CLI). Cipher suites that contain AES 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:



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

© 2008 Cisco Systems, Inc. All rights reserved.

- 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 (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 rekeying
- CKIP (Cisco Key Integrity Protocol)—The Cisco WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. (CKIP and CKIP-CMIC are supported only on the 2.4-GHz (802.11b/g) Cisco wireless mobile interface card (WMIC).)
- CMIC (Cisco Message Integrity Check)—Like TKIP, the Cisco message integrity check mechanism is designed to detect forgery attacks.

Configuring Cipher Suites

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

- [Configuring WEP, page 2](#)
- [Enabling Cipher Suite, page 5](#)

Encryption cipher suite and WEP are disabled by default.

Configuring WEP

Configuring WEP with 12.4(3)JK or Later Releases

Cisco 3201 WMICs with 12.4(3)JK or later release move encryption settings from the dot11 interface to each SSID configuration. Cisco 3202 WMIC and 3205WMIC supports this feature change starting 12.4(3)JL release.

To configure WEP encryptions, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	dot11 ssid <i>sample_ssid</i>	Enters SSID Configuration.

	Command	Purpose
Step 3	encryption key <i>1-4</i> size {40 128 } <i>encryption-key</i> [transmit-key]	Creates a WEP key for this SSID and sets its properties. <ul style="list-style-type: none"> Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN, but key slot 4 is reserved for the session key. Enter the key and 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) Set this key as the transmit key. The key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key for the transmit key in the same key slot on both root devices and non-root bridges.
Step 4	encryption mode wep { mandatory optional }	Sets WEP as the encryption mode for this VLAN.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot2 for SSID sample_ssid and sets the key as the transmit key:

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode mandatory
bridge(config-ssid)# encryption key 2 size 128 12345678901234567890123456 transmit-key
bridge(config-ssid)# end
```

Configuring WEP with 12.3(8)JK or Earlier Releases

To create a WEP key and 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 0	Enters interface configuration mode for the radio interface.
Step 3	encryption [vlan <i>vlan-id</i>] key <i>1-4</i> size {40 128 } <i>encryption-key</i> [transmit-key]	Creates 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, but key slot 4 is reserved for the session key. Enter the key and 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) Set this key as the transmit key. The key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key for the transmit key in the same key slot on both root devices and non-root bridges.

	Command	Purpose
Step 4	encryption [vlan <i>vlan-id</i>] mode wep { mandatory optional }	Sets WEP as the encryption mode for this VLAN.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 2 for VLAN 1 and sets the key as the transmit key:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(config-if)# encryption vlan 1 key 2 size 128 12345678901234567890123456
transmit-key
bridge(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 in slot 1.
LEAP or EAP authentication	Cannot configure a WEP transmit-key in 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 AES	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	Root devices and non-root bridges must use the same WEP key as the transmit key, and the key must be in the same key slot on both root devices and non-root bridges.

Example WEP Key Setup

Table 2 shows an example WEP key setup that would work for the root device and an associated non-root bridge.

Table 2 WEP Key Setup Example

Key Slot	Root Device		Associated Non-Root Bridge	
	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 root device's WEP key 1 is selected as the transmit key, WEP key 1 on the non-root bridge must have the same contents. WEP key 4 on the non-root bridge is set, but because it is not selected as the transmit key, WEP key 4 on the root device 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 root device and any non-root bridges with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled root device uses the key in slot 1 as the transmit key, a non-root bridge associated to the root device must use the same key in its slot 1, and the key in the non-root bridge's slot 1 must be selected as the transmit key.

Enabling Cipher Suite

Enabling Cipher Suite with 12.4(3)JK or Later Releases

Cisco 3201WMIC with 12.4(3)JK or later releases moves cipher settings from dot11 interface to each SSID configuration. Cisco 3202 WMIC and 3205 WMIC supports this feature change starting 12.4(3)JL release.

To configure cipher suite encryption, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	dot11 ssid sample_ssid	Enters SSID Configuration.

	Command	Purpose
Step 3	encryption mode ciphers {[aes-ccm ckip cmic ckip-cmic tkip]} {[wep128 wep40]}	<p>Enables a cipher suite containing the WEP protection you need. (Table 3 lists guidelines for selecting a cipher suite to match the type of authenticated key management you configure.)</p> <ul style="list-style-type: none"> Set the cipher options. <p>Note You can combine TKIP with 128-bit or 40-bit WEP.</p> <p>Note You can combine AES with TKIP. In this case, AES is the unicast cipher and TKIP becomes the group cipher.</p> <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 You can also use the encryption mode wep command to set up static WEP. However, you should use encryption mode wep only if none of the non-root bridges that associate to the root device 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 encryption mode wep command.</p> <p>Note When you configure TKIP-only, AES-only, or the combination of AES and TKIP (no WEP included) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you do not configure key management on the SSID, non-root bridge authentication fails on the SSID.</p> <p>Note Cisco Key Integrity Protocol (CKIP) and CKIP-Cisco Message Integrity Protocol (CMIP) are supported only on the 2.4-GHz (802.11b/g) WMIC.</p>
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

The following example sets up a cipher suite for SSID `sample_ssid` that enables CKIP, CMIC, and 128-bit WEP as the encryption mode:

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode ciphers ckip-cmic wep128
bridge(config-ssid)# end
```

The following example sets up a cipher suite for `ssid sample_ssid` that enables AES as the encryption mode:

```
bridge# configure terminal
bridge(config)# dot11 ssid sample_ssid
bridge(config-ssid)# encryption mode ciphers aes-ccm
bridge(config-ssid)# end
```

Enabling Cipher Suite with 12.3(8)JK or Earlier Releases

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 0	Enters interface configuration mode for the radio interface.
Step 3	encryption [vlan <i>vlan-id</i>] mode ciphers {[aes-ccm ckip cmic ckip-cmic tkip]} {[wep128 wep40]}	<p>Enables a cipher suite containing the WEP protection you need. (Table 3 lists guidelines for selecting a cipher suite to match 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. <p>Note You can combine TKIP with 128-bit or 40-bit WEP.</p> <p>Note You can combine AES with TKIP. In this case, AES is the unicast cipher and TKIP becomes the group cipher.</p> <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 You can also use the encryption mode wep command to set up static WEP. However, you should use encryption mode wep only if none of the non-root bridges that associate to the root device 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 encryption mode wep command.</p> <p>Note When you configure TKIP-only, AES-only, or the combination of AES and TKIP (no WEP included) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you do not configure key management on the SSID, non-root bridge authentication fails on the SSID.</p> <p>Note Cisco Key Integrity Protocol (CKIP) and CKIP-Cisco Message Integrity Protocol (CMIP) are supported only on the 2.4-GHz (802.11b/g) WMIC.</p>
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Saves 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 1 that enables CKIP, CMIC, and 128-bit WEP:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
```

```
bridge(config-if)# encryption vlan 1 mode ciphers ckip-cmic wep128
```

This example sets up a cipher suite for VLAN 1 that enables AES as the encryption mode:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode ciphers aes-ccm
bridge(config-if)# end
```

Matching Cipher Suites with WPA

If you configure your bridges 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
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 • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode ciphers aes-ccm
WPA	<ul style="list-style-type: none"> • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode aes-ccm • encryption mode aes-ccm wep128 • encryption mode aes-ccm wep40 • encryption mode aes-ccm tkip • encryption mode aes-ccm tkip wep128 • encryption mode aes-ccm tkip wep40



Note

When you configure TKIP-only cipher encryption (not TKIP + WEP128 or TKIP + WEP40) into SSID configuration, the SSID must be set to use WPA or CCKM key management. If you configure TKIP but you do not configure key management on the SSID, the authentication fails on this SSID.

For a complete description of WPA and CCKM and instructions for configuring authenticated key management, see the [“Authentication Types”](#) document.