



## Configuring Authentication Types

---

This chapter describes how to configure authentication types on the access point/bridge. This chapter contains these sections:

- [Understanding Authentication Types, page 10-2](#)
- [Configuring Authentication Types, page 10-9](#)
- [Matching Authentication Types on Root and Non-Root Access Point/Bridges, page 10-15](#)

# Understanding Authentication Types

This section describes the authentication types that you can configure on the access point/bridge. The authentication types are tied 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 [Chapter 4, “Configuring Multiple SSIDs,”](#) for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point/bridge, 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.



## Note

By default, the access point/bridge sends reauthentication requests to the authentication server with the service-type attribute set to `authenticate-only`. However, some Microsoft IAS servers do not support the `authenticate-only` service-type attribute. Changing the service-type attribute to `login-only` ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **`dot11 aaa authentication attributes service-type login-only`** global configuration command to set the service-type attribute in reauthentication requests to `login-only`.

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

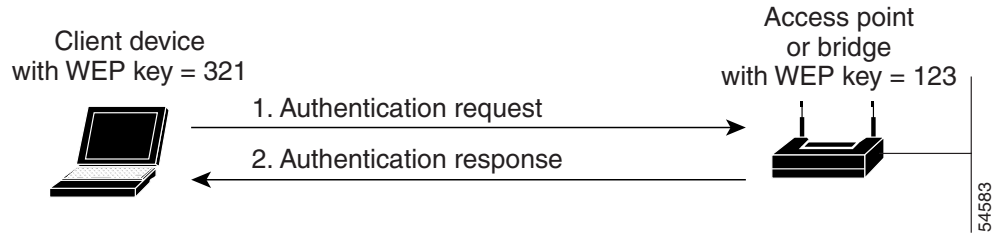
- [Open Authentication to the Access Point/Bridge, page 10-2](#)
- [Shared Key Authentication to the Access Point/Bridge, page 10-3](#)
- [EAP Authentication to the Network, page 10-4](#)
- [MAC Address Authentication to the Network, page 10-5](#)
- [Combining MAC-Based, EAP, and Open Authentication, page 10-6](#)
- [Using CCKM for Authenticated Clients, page 10-6](#)
- [Using WPA Key Management, page 10-7](#)
- [Software and Firmware Requirements for WPA and WPA-TKIP, page 10-9](#)
- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-14](#)

## Open Authentication to the Access Point/Bridge

Open authentication allows any 1300 series access point/bridge to authenticate and then attempt to communicate with another 1300 series access point/bridge. Using open authentication, a non-root access point/bridge can authenticate to a root access point/bridge, but the non-root access point/bridge can communicate only if its WEP keys match the root access point/bridge's. An access point/bridge that is not using WEP does not attempt to authenticate with an access point/bridge that is using WEP. Open authentication does not rely on a RADIUS server on your network.

[Figure 10-1](#) shows the authentication sequence between a non-root access point/bridge trying to authenticate and a root access point/bridge using open authentication. In this example, the device's WEP key does not match the access point/bridge's key, so it can authenticate but not pass data. The same scenario occurs when a client attempts to associate to the access point/bridge configured as an a root access point or repeater access points with clients.

Figure 10-1 Sequence for Open Authentication



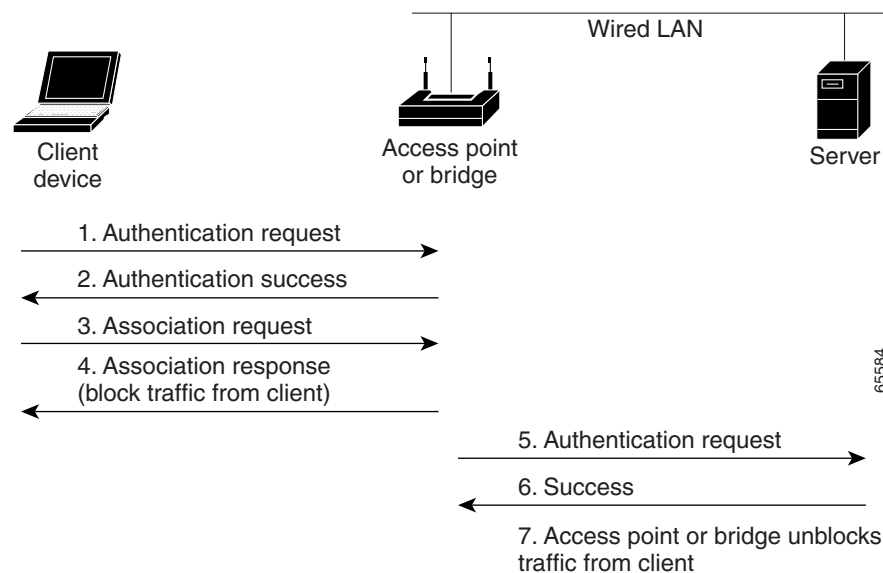
## Shared Key Authentication to the Access Point/Bridge

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 root access point/bridge sends an unencrypted challenge text string to other access point/bridges attempting to communicate with the root access point/bridge. The access point/bridge requesting authentication encrypts the challenge text and sends it back to the root access point/bridge. If the challenge text is encrypted correctly, the root access point/bridge allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the root access point/bridge open to attack from an intruder who 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.

Figure 10-2 shows the authentication sequence between a device trying to authenticate and an access point/bridge using shared key authentication. In this example the device’s WEP key matches the access point/bridge’s key, so it can authenticate and communicate. The same sequence occurs when the bridge is configured as a root access point or repeater access point with clients.

Figure 10-2 Sequence for Shared Key Authentication

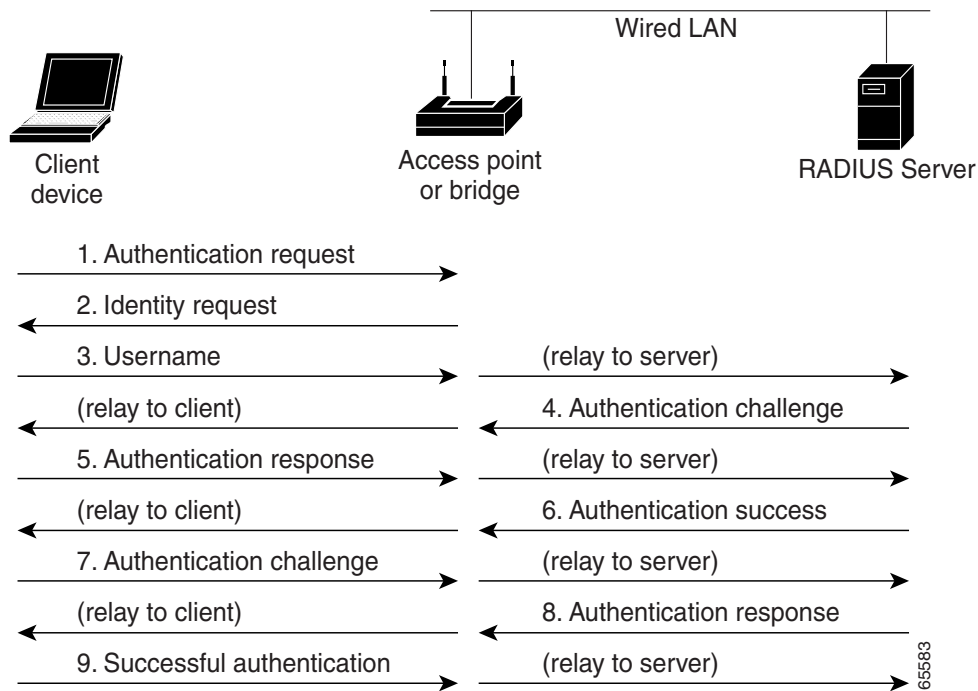


# EAP Authentication to the Network

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

When you enable EAP on your access point/bridges, authentication to the network occurs in the sequence shown in [Figure 10-3](#):

**Figure 10-3** Bridge Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 10-3](#), a non-root access point/bridge or wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root access point/bridge. The RADIUS server sends an authentication challenge to the non-root access point/bridge or client. The non-root access point/bridge 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 non-root access point/bridge or client. When the RADIUS server authenticates the non-root access point/bridge, the process repeats in reverse, and the non-root access point/bridge or client authenticates the RADIUS server.

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

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the root access point/bridge. The root access point/bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root access point/bridge, which uses the session key to decrypt it. The non-root access point/bridge and the root access point/bridge 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/bridge 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. See the [“Assigning Authentication Types to an SSID” section on page 10-10](#) for instructions on setting up EAP on the access point/bridge.

**Note**

---

If you use EAP authentication, you can select open or shared key authentication, but you don't have to. EAP authentication controls authentication both to your access point/bridge and to your network.

---

## MAC Address Authentication to the Network

The access point/bridge relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against 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 [“Assigning Authentication Types to an SSID” section on page 10-10](#) for instructions on enabling MAC-based authentication.

**Tip**

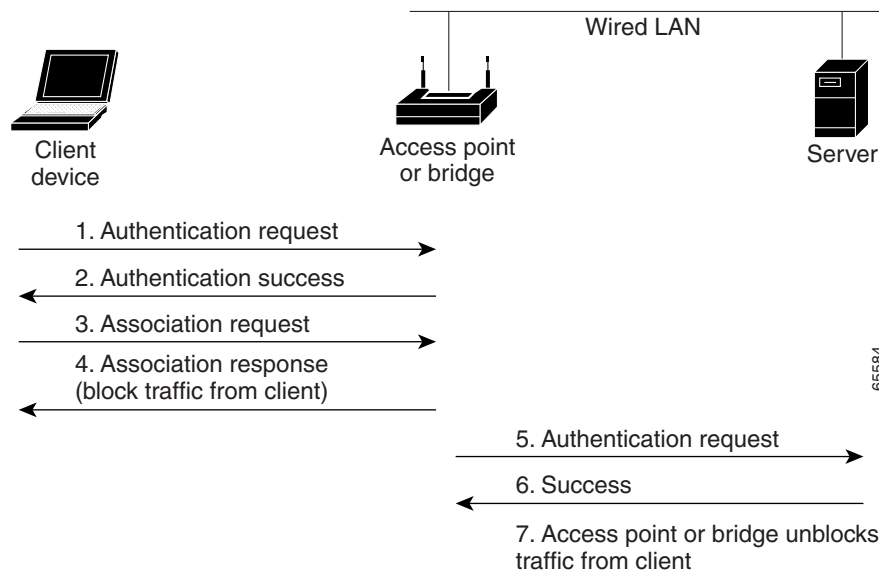
---

If you don't have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point/bridge's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

---

Figure 10-4 shows the authentication sequence for MAC-based authentication.

**Figure 10-4 Sequence for MAC-Based Authentication**



## Combining 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 an SSID”](#) section on page 10-10 for instructions on setting up this combination of authentications.

## Using CCKM for Authenticated Clients

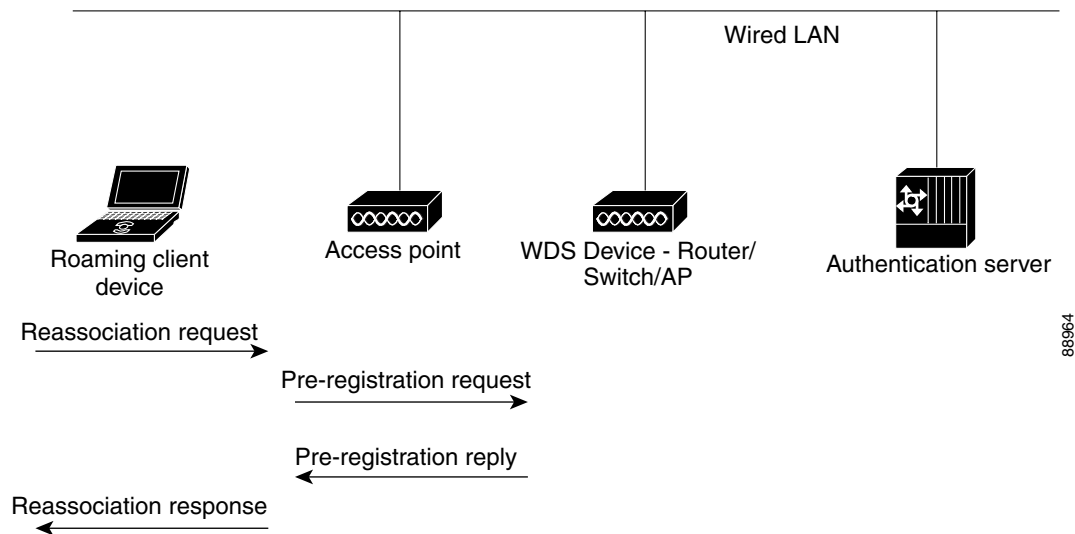
Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point’s cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client’s security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications. See the [“Assigning Authentication Types to an SSID”](#) section on page 10-10 for instructions on enabling CCKM on your access point. See the [“Configuring Access Points as Potential WDS Access Points”](#) section on page 11-7 for detailed instructions on setting up a WDS access point on your wireless LAN.

**Note**

The RADIUS-assigned VLAN feature is not supported for client devices that associate using SSIDs with CCKM enabled.

Figure 10-5 shows the reassociation process using CCKM.

**Figure 10-5 Client Reassociation Using CCKM**



## Using WPA Key Management

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, non-root access point/bridges and the authentication server authenticate to each other using an EAP authentication method, and the non-root access point/bridge and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the root access point/bridge. Using WPA-PSK, however, you configure a pre-shared key on both the non-root access point/bridge and the root access point/bridge, and that pre-shared key is used as the PMK.

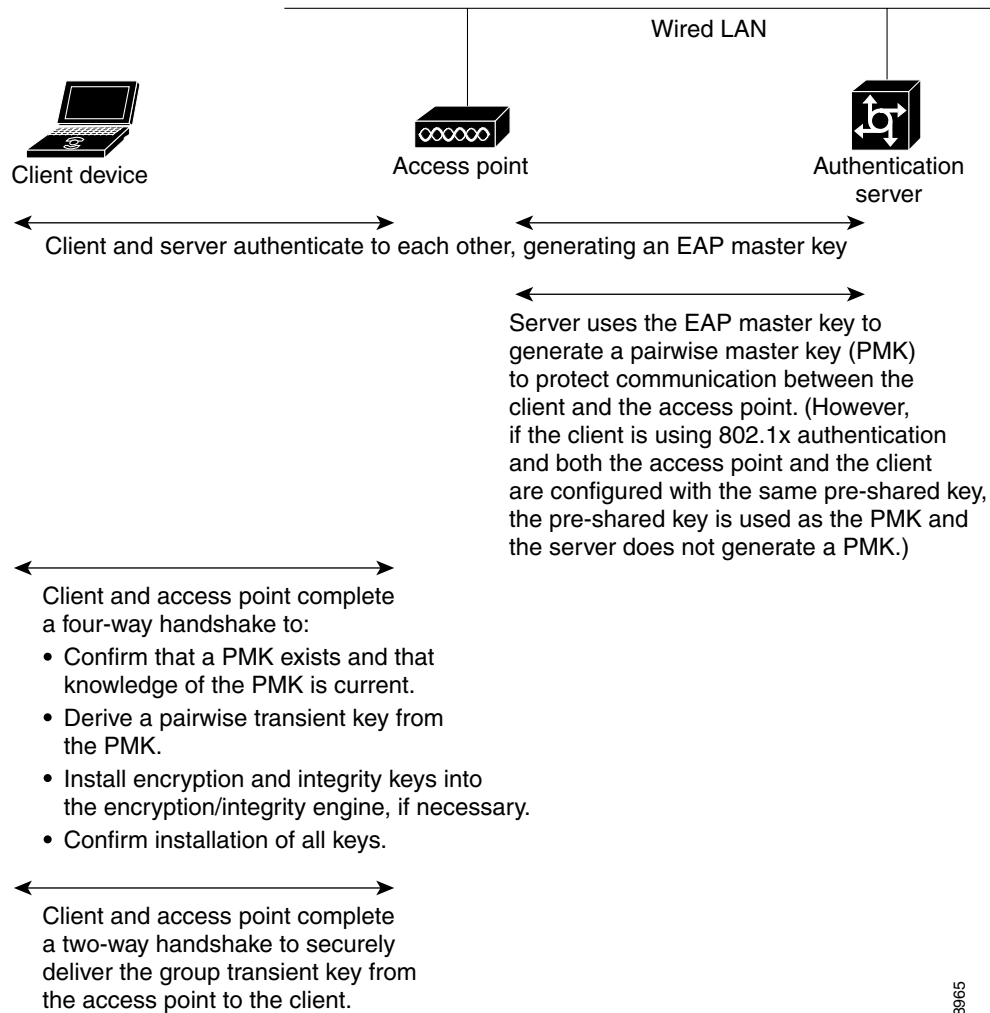
**Note**

Unicast and multicast cipher suites advertised in the WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new VLAN ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the root access point/bridge and the non-root access point/bridge to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the non-root access point/bridge is disassociated from the wireless LAN.

See the “[Assigning Authentication Types to an SSID](#)” section on page 10-10 for instructions on configuring WPA key management on your access point/bridge.

Figure 10-6 shows the WPA key management process.

**Figure 10-6 WPA Key Management Process**



## Software and Firmware Requirements for WPA and WPA-TKIP

Table 10-1 lists the firmware and software requirements required on access points and Cisco Aironet client devices to support WPA key management and WPA-TKIP encryption protocols.

To support the security combinations in Table 10-1, your Cisco Aironet access points and Cisco Aironet client devices must run the following software and firmware versions:

- Cisco IOS Release 12.2(13)JA or later on access points
- Install Wizard version 1.2 for 340, 350, and CB20A client devices, which includes these components:
  - PC, LM, and PCI card driver version 8.4
  - Mini PCI and PC-cardbus card driver version 3.7
  - Aironet Client Utility (ACU) version 6.2
  - Client firmware version 5.30.13

**Table 10-1 Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP**

Key Management and Encryption Protocol	Third Party Host Supplicant <sup>1</sup> Required?	Supported Platform Operating Systems
LEAP with WPA-TKIP	No	Windows XP and 2000
LEAP with WPA	No	Windows XP and 2000
Host-based EAP (such as PEAP and EAP-TLS) with WPA	No <sup>2</sup>	Windows XP
Host-based EAP (such as PEAP and EAP-TLS) with WPA	Yes	Windows 2000
WPA-PSK Mode	No <sup>2</sup>	Windows XP
WPA-PSK Mode	Yes	Windows 2000

1. Such as Funk Odyssey Client supplicant version 2.2 or Meetinghouse Data Communications Aegis Client version 2.1.

2. Windows XP does not require a third-party supplicant, but you must install Windows XP Service Pack 1 and Microsoft support patch 815485.



### Note

When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

## Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point/bridge's SSID. See Chapter 7, "Configuring Multiple SSIDs," for details on setting up the access point/bridge SSID. This section contains these topics:

- [Assigning Authentication Types to an SSID, page 10-10](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-14](#)

## Assigning Authentication Types to an SSID

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio 0</b>	Enter interface configuration mode for the radio interface.
Step 3	<b>ssid <i>ssid-string</i></b>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.  <b>Note</b> Do not include spaces in SSIDs.
Step 4	<b>authentication open</b> <b>[<i>mac-address list-name</i> [alternate]]</b> <b>[<i>eap list-name</i>]</b>	(Optional) Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point/bridge.  <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to open with EAP authentication. The access point/bridge forces all other client devices to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list. Click this link for more information on method lists: <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> </ul> Use the <b>alternate</b> keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network.  <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to open with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list.</li> </ul> <b>Note</b> A access point/bridge configured for EAP authentication forces all access point/bridges that associate to perform EAP authentication. Client devices that do not use EAP cannot communicate with the access point/bridge.
Step 5	<b>authentication shared</b> <b>[<i>mac-address list name</i>]</b> <b>[<i>eap list-name</i>]</b>	(Optional) Set the authentication type for the SSID to shared key.  <b>Note</b> Because of shared key's security flaws, Cisco recommends that you avoid using it.  <b>Note</b> You can assign shared key authentication to only one SSID.  <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to shared key with EAP authentication. For <i>list-name</i>, specify the authentication method list.</li> </ul>

	Command	Purpose
Step 6	<b>authentication network-eap</b> <i>list-name</i> [ <i>mac-address list name</i> ]	(Optional) Set the authentication type for the SSID to Network-EAP. Using the Extensible Authentication Protocol (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. However, the access point does not force all client devices to perform EAP authentication.  (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For list-name, specify the authentication method list.
Step 7	<b>authentication key-management</b> { [ <b>wpa</b> ] } [ <b>optional</b> ]	(Optional) Set the authentication type for the SSID to WPA. If you use the <b>optional</b> keyword, client devices other than WPA clients can use this SSID. If you do not use the <b>optional</b> keyword, only WPA client devices are allowed to use the SSID.  To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.  <b>Note</b> Before you can enable WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. See the “ <a href="#">Configuring Cipher Suites and WEP</a> ” section on page 9-3 for instructions on configuring the VLAN encryption mode.  <b>Note</b> If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK. See the “ <a href="#">Configuring Additional WPA Settings</a> ” section on page 10-13 for instructions on configuring a pre-shared key.
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the SSID access point/bridgeman to open with EAP authentication. Access points and bridges using the access point/bridge an SSID attempt EAP authentication using a server named *adam*.

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridgeman
ap(config-ssid)# authentication open eap adam
ap(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridgeman
ap(config-ssid)# authentication client username bridge7 password catch22
ap(config-ssid)# authentication open eap adam
```

This example sets the authentication type for the SSID access point/bridget to network-EAP with a static WEP key. EAP-enabled access point/bridges using the access point/bridget SSID attempt EAP authentication using a server named *eve*, and access point/bridges using static WEP rely on the static WEP key.

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# encryption key 2 size 128 12345678901234567890123456
ap(config-if)# ssid bridget
ap(config-ssid)# authentication network-eap eve
ap(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid bridget
ap(config-ssid)# authentication client username bridget1 password 99bottles
```

## Configuring WPA Migration Mode

WPA migration mode allows these client device types to associate to the access point/bridge using the same SSID:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP
- Static-WEP clients not capable of TKIP or authenticated key management

If all three client types associate using the same SSID, the multicast cipher suite for the SSID must be WEP. If only the first two types of clients use the same SSID the multicast key can be dynamic, but if the static-WEP clients use the SSID, the key must be static. The access point/bridge can switch automatically between a static and a dynamic group key to accommodate associated client devices. To support all three types of clients on the same SSID, you must configure the static key in key slots 2 or 3.

To set up an SSID for WPA migration mode, configure these settings:

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

This example sets the SSID migrate for WPA migration mode:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# encryption mode cipher tkip wep128
ap(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap(config-if)# ssid migrate
ap(config-ssid)# authentication open
ap(config-ssid)# authentication network-eap adam
ap(config-ssid)# authentication key-management wpa optional
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config-ssid)# exit
```

## Configuring the Root Access Point/Bridge to Interact with the WDS Device

To support non-root access point/bridges using CCKM, your root access point/bridge must interact with the WDS device on your network, and your authentication server must be configured with a username and password for the root access point/bridge. For detailed instructions on configuring WDS and CCKM on your wireless LAN, see Chapter 11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

On your root access point/bridge, enter this command in global configuration mode:

```
ap(config)# wlccp ap username username password password
```

You must configure the same username and password pair when you set up the root access point/bridge as a client on your authentication server.

## Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point/bridge and adjust the frequency of group key updates.

### Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the access point/bridge. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point/bridge expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

### Configuring Group Key Updates

In the last step in the WPA process, the access point/bridge distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination—the access point generates and distributes a new group key when any authenticated device disassociates from the access point/bridge. This feature keeps the group key private for associated devices, but it might generate some overhead traffic if clients on your network roam frequently among access points.
- Capability change—the access point/bridge generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point/bridge.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio 0</b>	Enter interface configuration mode for the radio interface.
Step 3	<b>ssid ssid-string</b>	Enter SSID configuration mode for the SSID.

	Command	Purpose
Step 4	<b>wpa-psk</b> { hex   ascii } [ 0   7 ] <i>encryption-key</i>	Enter a pre-shared key for access point/bridges using WPA that also use static WEP keys.  Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point/bridge expands the key for you. You can enter a maximum of 63 ASCII characters.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for non-root access point/bridges using WPA and static WEP, with group key update options:

```
ap# configure terminal
ap(config)# configure interface dot11radio 0
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config-ssid)# end
```

## Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for non-root access point/bridges and client devices authenticating through your root access point/bridge:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>dot11 holdoff-time</b> <i>seconds</i>	Enter the number of seconds a root access point/bridge must wait before it disassociates and idle client. Enter a value from 1 to 65555 seconds.
Step 3	<b>interface dot11radio 0</b>	Enter interface configuration mode for the radio interface.
Step 4	<b>dot1x client-timeout</b> <i>seconds</i>	Enter the number of seconds the bridge should wait for a reply from a non-root access point/bridge attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.

	Command	Purpose
Step 5	<code>dot1x reauth-period seconds [server]</code>	Enter the interval in seconds that the access point/bridge waits before forcing an authenticated non-root access point/bridge to reauthenticate. <ul style="list-style-type: none"> <li>(Optional) Enter the <b>server</b> keyword to configure the access point/bridge 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 non-root access point/bridge before termination of the session or prompt. The server sends this attribute to the root access point/bridge when a non-root access point/bridge performs EAP authentication.</li> </ul>
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to reset the values to default settings.

## Matching Authentication Types on Root and Non-Root Access Point/Bridges

To use the authentication types described in this section, the access point/bridge authentication settings must match the authentication settings on the client adapters that associate to the access point. Refer to the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for instructions on setting authentication types on wireless client adapters. Refer to [Chapter 9, “Configuring Cipher Suites and WEP,”](#) for instructions on configuring cipher suites and WEP on the access point.

[Table 10-2](#) lists the client and access point settings required for each authentication type.



### Note

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**.

**Table 10-2 Client and Access Point Security Settings**

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID

Table 10-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID <sup>1</sup>
802.1x authentication	Enable LEAP	Select a cipher suite and enable Network-EAP for the SSID
802.1x authentication and WPA	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication)  <b>Note</b> To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
802.1x authentication and WPA-PSK	Enable any 802.1x authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication). Enter a WPA pre-shared key.  <b>Note</b> To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select 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	Set up and enable WEP and enable EAP and Open authentication 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	Set up and enable WEP and enable EAP and Open Authentication for the SSID

**Table 10-2 Client and Access Point Security Settings (continued)**

Security Feature	Client Setting	Access Point Setting
PEAP authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication 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**.

