



Configuring Repeater and Standby Access Points and Workgroup Bridge Mode

This chapter describes how to configure your access point as a repeater, as a hot standby unit, or as a workgroup bridge. This chapter contains these sections:

- [Understanding Repeater Access Points, page 20-2](#)
- [Configuring a Repeater Access Point, page 20-3](#)
- [Understanding Workgroup Bridge Mode, page 20-11](#)
- [Configuring Workgroup Bridge Mode, page 20-14](#)

Understanding Repeater Access Points

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. You can configure access point/bridge radio as a repeater.

The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. When you configure the access point/bridge as a repeater, the access point's Ethernet port does not forward traffic.

You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

A repeater access point associates to the access point with which it has the best connectivity. However, you can specify the access point to which the repeater associates. Setting up a static, specific association between a repeater and a root access point improves repeater performance.

To set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions, which are enabled by default, improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point. Disabling Aironet extensions sometimes improves the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices might have difficulty communicating with repeater access points and the root access point to which repeaters are associated.

**Note**

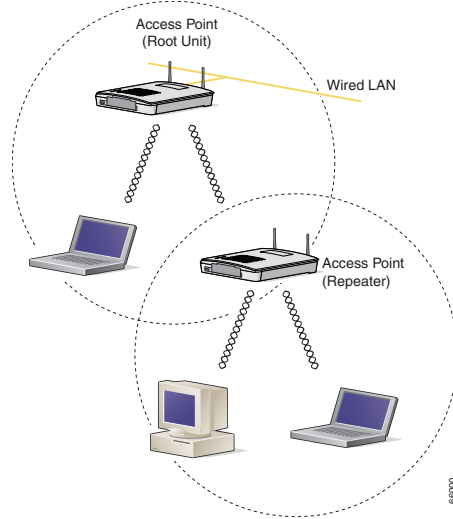
Because the access point/bridge creates a virtual interface for its radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

**Note**

You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Figure 20-1 shows an access point acting as a repeater.

Figure 20-1 Access Point as a Repeater



Configuring a Repeater Access Point

This section provides instructions for setting up an access point as a repeater and includes these sections:

- [Default Configuration, page 20-3](#)
- [Guidelines for Repeaters, page 20-3](#)
- [Setting Up a Repeater, page 20-4](#)
- [Verifying Repeater Operation, page 20-5](#)
- [Setting Up a Repeater As a LEAP Client, page 20-6](#)
- [Setting Up a Repeater As a WPA Client, page 20-7](#)

Default Configuration

The access point/bridge boots in the Root AP mode by default. [Table 20-1](#) shows the default values for settings that control the access point's role in the wireless LAN.

Table 20-1 Default Settings for Role in Wireless LAN

Feature	Default Setting
Station role	Root AP
Optimize Radio Network for	Default
Extensions	Aironet

Guidelines for Repeaters

Follow these guidelines when configuring repeater access points:

- Use repeaters to serve client devices that do not require high throughput. Repeaters extend the coverage area of your wireless LAN, but they drastically reduce throughput.
- Use repeaters when most if not all client devices that associate with the repeaters are Cisco Aironet clients. Non-Cisco client devices sometimes have trouble communicating with repeater access points.
- Make sure that the data rates configured on the repeater access point match the data rates on the parent access point. For instructions on configuring data rates, see the “[Configuring Radio Data Rates](#)” section on page 6-4.
- Repeater access points support only the native VLAN. You cannot configure multiple VLANs on a repeater access point.

**Note**

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run Cisco IOS software.

**Note**

Repeater access points do not support wireless domain services (WDS). Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

**Note**

If multiple BSSIDs are configured on a root access point that is designated as the parent of a repeater, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a repeater on your wireless LAN is configured to associate to a specific parent, check the association status of the repeater when you add or delete BSSIDs on the parent access point.

Setting Up a Repeater

Beginning in Privileged Exec mode, follow these steps to configure an access point as a repeater:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Create the SSID that the repeater uses to associate to a root access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the root access point, create the same SSID on the repeater, also.
Step 4	infrastructure-ssid [optional]	Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root access point. Infrastructure devices must associate to the repeater access point using this SSID unless you also enter the optional keyword.
Step 5	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 6	station-role repeater	Set the access point's role in the wireless LAN to repeater.

	Command	Purpose
Step 7	dot11 extensions aironet	If Aironet extensions are disabled, enable Aironet extensions.
Step 8	parent {1-4} mac-address <i>[timeout]</i>	<p>(Optional) Enter the MAC address for the access point to which the repeater should associate.</p> <ul style="list-style-type: none"> You can enter MAC addresses for up to four parent access points. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list. <p>Note If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted.</p> <ul style="list-style-type: none"> (Optional) You can also enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	end	Return to privileged EXEC mode.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to set up a repeater access point with three potential parents:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid chicago
ap(config-ssid)# infrastructure-ssid
ap(config-ssid)# exit
ap(config-if)# station-role repeater
ap(config-if)# dot11 extensions aironet
ap(config-if)# parent 1 0987.1234.h345 900
ap(config-if)# parent 2 7809.b123.c345 900
ap(config-if)# parent 3 6543.a456.7421 900
ap(config-if)# end
```

Verifying Repeater Operation

After you set up the repeater, check the access point/bridge LEDs. If your repeater is functioning correctly, the LEDs on the repeater and the root access point to which it is associated behave like this:

- The status LED on the root access point is steady green, indicating that at least one client device is associated with it (in this case, the repeater).
- The status LED on the repeater access point is steady green when it is associated with the root access point and the repeater has client devices associated to it. The repeater's status LED flashes (steady green for 7/8 of a second and off for 1/8 of a second) when it is associated with the root access point but the repeater has no client devices associated to it.

The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a LEAP Client

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

Setting up a repeater as a LEAP client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure LEAP authentication on the root access point to which the repeater associates. The access point to which the repeater associates is called the parent access point. See [Chapter 10, “Configuring Authentication Types,”](#) for instructions on setting up authentication.



Note On the repeater access point, you must enable the same cipher suite or WEP encryption method and WEP features that are enabled on the parent access point.

3. Configure the repeater to act as a LEAP client. Beginning in Privileged Exec mode, follow these instructions to set up the repeater as a LEAP client:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters, but they should not include spaces. SSIDs are case-sensitive.
Step 4	authentication network-eap <i>list-name</i>	Enable LEAP authentication on the repeater so that LEAP-enabled client devices can authenticate through the repeater. For <i>list-name</i> , specify the list name you want to use for EAP authentication. You define list names for EAP and for MAC addresses using the aaa authentication login command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.
Step 5	authentication client username <i>username</i> password <i>password</i>	Configure the username and password that the repeater uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the repeater on the authentication server.
Step 6	infrastructure ssid [optional]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the optional keyword.
Step 7	end	Return to privileged EXEC mode.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Setting Up a Repeater As a WPA Client

WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. You can set up a repeater access point to authenticate to your network like other WPA-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA client:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	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	authentication open	Enable open authentication for the SSID.
Step 5	authentication key-management wpa	Enable WPA authenticated key management for the SSID.
Step 6	infrastructure ssid	Designate the SSID as the SSID that the repeater uses to associate to other access points.
Step 7	wpa-psk { hex ascii } [0 7] <i>encryption-key</i>	Enter a pre-shared key for the repeater. 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 from 8 to 63 ASCII characters, and the access point expands the key for you.
Step 8	end	Return to privileged EXEC mode.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Understanding Hot Standby

Hot Standby mode designates an access point as a backup for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and sends IAPP queries to the monitored access point through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. If the monitored access point goes offline and the standby access point takes its place in the network, matching settings ensures that client devices can switch easily to the standby access point.

Hot standby mode is disabled by default.

**Note**

If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

**Note**

The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit will monitor. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point also must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask
- Default Gateway
- Data rates
- WEP settings
- Authentication types and authentication servers

Check the monitored access point and record these settings before you set up the standby access point.

**Note**

Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

**Tip**

To quickly duplicate the monitored access point's settings on the standby access point, save the monitored access point configuration and load it on the standby access point. See the [“Working with Configuration Files” section on page 18-8](#) for instructions on uploading and downloading configuration files.

Beginning in Privileged Exec mode, follow these steps to enable hot standby mode on an access point:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	iapp standby <i>mac-address</i>	Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point. Note When you configure a 1200 Series access point with two radios to monitor a 1200 Series access point with two radios, you must enter the MAC addresses of both the monitored 2.4-GHz and 5-GHz radios. Enter the 2.4-GHz radio MAC address first, followed by the 5-GHz radio MAC address. Note The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point.
Step 3	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 4	ssid <i>ssid-string</i>	Create the SSID that the standby access point uses to associate to the monitored access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the monitored access point, create the same SSID on the standby access point, also.
Step 5	infrastructure-ssid [optional]	Designate the SSID as an infrastructure SSID. The standby uses this SSID to associate to the monitored access point. If the standby access point takes the place of the monitored access point, infrastructure devices must associate to the standby access point using this SSID unless you also enter the optional keyword.
Step 6	authentication client username <i>username</i> password <i>password</i>	If the monitored access point is configured to require LEAP authentication, configure the username and password that the standby access point uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the standby access point on the authentication server.
Step 7	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	iapp standby poll-frequency <i>seconds</i>	Sets the number of seconds between queries that the standby access point sends to the monitored access point's radio and Ethernet ports. The default poll frequency is 2 seconds.

	Command	Purpose
Step 9	iapp standby timeout <i>seconds</i>	Sets the number of seconds the standby access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned. The default timeout is 20 seconds. Note You should increase the standby timeout setting if the bridged path between the standby and monitored access points can be lost for periods greater than 20 seconds (during spanning tree recalculation, for example). Note If the monitored access point is configured to select the least congested radio channel, you might need to increase the standby timeout setting. The monitored unit might take up to 40 seconds to select the least congested channel.
Step 10	iapp standby primary-shutdown	(Optional) Configures the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.
Step 11	show iapp standby-parms	Verify your entries. If the access point is in standby mode, this command displays the standby parameters, including the MAC address of the monitored access point and the poll-frequency and timeout values. If the access point is not in standby mode, <i>no iapp standby mac-address</i> appears.
Step 12	end	Return to privileged EXEC mode.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

After you enable standby mode, configure the settings that you recorded from the monitored access point to match on the standby access point.

Verifying Standby Operation

Use this command to check the status of the standby access point:

show iapp standby-status

This command displays the status of the standby access point. [Table 20-2](#) lists the standby status messages that can appear.

Table 20-2 Standby Status Messages

Message	Description
IAPP Standby is Disabled	The access point is not configured for standby mode.
IAPP—AP is in standby mode	The access point is in standby mode.

Table 20-2 Standby Status Messages (continued)

Message	Description
IAPP—AP is operating in active mode	The standby access point has taken over for the monitored access point and is functioning as a root access point.
IAPP—AP is operating in repeater mode	The standby access point has taken over for the monitored access point and is functioning as a repeater access point.
Standby status: Initializing	The standby access point is initializing link tests with the monitored access point.
Standby status: Takeover	The standby access point has transitioned to active mode.
Standby status: Stopped	Standby mode has been stopped by a configuration command.
Standby status: Ethernet Linktest Failed	An Ethernet link test failed from the standby access point to the monitored access point.
Standby status: Radio Linktest Failed	A radio link test failed from the standby access point to the monitored access point.
Standby status: Standby Error	An undefined error occurred.
Standby State: Init	The standby access point is initializing link tests with the monitored access point.
Standby State: Running	The standby access point is operating in standby mode and is running link tests to the monitored access point.
Standby State: Stopped	Standby mode has been stopped by a configuration command.
Standby State: Not Running	The access point is not in standby mode.

Use this command to check the standby configuration:

show iapp standby-parms

This command displays the MAC address of the standby access point, the standby timeout, and the poll-frequency values. If no standby access point is configured, this message appears:

```
no iapp standby mac-address
```

If a standby access point takes over for the monitored access point, you can use the **show iapp statistics** command to help determine the reason that the standby access point took over.

Understanding Workgroup Bridge Mode

You can configure the access point/bridge as a workgroup bridges. In workgroup bridge mode, the access point/bridge associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point/bridge Ethernet port, and configure the access point/bridge as a workgroup bridge. The workgroup bridge associates to an access point on your network.

There is no limit on the number of devices that you can connect to the workgroup bridge's Ethernet port. However, the connected devices share the bandwidth provided by the link from the workgroup bridge to the root access point or bridge.

**Caution**

An access point/bridge in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

**Note**

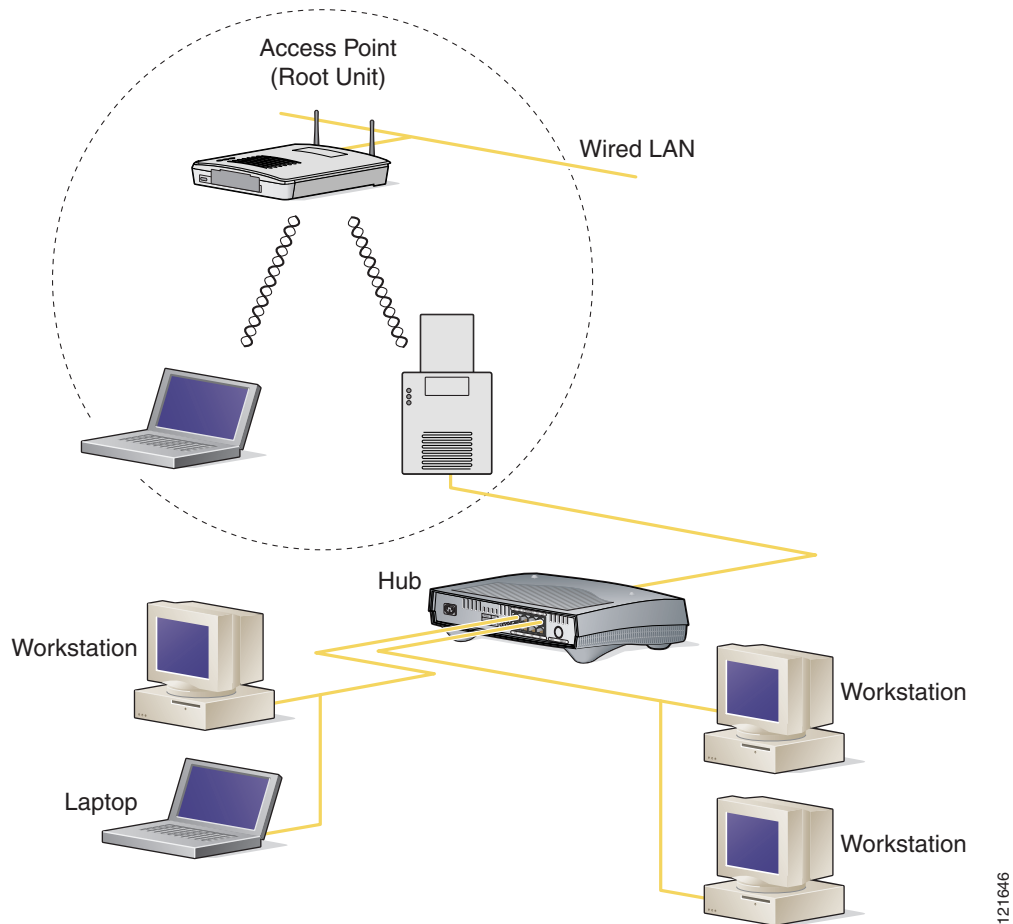
An access point/bridge in workgroup bridge mode can associate only to a Cisco Aironet access point or bridge.

**Note**

If multiple BSSIDs are configured on a root access point that is designated as the parent of a workgroup bridge, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a workgroup bridge on your wireless LAN is configured to associate to a specific parent, check the association status of the workgroup bridge when you add or delete BSSIDs on the parent access point.

Figure 20-2 shows an access point in workgroup bridge mode.

Figure 20-2 Access Point in Workgroup Bridge Mode



121646

Treating Workgroup Bridges as Infrastructure Devices or as Client Devices

The access point to which a workgroup bridge associates can treat the workgroup bridge as an infrastructure device or as a simple client device. By default, access points and bridges treat workgroup bridges as client devices.

For increased reliability, you can configure access points and bridges to treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge. You use the **infrastructure-client** configuration interface command to configure access points and bridges to treat workgroup bridges as infrastructure devices.

Configuring access points and bridges to treat a workgroup bridge as a client device allows more workgroup bridges to associate to the same access point, or to associate using an SSID that is not an infrastructure SSID. The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to an access point or bridge. To increase beyond 20 the number of workgroup bridges that can associate to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability. You use the **no infrastructure-client** configuration interface command to configure access points and bridges to treat workgroup bridges as simple client devices. This is the default setting.

You should use a workgroup bridge as an infrastructure device if the devices connected to the workgroup bridge require network reliability equivalent to that of an access point or a bridge. You should use a workgroup bridge as a client device if these conditions are true:

- More than 20 workgroup bridges associate to the same access point or bridge
- The workgroup bridge associates using an SSID that is not an infrastructure SSID
- The workgroup bridge is mobile

Configuring a Workgroup Bridge for Roaming

If your workgroup bridge is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use this command to configure the workgroup bridge as a mobile station:

```
BR(config)# mobile station
```

When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a workgroup bridge configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.

Configuring a Client VLAN

If the devices connected to the workgroup bridge's Ethernet port should all be assigned to a particular VLAN, you can configure a VLAN for the connected devices. Enter this command on the workgroup bridge:

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

All the devices connected to the workgroup bridge's Ethernet port are assigned to that VLAN.

Configuring Workgroup Bridge Mode

Beginning in privileged EXEC mode, follow these steps to configure an access point/bridge as a workgroup bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1}	Enter interface configuration mode for the radio interface.
Step 3	station-role workgroup-bridge	Set the radio role to workgroup bridge. If your access point contains two radios, the radio not set to workgroup bridge mode is automatically disabled.
Step 4	ssid <i>ssid-string</i>	Create the SSID that the workgroup bridge uses to associate to a parent access point or bridge.
Step 5	infrastructure-ssid	Designate the SSID as an infrastructure SSID. Note The workgroup bridge must use an infrastructure SSID to associate to a root access point or bridge.
Step 6	authentication client username <i>username</i> password <i>password</i>	(Optional) If the parent access point is configured to require LEAP authentication, configure the username and password that the workgroup bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the workgroup bridge on the authentication server.
Step 7	exit	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	parent {1-4} <i>mac-address</i> [<i>timeout</i>]	(Optional) Enter the MAC address for the access point to which the workgroup bridge should associate. <ul style="list-style-type: none"> You can enter MAC addresses for up to four parent access points. The workgroup bridge attempts to associate to MAC address 1 first; if that access point does not respond, the workgroup bridge tries the next access point in its parent list. Note If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted. <ul style="list-style-type: none"> (Optional) You can also enter a timeout value in seconds that determines how long the workgroup bridge attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	exit	Exit radio configuration mode and return to global configuration mode.

	Command	Purpose
Step 10	workgroup-bridge client-vlan <i>vlan-id</i>	(Optional) Specify the VLAN to which the devices that are connected to the workgroup bridge's Ethernet port are assigned.
Step 11	mobile station	(Optional) Configure the workgroup bridge as a mobile station. When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. When this setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.
Step 12	end	Return to privileged EXEC mode.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure an access point/bridge as a workgroup bridge. In this example, the workgroup bridge uses the configured username and password to perform LEAP authentication, and the devices attached to its Ethernet port are assigned to VLAN 22:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# station-role workgroup-bridge
ap(config-if)# ssid infra
ap(config-ssid)# infrastructure-ssid
ap(config-ssid)# authentication client username wgb1 password cisco123
ap(config-ssid)# exit
ap(config-if)# exit
ap(config)# workgroup-bridge client-vlan 22
ap(config)# end
```

