Securing a Wireless LAN

This module describes how to apply strong wireless security mechanisms on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point (AP), to ensure that a wireless LAN is protected against unauthorized access and eavesdropping.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Securing a Wireless LAN, on page 34.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Securing a Wireless LAN

The following prerequisites apply to securing a wireless LAN:

- Read the "Wireless LAN Overview" module.
- Read the "Configuring a Basic Wireless LAN Connection" module.

Information About Securing a Wireless LAN

Wired Equivalent Privacy in a Wireless LAN

The first, most basic level of a secure wireless LAN is the presence of a Wired Equivalent Privacy (WEP) key. The WEP key is unique to the client and provides the client with the appropriate level of network access. WEP keys encrypt both unicast and multicast messages. Because WEP is the first line of defense against intruders, we recommend that you use full encryption on your wireless network.

WEP Weaknesses

WEP is vulnerable to attack for several reasons:

- Distributing WEP keys manually is a time-intensive, laborious task. Because it is tedious to manually rekey the WEP code, the keys are not likely to change frequently. Therefore, an attacker probably has enough time to decipher the key.
- When keys are not changed often, attackers can compile so-called *decryption dictionaries* . These are huge collections of frames, encrypted with the same key. These frames can then be analyzed and used for attack.
- Standardized WEP implementations use 64- or 128-bit shared keys. Although the 128-bit key sounds excessively durable, it is still possible to crack a key this size within a short interval with sustained traffic.
- WEP uses Rivest Cipher 4 (RC4) for encryption. Of all the possible RC4 keys, the statistics for the first few bytes of output are nonrandom, which can provide information about the key.

Note RC4 is the most widely used software stream cipher. In addition to WEP, it is used in Secure Socket Layer (SSL), the encryption medium used for web pages. Although widely deployed and adequate for web use, it is generally not considered a good means of encryption for WLANs.

Wi-Fi Protected Access in a Wireless LAN

Wi-Fi Protected Access (WPA) was designed as a more secure replacement for WEP. The Temporal Key Integrity Protocol (TKIP), also known as *WEP key hashing* , is an improvement over WEP. It causes keys to automatically change, and when used in conjunction with a larger initialization vector (IV), it makes discovering keys highly unlikely.

Note An IV is a block of bits added to the first block of data of a block cipher. This block is added--or hashed--with the base key and is used with other types of ciphers. This block strengthens security because the same transmissions with the same key yield the same output. As a result, attackers can notice the similarities and derive both the messages and the keys being used.

In addition to improving authentication and encryption, WPA secures the payload better than in WEP. With WEP, cyclic redundancy checks (CRC) are used to ensure packet integrity. However, it is possible to alter the payload and update the message CRC without knowing the WEP key because the CRC is not encrypted. WPA uses Message Integrity Check (MIC) to ensure packet integrity. The MICs also employ a frame counter, which prevents replay attacks.

Note A replay attack occurs when an intruder intercepts an encrypted transmission, and then rebroadcasts that transmission at a later time. For example, if a password is intercepted, the attacker need not know how to read the message; the attacker can simply rebroadcast it later, and then gain access using the victim's credentials.

Breaking into a WLAN that uses WPA is more difficult than breaking into one that uses WEP because the IVs are larger, there are more keys in use, and there is a sturdier message verification system.

WPA 2 is the next generation of Wi-Fi security. WPA 2 is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 implements the Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

Note CCMP is also referred to as CBC-MAC.

WPA 2 offers a higher level of security than WPA because AES offers stronger encryption than Temporal Key Integrity Protocol (TKIP). TKIP is the encryption algorithm that WPA uses. WPA 2 creates fresh session keys on every association. The encryption keys that are used for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key. Security is enhanced with the use of a new and unique encryption key because there is no key reuse.

For more information on WPA 2, refer to Configuration of WPA/WPA2 with Pre-Shared Key.

Broadcast Key Rotation in a Wireless LAN

Extensible Authentication Protocol (EAP) authentication provides dynamic unicast WEP keys for client devices but uses static broadcast keys. When you enable broadcast key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Because broadcast key rotation is used to protect multicast traffic and TKIP is used to protect unicast traffic, they can be enabled at the same time on a wireless LAN. You should enable broadcast key rotation if you are running multicast applications on your wireless LAN.

Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Only wireless client devices using 802.1x authentication, such as Lightweight Extensible Authentication Protocol (LEAP), EAP with Transport Layer Security (EAP-TLS), or Protected Extensible Authentication Protocol (PEAP), can use the access point when you enable broadcast key rotation.

Types of Access Point Authentication

This section describes the authentication types that you can configure to the access point. The authentication types correspond to the SSIDs that you configure for the access point. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 18 section for instructions on how to configure multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, authentication types that rely on an authentication server on your network.

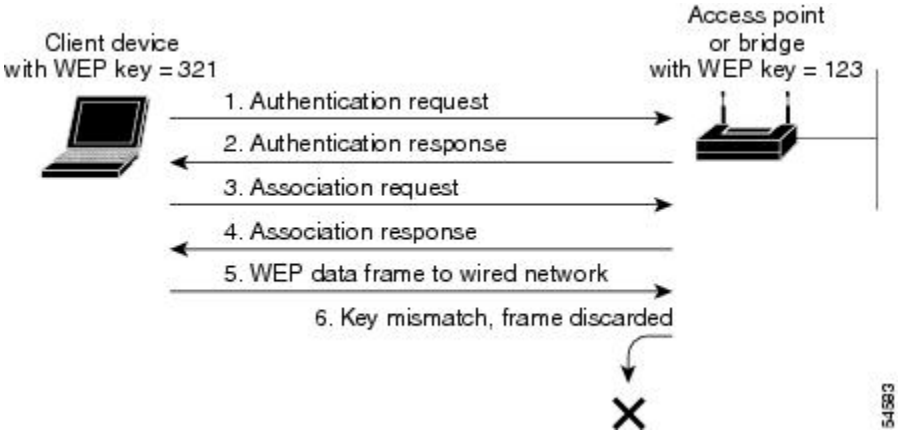
The access point uses four authentication mechanisms or types and can use more than one at the same time. The following sections explain each authentication type:

Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. If encryption is enabled, any wireless device using open authentication can authenticate to the access point, but the device can communicate only if its WEP keys match the access point's. Open authentication with no encryption is normally used for guest access. Any wireless client can communicate with the AP if open authentication and no encryption are configured. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

The figure below shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 1: Sequence for Open Authentication



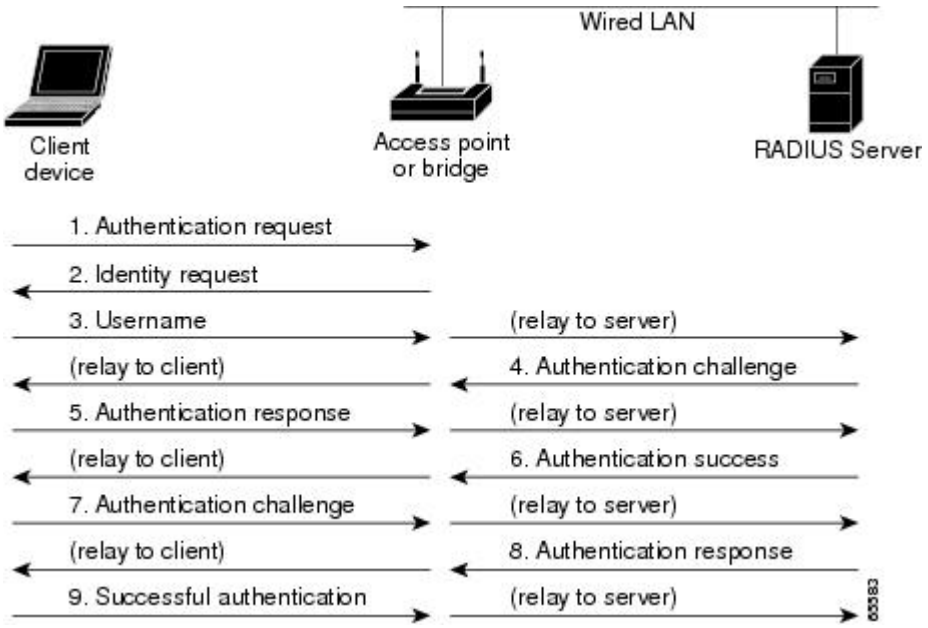
EAP Authentication to the Access Point

EAP provides the highest level of security for a wireless network. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

EAP 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 a network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in the figure below.

Figure 2: Sequence for EAP Authentication



In Steps 1 through 9 in EAP Authentication to the Access Point, on page 5, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the login session.

During the login session, the RADIUS server encrypts and sends the WEP key, called a session key, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: It relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device.

To set up EAP authentication on the access point, see the Separating a Wireless Network by Configuring Multiple SSIDs, on page 18 task.

Note If you use EAP authentication, you can select open or shared key authentication, but you need not. EAP authentication controls authentication both to your access point and to your network.

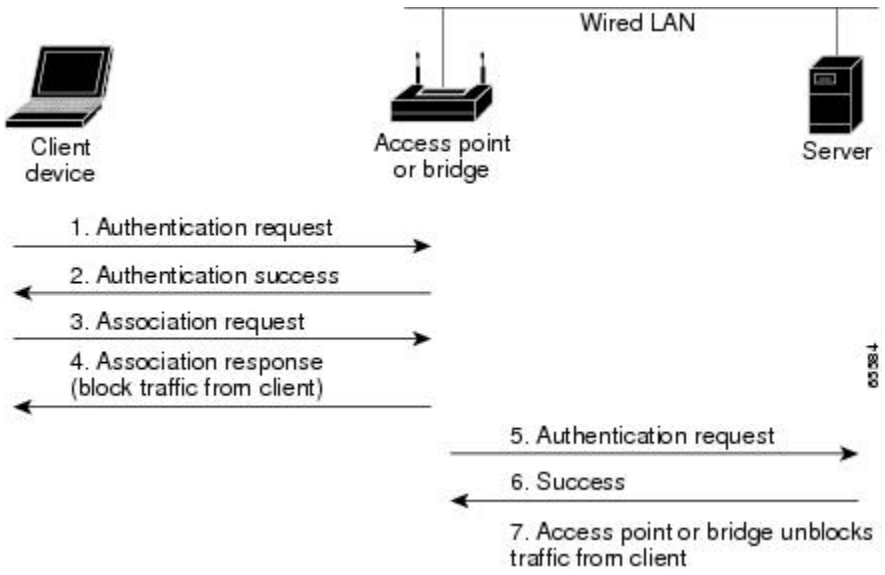
MAC Address Authentication to the Access Point

The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server compares the address to a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 18 section for instructions on enabling MAC-based authentication.

If you do not have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point. Devices with MAC addresses not on the list are not allowed to authenticate. When you create the list of allowed MAC addresses, use lowercase for all letters in the addresses that you enter.

The figure below shows the authentication sequence for MAC-based authentication.

Figure 3: Sequence for MAC-Based Authentication



MAC-Based EAP and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. See the "Assigning Authentication Types to SSIDs" section for instructions on setting up this combination of authentications.

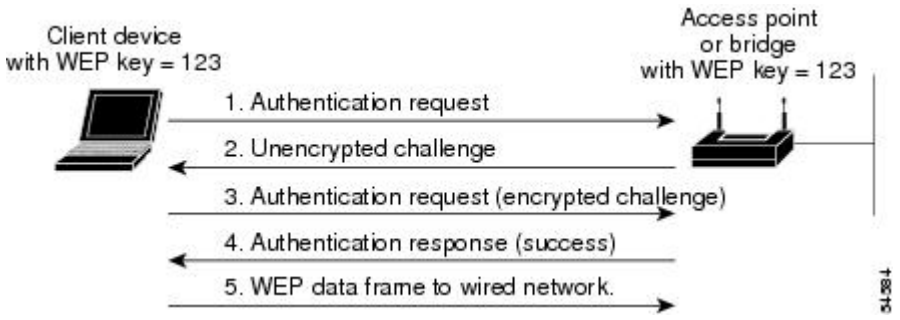
Shared Key Authentication to the Access Point

Note Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder that calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

The figure below shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 4: Sequence for Shared Key Authentication



Correspondence Between Access Point and Client Authentication Types

The authentication settings on the access point must match the authentication settings on the clients that associate to the access point. Refer to the installation guide for your wireless LAN client adapter for instructions on setting authentication types.

Note Some non-Cisco client adapters do not perform 802.1x authentication to the access point unless you configure open authentication with EAP. To allow both Cisco clients using LEAP and non-Cisco clients using LEAP to associate using the same SSID, it might be necessary to configure the SSID for both network EAP authentication and open authentication with EAP.

The table below lists the client and access point settings required for each authentication type.

Table 1: Client and Access Point Settings for Authentication

Authentication Type	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication.	Configure WEP and enable open authentication for the Service Set Identifier (SSID).
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication.	Configure WEP and enable shared key authentication for the SSID.
LEAP authentication	Enable LEAP on Cisco clients. Use the vendor authentication application for non-Cisco clients.	Configure WEP and enable network EAP for the SSID[1].
802.1x authentication	Enable EAP-TLS, PEAP MS-CHAP v2, or EAP-FAST.	Enable mandatory WEP. Enable open authentication with EAP for the SSID.
802.1x authentication and WPA	Enable any 802.1x authentication method and WPA.	Choose TKIP as the cipher suite and enable open authentication with EAP and/or network EAP for the SSID. You can enable network EAP authentication in addition to or instead of open authentication. To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA. If WPA is set as mandatory, TKIP is the only valid cipher suite. If WPA is set as optional, the only available ciphers are TKIP+WEP40 or TKIP+WEP128.
WPA-PSK authentication	Enable WPA-PSK and configure a preshared key.	Choose a cipher suite and enable open authentication and WPA for the SSID. Enter a WPA preshared key. To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS Authentication		

Authentication Type	Client Setting	Access Point Setting
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and choose Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP.	Configure WEP and enable open authentication with EAP for the SSID.
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP type.	Configure WEP and enable open authentication with EAP for the SSID.
PEAP Authentication		
If using Aironet Client Utility (ACU) to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and choose Enable network access control using IEEE 802.1X and PEAP as the EAP type in Windows 2000 (with Service Pack 3) or Windows XP.	Configure WEP and enable open authentication with EAP for the SSID.
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and PEAP as the EAP type.	Configure WEP and enable open authentication with EAP for the SSID.

[1] Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure open authentication with EAP. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both network EAP authentication and open authentication with EAP.

MAC Address and IP Filters on Access Point Interfaces

In addition to managing access to a WLAN through WEP keys or authentication, you can configure access to be restricted according to device; to do this, you use the MAC address or IP address. For example, you can employ filtering on your APs to keep out clients that do not have an authorized client adapter. Without an explicitly approved MAC address on the network adapter, it does not matter if the correct username and password are presented because the AP does not allow access.

Simply put, filtering checks a wireless client's MAC or IP address against a list of authorized MAC or IP addresses maintained on the access point. When a client tries to connect to the access point, it must be on the list. If it is not, the client cannot connect.

Filtering should not be the only security measure, however. Both MAC and IP addresses can be spoofed, thus circumventing this layer of security.

To configure filters, you use access control lists (ACLs) and bridge groups.

Note You can include filters in the access point's quality of service policies. Refer to the "Implementing Quality of Service in a Wireless LAN" module for detailed instructions on configuring QoS policies on an access point.

MAC Address Filters

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes or blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, you may need to attach to the AP using a console, disable the filters, then correct each filter accordingly.

Note Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point reboots, or when the clients associate with another access point.

IP Filters

You can limit access to your AP with IP filters. IP filters can be applied based on IP address, IP protocol, and IP port. IP filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Note If you create an IP filter and intend to block traffic to all IP addresses except those specified, make sure you include the IP address of your own computer in the list of specified exceptions; otherwise, your computer is shut out from the access point.

How to Secure a Wireless LAN

Configuring WEP Encryption and Key Management Features

Perform this task to configure WEP encryption and additional key management features, such as MIC, TKIP, and broadcast key rotation.

Configure static WEP keys only if the access point must 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.

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

Before You Begin

Determine if all the clients that will associate to the access point are capable of key management. If they are, use the **encryption mode ciphers** command rather than the **encryption mode wep** command to configure WEP. See the relevant command pages in the Cisco IOS Wireless LAN Command Reference for more details.

Note The table below lists WEP key restrictions based on your security configuration.

Table 2: 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 transmit 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 transmit 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **encryption** [**vlan** *vlan-id*] **mode wep**[**mandatory** | **optional**]
5. **encryption** [**vlan** *vlan-id*] **key** *number* **size** {**40bit** | **128bit**} [**0** | **7**] *encryption-key* [**transmit-key**]
6. **encryption** [**vlan** *vlan-id*] **mode ciphers {aes-ccm tkip}**[**wep128** | **wep40**]
7. **broadcast-key** [**vlan** *vlan-id*][**change** *seconds*] [**membership-termination**] [**capability-change**]
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.
Step 4	**encryption** [**vlan** *vlan-id*] **mode wep**[**mandatory**	**optional**] **Example:** `Router(config-if)# encryption vlan 1 mode wep`	Enables WEP encryption on the wireless LAN or a specific VLAN.
Step 5	**encryption** [**vlan** *vlan-id*] **key** *number* **size** {**40bit**	**128bit**} [**0**	**7**] *encryption-key* [**transmit-key**]	Defines the WEP key used for data encryption on the wireless LAN or on a specific VLAN. • When you have configured the encryption key for static WEP clients, skip to Step 8.

	Command or Action	Purpose
	Example: `Router(config-if)# encryption vlan 1 key 1 size 40bit 11aa33bb55 transmit-key`	
Step 6	**encryption** [**vlan** *vlan-id*] **mode ciphers** {**aes-ccm tkip**}[**wep128** | **wep40**] **Example:** `Router(config-if)# encryption vlan 10 mode ciphers tkip wep40`	Enables WEP encryption and a cipher suite that contains Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Code Protocol (AES-CCMP) or TKIP, which provides better security for your wireless LAN. • When you configure the TKIP cipher 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 TKIP cipher without enabling WPA key management. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 18 section for more information on configuring WPA.
Step 7	**broadcast-key** [**vlan** *vlan-id*][**change** *seconds*] [**membership-termination**] [**capability-change**] **Example:** `Router(config-if)# broadcast key vlan 10 change 300`	(Optional) Enables broadcast key rotation--the time interval between rotations of the broadcast encryption key used for clients. • Client devices using static WEP cannot access the access point 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 when you enable broadcast key rotation.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you have configured encryption, configure authentication mechanisms as shown in the Controlling Access to a Wireless Network by Using Authentication Mechanisms, on page 15 section.

Controlling Access to a Wireless Network by Using Authentication Mechanisms

In a wireless network, you need to ascertain the identity of the users and devices using authentication mechanisms. This is important because access control is established depending on the user's identity.

Perform this task to configure authentication mechanisms.

Before You Begin

The following prerequisites apply to using authentication mechanisms:

- If you are going to use 802.1*x* authentication mechanisms (for example, network EAP), an EAP-compatible RADIUS server must be configured and accessible in the network to provide AAA services.
- If you are going to use MAC address or EAP authentication, you need to define the MAC and EAP address lists using the **aaa authentication login** command, which can be found in the *Cisco IOS Security Command Reference* , Release 12.4T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **authentication open [mac-address** *list-name* **] [eap** *list-name* **]**
5. **authentication shared [mac-address** *list-name* **] [eap** *list-name* **]**
6. **authentication network-eap** *list-name* **[mac-address** *list-name* **]**
7. **authentication key-management wpa** [**optional**]
8. **exit**
9. **interface dot11Radio** *interface*
10. **ssid** *name*
11. **end**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid anyname`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • The SSID is inactive until you use the ssid command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**authentication open [mac-address** *list-name* **] [eap** *list-name* **]** **Example:** `Router(config-ssid)# authentication open`	(Optional) Sets the authentication type to open for this SSID. • The **mac-address** keyword sets the SSIDs authentication type to open with MAC address authentication. This requires all clients to perform MAC address authentication before joining the network. • The **eap** keyword sets the SSIDs authentication type to open with EAP authentication. The AP requires all clients to perform EAP authentication before joining the network. • For the *list-name* argument, specify the authentication method list.
Step 5	**authentication shared [mac-address** *list-name* **] [eap** *list-name* **]** **Example:** `Router(config-ssid)# authentication shared mac-address mac-list1`	(Optional) Sets the authentication type for this SSID to shared key. • The **mac-address** keyword sets the SSID's authentication type to shared key with MAC address authentication. For the *list-name*argument, specify the authentication method list. • The **eap** keyword sets the SSID's authentication type to shared key with EAP authentication. • For the *list-name*argument,specify the authentication method list. **Note** Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.
Step 6	**authentication network-eap** *list-name* **[mac-address** *list-name* **]** **Example:** `Router(config-ssid)# authentication network-eap list1`	(Optional) Sets the authentication type for this SSID to Network-EAP. • This command is used to authenticate an EAP client with an EAP-compatible RADIUS server. • The SSID's authentication type can be altered so that it also requires MAC address authentication. For the *list-name* argument, specify the authentication method list.
Step 7	**authentication key-management wpa** [**optional**]	(Optional) Sets the authentication type for the SSID to WPA.

	Command or Action	Purpose
	Example: `Router(config-ssid)# authentication key-management wpa`	• If you use the **optional** keyword, clients that do not use WPA are allowed to use the SSID. However, if **optional** is not used, clients must use WPA to connect. • To enable WPA for an SSID, you must also enable open authentication, network EAP, or both.
Step 8	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode.
Step 9	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.
Step 10	**ssid** *name* **Example:** `Router(config-if)# ssid anyname`	Creates an SSID and enters SSID configuration mode. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters.
Step 11	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 12	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you configure authentication mechanisms, you can configure authentication timeouts and reauthentication periods on the access point by completing the optional task in the Configuring Authentication Timeouts and Reauthentication Periods, on page 20 section.

Separating a Wireless Network by Configuring Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. You can configure up to 10 SSIDs on the Cisco 800 and 1800 series fixed-configuration routers and up to 16 SSIDs on the Cisco 1800 modular, 2800, and 3800 series routers and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs.

These are the settings you can assign to each SSID:

- VLAN--You can use VLANs to configure different security features for each user or group in the wireless network. For example, users in VLAN 1 may be forced to use MAC authentication while users in VLAN 2 do not have that requirement.
- Client authentication method--You can apply separate authentication methods to different user groups on the wireless network.
- Guest mode--If you want an access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. The access point's default SSID is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID on most access points.
- Repeater mode, including authentication username and password--If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

Note If your network uses VLANs, you must assign, or bind, each SSID to an individual VLAN. Client devices using the SSID are grouped in that VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **vlan** *vlan-id*
5. **exit**
6. **interface dot11Radio** *interface*
7. **ssid** *name*
8. Repeat Step 2 through Step 7 for each SSID you want to create.
9. **end**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid floor2`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • The SSID is inactive until you use the ssid command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**vlan** *vlan-id* **Example:** `Router(config-ssid)# vlan 1`	Assigns the SSID to a VLAN on your network. • Client devices that associate using the SSID are grouped into this VLAN. • The *vlan-id* argument range is from 1 to 4095.
Step 5	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode and returns to global configuration mode.
Step 6	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.
Step 7	**ssid** *name* **Example:** `Router(config-if)# ssid floor2`	Creates an SSID and enters SSID configuration mode. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length.

	Command or Action	Purpose
Step 8	Repeat Step 2 through Step 7 for each SSID you want to create.	--
Step 9	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you have configured the SSIDs, configure authentication mechanisms by completing the task in the Controlling Access to a Wireless Network by Using Authentication Mechanisms, on page 15 section.

Configuring Authentication Timeouts and Reauthentication Periods

Perform this task to configure authentication timeouts and reauthentication periods for client devices authenticating through your access point.

This task is optional and can be used only if 802.1*x* authentication is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **dot1x client-timeout** *seconds*
5. **dot1x reauth-period {** *seconds* **| server}**
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.
Step 4	**dot1x client-timeout** *seconds* **Example:** `Router(config-if)# dot1x client-timeout 120`	Specifies the length of time, in seconds, the access point waits for a reply from a client attempting to authenticate before the authentication fails.
Step 5	**dot1x reauth-period {** *seconds* **| server}** **Example:** `Router(config-if)# dot1x reauth-period 120`	Specifies the length of time, in seconds, the access point waits before forcing an authenticated client to reauthenticate. • Use the server keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for Securing a Wireless LAN

Configuring an Access Point in Bridging Mode with Open Authentication and Static WEP Encryption Example

The following configuration example shows how to:

- Configure a Cisco 3800 series access point in bridging mode with open authentication and static WEP encryption.
- Define a bridge group and assign it to the radio interface and a VLAN interface.
- Create a bridge virtual interface (BVI) and assign an IP address to that interface.

- Save the new entries in the configuration file.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open
 exit
 interface dot11Radio 0/0/0
 encryption mode wep mandatory
 encryption key 1 size 40bit 11aa33bb55
 ssid ssid1
 exit
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 copy running-config startup-config
```

Configuring an Access Point in Bridging Mode with WPA-PSK Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with authenticated key management and encryption that uses a cipher suite that contains TKIP and a WPA preshared key.
- Define a bridge group and assign it to the radio interface and a VLAN interface.

- Create a BVI and assign an IP address to that interface.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open
 authentication key-management wpa
 wpa-psk ascii shared-key-name
 exit
 interface dot11Radio 0/3/0
 encryption mode ciphers tkip
 ssid ssid1
 exit
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 copy running-config startup-config
```

Configuring an Access Point in Bridging Mode with MAC Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with open authentication and MAC authentication using a local MAC address list.
- Define a bridge group and assign it to the radio interface and a VLAN interface.
- Create a BVI and assign an IP address to that interface.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 exit
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 configure terminal
 username 000011111111 password 000011111111
 aaa new-model
 aaa authentication login maclist1 local
 end
 copy running-config startup-config
```

This example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with open authentication and MAC authentication using a MAC address list located on an external RADIUS server.
- Define a bridge group and assign it to the radio interface and a VLAN interface.
- Create a BVI and assign an IP address to that interface.

- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 exit
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 configure terminal
 aaa new-model
 ip radius source-interface bvi 1
 radius-server host 11.2.0.1 auth-port 1812 acct-port 1813 key sharedsecret
 aaa group server radius rad_mac
 server 11.2.0.1 auth-port 1812 acct-port 1813
 exit
 aaa authentication login maclist1 group rad_mac
 end
 copy running-config startup-config
```

Configuring an Access Point in Bridging Mode with 802.1x Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with 802.1*x* (network EAP) authentication.
- Define a bridge group and assign it to the radio interface and VLAN interface.
- Create a BVI and assign an IP address to that interface.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication network-eap eaplist1
 authentication open eap eaplist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 exit
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with Open Authentication and Static WEP Encryption Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with open authentication and static WEP encryption.
- Assign an IP address to the radio interface.
- Create an SSID for the access point.
- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 encryption mode wep mandatory
 encryption key 1 size 40bit 11aa33bb55
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with WPA-PSK Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with authenticated key management and encryption that uses a cipher suite that contains TKIP and a WPA preshared key.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication key-management wpa
 wpa-psk ascii shared-key-name
 authentication open
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 encryption mode ciphers tkip
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with MAC Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with MAC authentication using a local list.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 configure terminal
 username 000011111111 password 000011111111
 aaa new-model
 aaa authentication login maclist1 local
 end
 copy running-config startup-config
```

This example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with MAC authentication using a MAC address list located on an external RADIUS server.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid2
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 configure terminal
 aaa new-model
 ip radius source-interface bvi 1
 radius-server host 11.2.0.1 auth-port 1812 acct-port 1813 key sharedsecret
 aaa group server radius rad_mac
 server 11.2.0.1 auth-port 1812 acct-port 1813
 exit
 aaa authentication login maclist1 group rad_mac
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with 802.1x Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with 802.1*x* (network EAP) authentication.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open eap eaplist1
 authentication network-eap eaplist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Where to Go Next

- If you are using a RADIUS server in your wireless LAN for AAA services, or you need to configure an access point to serve as a local authenticator, see the "Configuring RADIUS or a Local Authenticator in a Wireless LAN" module.
- If you want to configure quality of service (QoS) settings on an access point, see the "Implementing Quality of Service in a Wireless LAN" module.
- If you want to configure wireless VLANs, see the "Configuring Wireless VLANs" module.

Additional References

The following sections provide references related to securing a wireless LAN.

Related Documents

Related Topic	Document Title
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Wireless LAN Command Reference
Cisco IOS security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Securing a Wireless LAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 3: Feature Information for Securing a Wireless LAN

Feature Name	Releases	Feature Information
Advanced Encryption Standard (AES) - CCMP	12.4(15)T	AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is a superior to WEP encryption and is defined in the IEEE 802.11i standard.
Broadcast Key Rotation	12.4T	This feature allows a user to set a timeout for the shared broadcast key.
IEEE 802.11 Wireless Standards Support	12.4T	This feature provides support for 802.11 standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11a Support	12.4T	This feature provides support for 802.11a standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11b Support	12.4T	This feature provides support for 802.11b standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11g Support	12.4T	This feature provides support for 802.11g standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
MAC Address Local Authentication	12.4T	This feature provides support for MAC authentication of users on an access point.

Feature Name	Releases	Feature Information
Multiple SSIDs	12.4T	This feature allows a user to configure up to 10 SSIDs on the Cisco 800 and 1800 series fixed-configuration routers and up to 16 SSIDs on the Cisco 1800 modular, 2800, and 3800 series routers and assign different configuration settings to each SSID.
Wi-Fi Protected Access (WPA)	12.4T	This feature provides support for wireless fidelity protected access, which is a standards-based, interoperable security enhancement that greatly increases the level of data protection and access control for existing and future wireless LAN systems.