



## Configuring Authentication Types

---

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

- [Understanding Authentication Types, page 10-2](#)
- [Configuring Authentication Types, page 10-8](#)
- [Matching Access Point and Client Device Authentication Types, page 10-13](#)

# Understanding Authentication Types

This section describes the authentication types that you can configure on the access point. 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 7, “Configuring Multiple SSIDs,”](#) for complete instructions on configuring 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. These sections explain each authentication type:

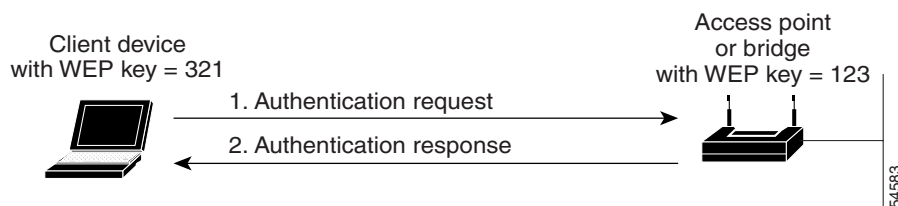
- [Open Authentication to the Access Point, page 10-2](#)
- [Shared Key Authentication to the Access Point, page 10-3](#)
- [EAP Authentication to the Network, page 10-3](#)
- [MAC Address Authentication to the Network, page 10-5](#)
- [Combining MAC-Based, EAP, and Open Authentication, page 10-5](#)
- [Using CCKM for Authenticated Clients, page 10-6](#)
- [Using WPA Key Management, page 10-6](#)

## Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can communicate only if its WEP keys match the access point's. 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.

[Figure 10-1](#) 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 10-1** Sequence for Open Authentication



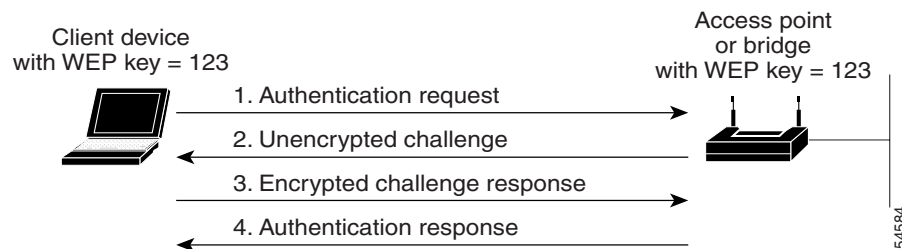
## Shared Key Authentication to the Access Point

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 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 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 10-2** Sequence for Shared Key Authentication

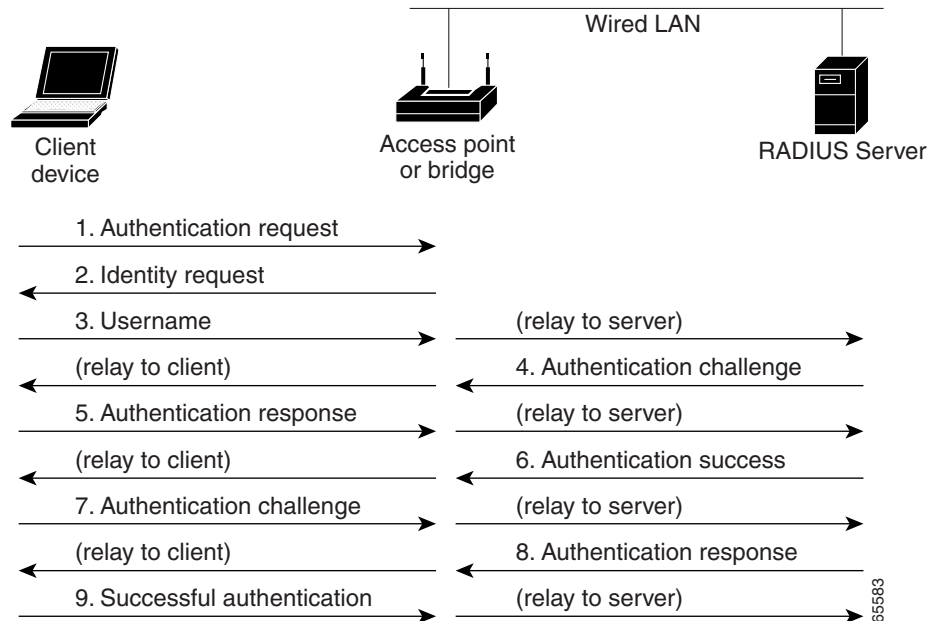


## EAP Authentication to the Network

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 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.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in [Figure 10-3](#):

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



In Steps 1 through 9 in [Figure 10-3](#), 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 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 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. See the [“Assigning Authentication Types to an SSID” section on page 10-8](#) for instructions on setting up EAP on the access point.



**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 and to your network.

## MAC Address Authentication to the Network

The access point 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 10-8 for instructions on enabling MAC-based authentication.

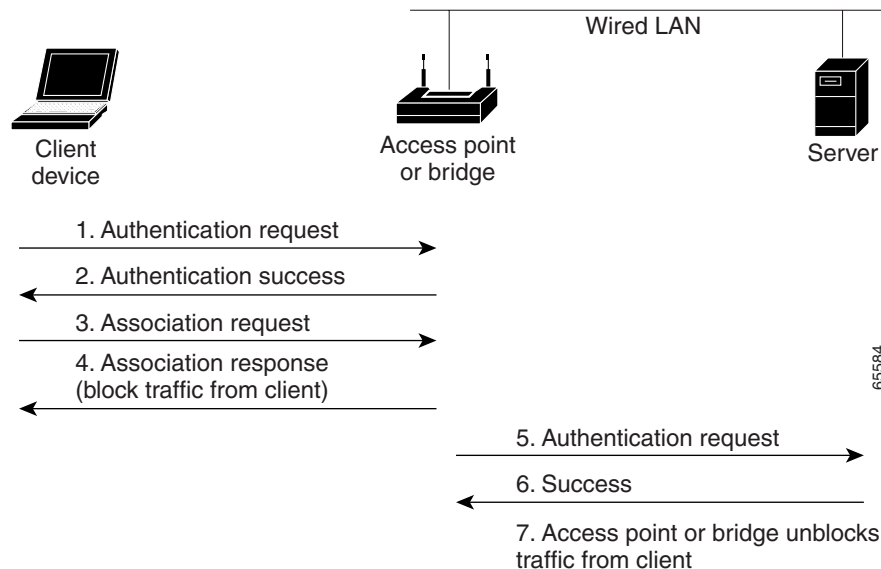


**Tip**

If you don't have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate. When you create the list of allowed MAC addresses, use lower case for all letters in the addresses that you enter.

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 10-8 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 10-8 for instructions on enabling CCKM on your access point. See the [“Configuring Access Points as Potential WDS Access Points”](#) section on page 11-5 for detailed instructions on setting up a WDS access point on your wireless LAN.

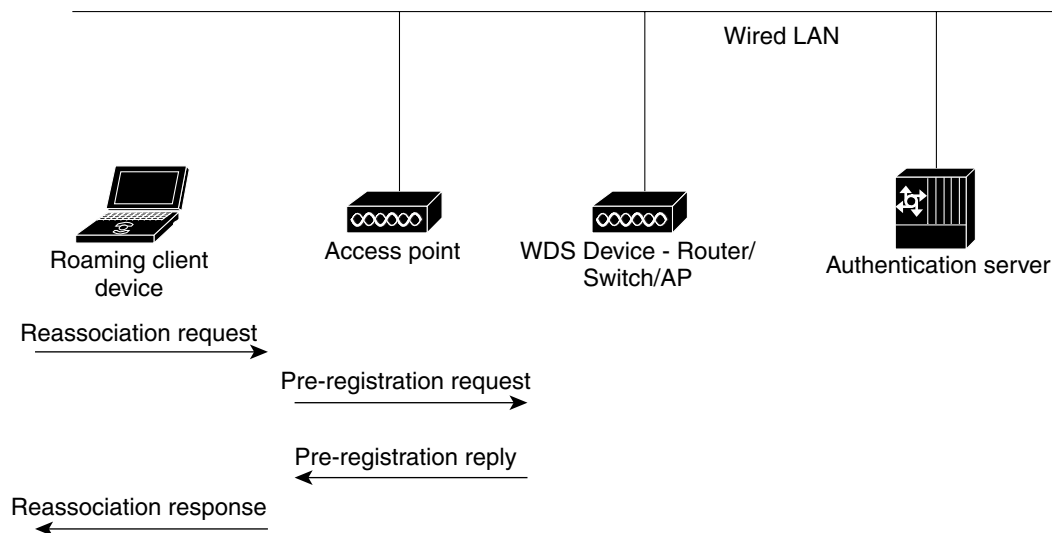


### Note

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 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, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key

(PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

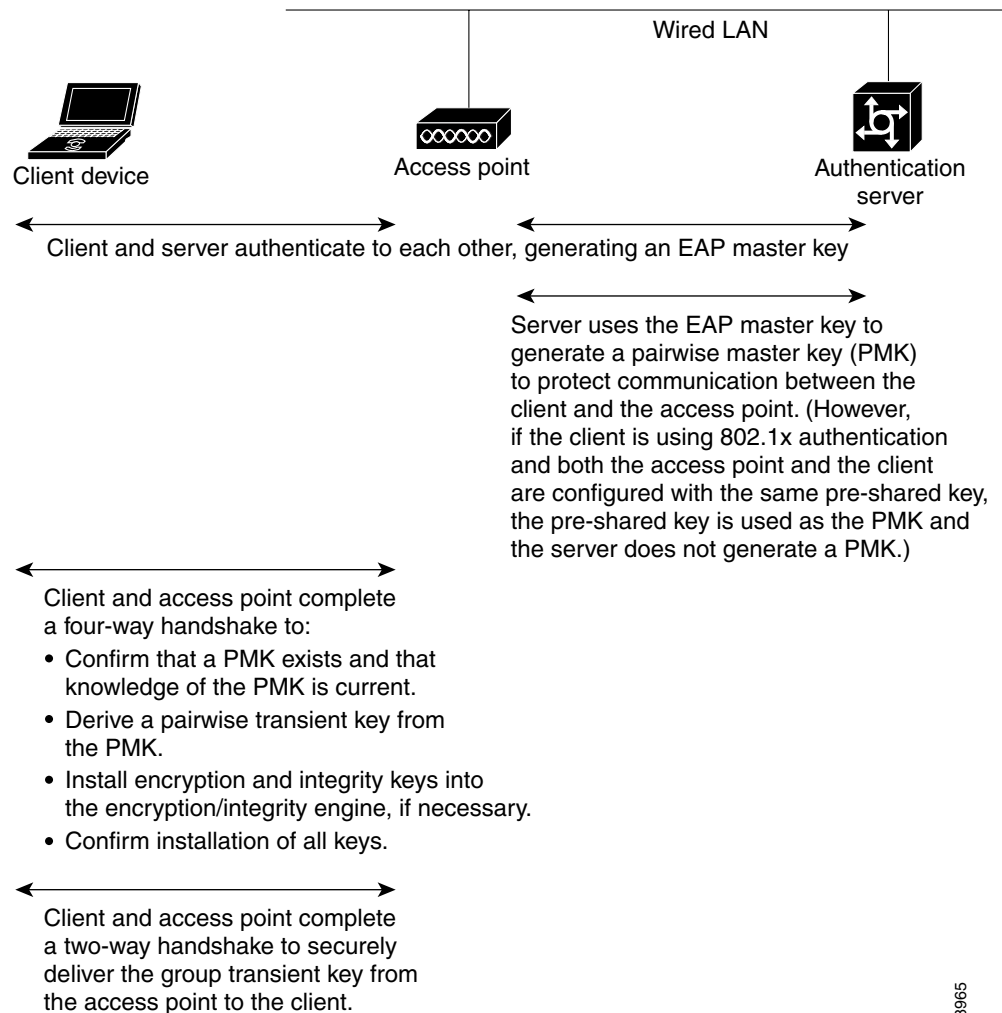
**Note**

Unicast and multicast cipher suites advertised in 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 access point and client 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 client device is disassociated from the wireless LAN.

See the “[Assigning Authentication Types to an SSID](#)” section on page 10-8 for instructions on configuring WPA key management on your access point.

Figure 10-6 shows the WPA key management process.

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



# Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See [Chapter 7, “Configuring Multiple SSIDs,”](#) for details on setting up multiple SSIDs. This section contains these topics:

- [Default Authentication Settings, page 10-8](#)
- [Assigning Authentication Types to an SSID, page 10-8](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-13](#)

## Default Authentication Settings

The default SSID on the access point is *tsunami*. [Table 10-1](#) shows the default authentication settings for the default SSID.

**Table 10-1** Default Authentication Configuration

Feature	Default Setting
SSID	tsunami
Guest Mode SSID	tsunami (The access point broadcasts this SSID in its beacon and allows client devices with no SSID to associate.)

## Assigning Authentication Types to an SSID

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio { 0   1 }</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<code>ssid ssid-string</code>	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.

	Command	Purpose
Step 4	<b>authentication open</b> [mac-address <i>list-name</i> [alternate]] [eap <i>list-name</i> ]	<p>(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.</p> <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC-address 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/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> </ul> <p>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.</p> <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> <p><b>Note</b> An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point.</p>
Step 5	<b>authentication shared</b> [mac-address <i>list-name</i> ] [eap <i>list-name</i> ]	<p>(Optional) Set the authentication type for the SSID to shared key.</p> <p><b>Note</b> Because of shared key's security flaws, Cisco recommends that you avoid using it.</p> <p><b>Note</b> You can assign shared key authentication to only one SSID.</p> <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to shared key with MAC address authentication. For <i>list-name</i>, specify the authentication method list.</li> <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> [ <b>mac-address</b> <i>list-name</i> ]	<p>(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.</p> <ul style="list-style-type: none"> <li>(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.</li> </ul>
Step 7	<b>authentication key-management</b> { <b>cckm</b>   <b>wpa</b> } [ <b>optional</b> ]	<p>(Optional) Set the authentication type for the SSID to CCKM or WPA. If you use the <b>optional</b> keyword, client devices other than CCKM and WPA clients can use this SSID. If you do not use the <b>optional</b> keyword, only CCKM or WPA client devices are allowed to use the SSID.</p> <p>To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.</p> <p><b>Note</b> Before you can enable CCKM or 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.</p> <p><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 10-11 for instructions on configuring a pre-shared key.</p> <p>See <a href="#">Chapter 11, “Configuring Fast Reassociation,”</a> for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager.</p>
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 *batman* to Network-EAP with CCKM authenticated key management. Client devices using the *batman* SSID authenticate using the *adam* server list. After they are authenticated, CCKM-enabled clients can perform fast reassociations using CCKM.

```
ap1200# configure terminal
ap1200(config)# configure interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
```

```
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config-ssid)# end
```

## Configuring WPA Migration Mode

WPA migration mode allows these client device types to associate to the access point 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 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:

```
ap1200# configure terminal
ap1200(config)# configure interface dot11radio 0
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config-ssid)# end
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-if)# end
```

## Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point 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. 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 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 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. 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 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.

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   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>ssid <i>ssid-string</i></b>	Enter SSID configuration mode for the SSID.
Step 4	<b>wpa-psk { hex   ascii } [ 0   7 ]</b> <i>encryption-key</i>	Enter a pre-shared key for client devices 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 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>broadcast-key [ vlan <i>vlan-id</i> ]</b> <b>{ change <i>seconds</i> }</b> <b>[ membership-termination ]</b> <b>[ capability-change ]</b>	Use the <b>broadcast key rotation</b> command to configure additional updates of the WPA group key.
Step 7	<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 clients using WPA and static WEP, with group key update options:

```
ap1200# configure terminal
ap1200(config)# configure interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config-ssid)# end
ap (config)# broadcast-key vlan 87 membership-termination capability-change
```

## Configuring Authentication Holdoffs, Timeouts, and Intervals

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>dot11 holdoff-time seconds</code>	Enter the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication. Enter a value from 1 to 65555 seconds.
Step 3	<code>interface dot11radio { 0   1 }</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 4	<code>dot1x client-timeout seconds</code>	Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.
Step 5	<code>dot1x reauth-period seconds [server]</code>	Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. <ul style="list-style-type: none"> <li>(Optional) Enter the <b>server</b> 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.</li> </ul>
Step 6	<code>countermeasure tkip hold-time seconds</code>	Configure a TKIP MIC failure holdtime. If the access point detects two MIC failures within 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.
Step 7	<code>end</code>	Return to privileged EXEC mode.
Step 8	<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 Access Point and Client Device Authentication Types

To use the authentication types described in this section, the access point 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.

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

<b>Security Feature</b>	<b>Client Setting</b>	<b>Access Point Setting</b>
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
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID
802.1x authentication and CCKM	Enable LEAP	Select a cipher suite and enable Network-EAP and CCKM for the SSID  <b>Note</b> To allow both 802.1x clients and non-802.1x clients to use the SSID, enable optional CCKM.
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.

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

Security Feature	Client Setting	Access Point Setting
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
EAP-MD5 authentication		
If using ACU to configure card	Create a WEP key, enable Host Based EAP, and enable Use Static WEP Keys in ACU and select Enable network access control using IEEE 802.1X and MD5-Challenge 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 MD5-Challenge as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID
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

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

<b>Security Feature</b>	<b>Client Setting</b>	<b>Access Point Setting</b>
EAP-SIM 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 SIM Authentication as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP with full encryption 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 SIM Authentication as the EAP Type	Set up and enable WEP with full encryption and enable Require EAP and Open Authentication for the SSID