



Configuring WEP and WEP Features

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

- [Understanding WEP, page 9-2](#)
- [Configuring WEP and WEP Features, page 9-2](#)

Understanding 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 an 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.

WEP encryption scrambles the radio communication between bridges to keep the communication private. 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. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See [Chapter 10, “Configuring Authentication Types,”](#) for detailed information on EAP and other authentication types.

Two additional security features defend your wireless network's WEP keys:

- Message Integrity Check (MIC)—MIC prevents attacks on encrypted packets called *bit-flip attacks*. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on associated bridges, adds a few bytes to each packet to make the packets tamper proof.
- TKIP (Temporal Key Integrity Protocol, also known as *WEP key hashing*)—This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.



Note

If VLANs are enabled on your bridges, WEP, MIC, and TKIP are supported only on the native VLAN.

Configuring WEP and WEP Features

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

- [Creating WEP Keys, page 9-2](#)
- [Enabling and Disabling WEP and Enabling TKIP and MIC, page 9-3](#)

WEP, TKIP, and MIC are disabled by default.

Creating 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	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	encryption [vlan <i>vlan-id</i>] key 1-4 size { 40 128 } encryption-key [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. WEP, MIC, and TKIP are supported only on the native VLAN. 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. 40-bit keys contain 10 hexadecimal digits; 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 as the transmit key in the same key slot on both root and non-root bridges.
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 2 for VLAN 1 and sets the key as the transmit key:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 key 2 size 128 12345678901234567890123456
transmit-key
bridge(config-if)# end
```

Enabling and Disabling WEP and Enabling TKIP and MIC

Beginning in privileged EXEC mode, follow these steps to enable WEP, TKIP, and MIC:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	encryption [vlan <i>vlan-id</i>] mode wep { optional [key-hash] mandatory [mic] [key-hash]}	<p>Enable WEP, MIC, and TKIP.</p> <ul style="list-style-type: none"> (Optional) Select the VLAN for which you want to enable WEP and WEP features. Set the WEP level and enable TKIP and MIC. If you enter optional, another bridge can associate to the bridge with or without WEP enabled. You can enable TKIP with WEP set to optional but you cannot enable MIC. If you enter mandatory, other bridges must have WEP enabled to associate to the bridge. You can enable both TKIP and MIC with WEP set to mandatory. <p>Note If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non-root bridges.</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 WEP or to disable WEP features.

This example sets WEP to mandatory for VLAN 1 and enables MIC and TKIP.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode wep mandatory mic key-hash
bridge(config-if)# end
```