



## Configuring Authentication Types

---

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

- [Understanding Authentication Types, page 10-2](#)
- [Configuring Authentication Types, page 10-5](#)
- [Matching Authentication Types on Root and Non-Root Bridges, page 10-11](#)

# Understanding Authentication Types

This section describes the authentication types that you can configure on the bridge. The authentication types are tied to the SSID that you configure on the bridge.

Before bridges can communicate, they must authenticate to each other using open or shared-key authentication. For maximum security, bridges should also authenticate to your network using EAP authentication, an authentication type that relies on an authentication server on your network.

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

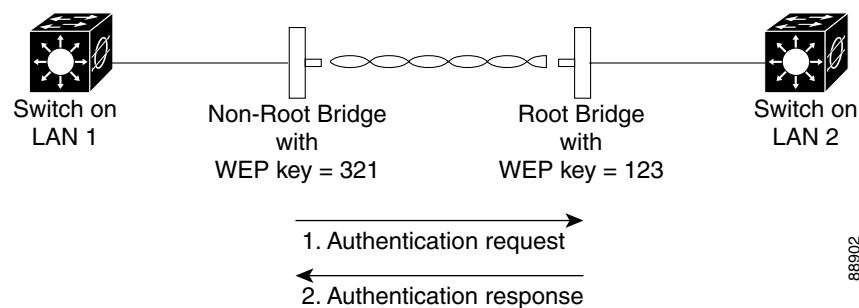
- [Open Authentication to the Bridge, page 10-2](#)
- [Shared Key Authentication to the Bridge, page 10-2](#)
- [EAP Authentication to the Network, page 10-3](#)
- [Using WPA Key Management, page 10-5](#)

## Open Authentication to the Bridge

Open authentication allows any 1400 series bridge to authenticate and then attempt to communicate with another 1400 series bridge. Using open authentication, a non-root bridge can authenticate to a root bridge, but the non-root bridge can communicate only if its WEP keys match the root bridge's. A bridge that is not using WEP does not attempt to authenticate with a 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 bridge trying to authenticate and a root bridge using open authentication. In this example, the device's WEP key does not match the bridge's key, so it can authenticate but not pass data.

**Figure 10-1** Sequence for Open Authentication



## Shared Key Authentication to the Bridge

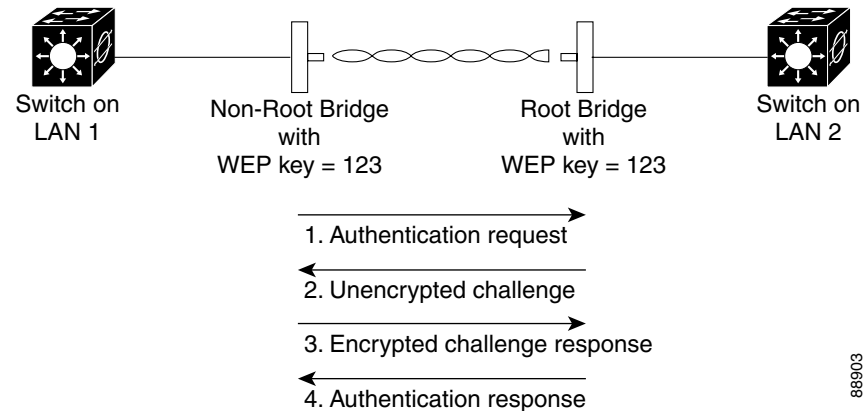
Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, Cisco recommends that you avoid using it.

During shared key authentication, the root bridge sends an unencrypted challenge text string to other bridges attempting to communicate with the root bridge. The bridge requesting authentication encrypts the challenge text and sends it back to the root bridge. If the challenge text is encrypted correctly, the root bridge allows the requesting device to authenticate. Both the unencrypted challenge and the

encrypted challenge can be monitored, however, which leaves the root 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 bridge using shared key authentication. In this example the device's WEP key matches the bridge's key, so it can authenticate and communicate.

**Figure 10-2 Sequence for Shared Key Authentication**

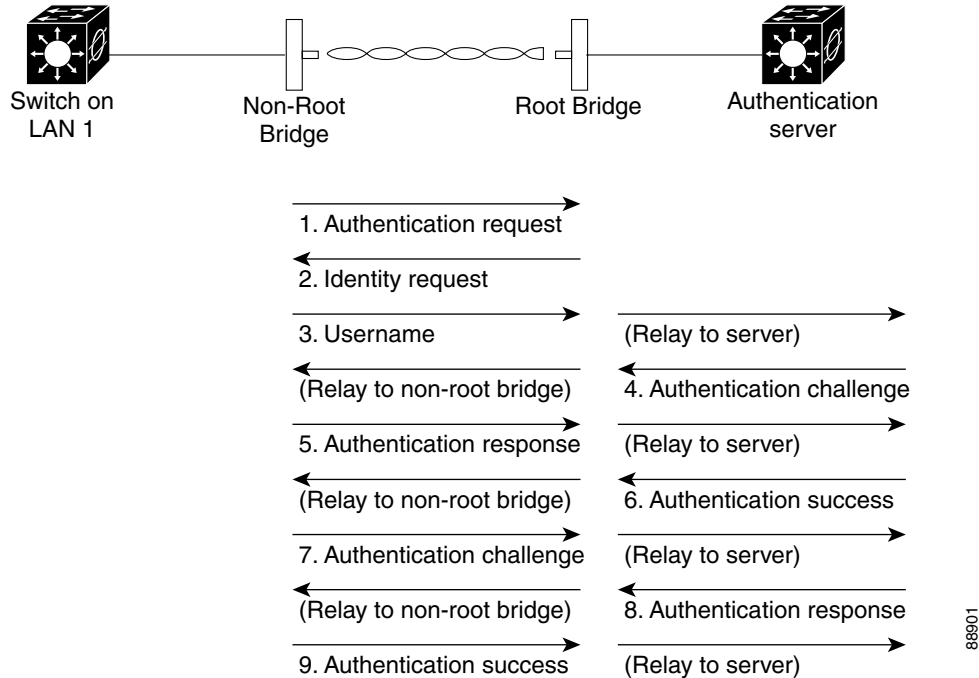


## EAP Authentication to the Network

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 root bridge helps another 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 bridge, which uses it for all unicast data signals that it sends to or receives from the non-root bridge. The root bridge also encrypts its broadcast WEP key (entered in the bridge's WEP key slot 1) with the non-root bridge's unicast key and sends it to the non-root bridge.

When you enable EAP on your bridges, 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 non-root bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root bridge. The RADIUS server sends an authentication challenge to the non-root bridge. The non-root 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 bridge. When the RADIUS server authenticates the non-root bridge, the process repeats in reverse, and the non-root bridge authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root bridge determine a WEP key that is unique to the non-root bridge and provides the non-root 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 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 bridge. The root bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root bridge, which uses the session key to decrypt it. The non-root bridge and the root 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 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 10-6](#) for instructions on setting up EAP on the 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 bridge and to your network.

## 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 bridges and the authentication server authenticate to each other using an EAP authentication method, and the non-root bridge and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the root bridge. Using WPA-PSK, however, you configure a pre-shared key on both the non-root bridge and the root 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 bridge and the non-root bridge to switch back to the new cipher suite. Currently, the WPA protocol does not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the non-root bridge is disassociated from the wireless LAN.

See the [“Assigning Authentication Types to an SSID”](#) section on page 10-6 for instructions on configuring WPA key management on your bridge.

## Configuring Authentication Types

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

- [Default Authentication Settings, page 10-6](#)
- [Assigning Authentication Types to an SSID, page 10-6](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-9](#)

## Default Authentication Settings

The default SSID on the bridge is *autoinstall*. Table 10-1 shows the default authentication settings for the default SSID:

**Table 10-1** Default Authentication Configuration

Feature	Default Setting
SSID	autoinstall
Guest Mode SSID	autoinstall (The bridge broadcasts this SSID in its beacon and allows bridges with no SSID to associate.)
Authentication types assigned to tsunami	open

## 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>eap <i>list-name</i></b> ]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any bridge to authenticate and then attempt to communicate with the bridge.  <ul style="list-style-type: none"> <li>(Optional) Set the SSID's authentication type to open with EAP authentication. The bridge forces all other bridges 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 bridge configured for EAP authentication forces all bridges that associate to perform EAP authentication. Bridges that do not use EAP cannot communicate with the bridge.
Step 5	<b>authentication shared</b> [ <b>eap <i>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.  <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>	(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 bridge helps a non-root bridge and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the bridge does not force all non-root bridges to perform EAP authentication.
Step 7	<b>authentication key-management</b> {[wpa] [cckm]} [optional]	<p>(Optional) Set the authentication type for the SSID to WPA. If you use the <b>optional</b> keyword, non-root bridges not configured for WPA can use this SSID. If you do not use the <b>optional</b> keyword, only WPA bridges are allowed to use the SSID.</p> <p>To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.</p> <p><b>Note</b> The bridge does not support the CCKM option in the <b>authentication key-management</b> command.</p> <p><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.</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 10-8 for instructions on configuring a pre-shared key.</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 *bridgeman* to open with EAP authentication. Bridges using the *bridgeman* SSID attempt EAP authentication using a server named *adam*.

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

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

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

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

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

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

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication client username bridge11 password 99bottles
```

## Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the 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 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 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 root bridge distributes a group key to the authenticated non-root bridge. You can use these optional settings to configure the root bridge to change and distribute the group key based on association and disassociation of non-root bridges:

- Membership termination—the root bridge generates and distributes a new group key when any authenticated non-root bridge disassociates from the root bridge. This feature keeps the group key private for associated bridges.
- Capability change—the root bridge generates and distributes a dynamic group key when the last non-key management (static WEP) non-root bridge disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) non-root bridge authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP bridges associated to the root 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 <i>ssid-string</i></b>	Enter SSID configuration mode for the SSID.

	Command	Purpose
Step 4	<b>wpa-psk { hex   ascii } [ 0   7 ]</b> <i>encryption-key</i>	Enter a pre-shared key for 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 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 bridges using WPA and static WEP, with group key update options:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(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 bridges authenticating through your root 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 non-root bridge must wait before it can reattempt to authenticate following a failed authentication. 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 bridge attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.
Step 5	<b>dot1x reauth-period</b> <i>seconds</i> <b>[server]</b>	Enter the interval in seconds that the bridge waits before forcing an authenticated non-root bridge to reauthenticate. <ul style="list-style-type: none"> <li>(Optional) Enter the <b>server</b> keyword to configure the 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 bridge before termination of the session or prompt. The server sends this attribute to the root bridge when a non-root bridge performs EAP authentication.</li> </ul>

	Command	Purpose
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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

## Setting Up a Non-Root Bridge as a LEAP Client

You can set up a non-root bridge to authenticate to your network like other wireless client devices. After you provide a network username and password for the non-root bridge, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

Setting up a non-root bridge as a LEAP client requires three major steps:

1. Create an authentication username and password for the non-root bridge on your authentication server.
2. Configure LEAP authentication on the root bridge to which the non-root bridge associates.
3. Configure the non-root bridge to act as a LEAP client.

Beginning in Privileged Exec mode, follow these instructions to set up the non-root bridge as a LEAP client:

	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.
Step 4	<b>authentication client</b> <b>username <i>username</i></b> <b>password <i>password</i></b>	Configure the username and password that the non-root bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the non-root bridge on the authentication server.
Step 5	<b>authentication network-eap</b> <b><i>list-name</i></b>	Set the authentication type for the SSID to Network-EAP.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

This example sets a LEAP username and password for the SSID *bridgeman*, and configures Network-EAP as the authentication type for the SSID on the non-root bridge:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bugsy password run4yerlife
bridge(config-ssid)# authentication network-eap romeo
bridge(config-ssid)# end
```

# Matching Authentication Types on Root and Non-Root Bridges

To use the authentication types described in this section, the root bridge authentication settings must match the settings on the non-root bridges that associate to the root bridge.

Table 10-2 lists the settings required for each authentication type on the root and non-root bridges.

**Table 10-2 Non-Root and Root Bridge Security Settings**

Security Feature	Non-Root Bridge Setting	Root Bridge Setting
Static WEP with open authentication	Set up and enable WEP	Set up and enable WEP and enable Open authentication
Static WEP with shared key authentication	Set up and enable WEP and enable Shared Key Authentication	Set up and enable WEP and enable Shared Key authentication
LEAP authentication	Set up and enable WEP and Network-EAP authentication and configure a LEAP username and password	Set up and enable WEP and enable network-EAP authentication
WPA key management	Set up and enable WEP and enable WPA authentication	Set up and enable WEP and enable WPA authentication

■ Matching Authentication Types on Root and Non-Root Bridges