CHAPTER 19

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.

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 either the 2.4 GHz radio or the 5 GHz radio as a repeater. In access points with two radios, only one radio can be a repeater; the other radio must be shut down or be configured as a root, scanner, or spectrum radio.

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 an access point 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.

To use an SSID between an access point and a repeater, the **Infrastructure SSID** option has to be enabled on the SSID to allow AP to repeater communication.

The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN:

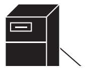
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

Note Access points create a virtual interface for each radio interface, and so repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

Note You cannot set a radio to act as a repeater and support other SSIDs at the same time. The repeater radio can only repeat the native VLAN. You cannot set a radio as a repeater, and then map to that radio an SSID that is mapped to a VLAN other than the native VLAN. However, the other radio can be configured to support several SSIDs and several VLANs.

Figure 19-1 shows an access point acting as a repeater.

Figure 19-1 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 19-4
- Guidelines for Repeaters, page 19-4
- Setting Up a Repeater, page 19-5
- Verifying Repeater Operation, page 19-7
- Aligning Antennas, page 19-6
- Setting Up a Repeater As a EAP-FAST Client, page 19-8
- Setting Up a Repeater As a WPA2 Client, page 19-7

Default Configuration

Access points are configured as root units by default. Table 19-1 shows the default values for settings that control the access point's role in the wireless LAN.

Table 19-1 Default Settings for Role in Wireless LAN

Feature	Default Setting
Station role	Root
Parent	none
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. When non-Cisco clients are expected, verify that these clients support the Aironet IE extension, as this option is required on the SSID to allow for the communication between an AP and a repeater.
- 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 e "Configuring Radio Data Rates" section on page 6-12.
- The SSID configured on the repeater radio must be mapped to the native VLAN.

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. Repeaters can join a WDS infrastructure and act as WDS clients whenever needed.

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. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

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 | 1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**ssid** *ssid-string*	Call 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. 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. The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN: `SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid`
Step 4	**station-role repeater**	Set the access point's role in the wireless LAN to repeater.
Step 5	**dot11 extension aironet**	If Aironet extensions are disabled, enable Aironet extensions.
Step 6	**parent** {*1-4*} *mac-address* [*timeout*]	(Optional) Enter the MAC address for the access point to which the repeater should associate. • You can enter MAC addresses for up to four parent access points, designated 1 to 4. The repeater always attempts to associate to the best access point from the list of its parent access points. The repeater does not associate with a MAC address that is not in its parent list unless you set the 'timeout' option. **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. • (Optional) You can enter a timeout value in seconds, which determines how long the repeater attempts to associate to an access point that is in its parent list. If the repeater fails to associate within the timeout period, it will try to associate to parent access points that are not from its parent list. You can enter a timeout value ranging from 0 to 65535 seconds.

	Command	Purpose
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The following example shows how to set up a repeater access point with three potential parents, designated 1 to 3:

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

This example shows how to remove a parent, here parent 2, from the parent list:

```
AP(config-if)# no parent 2
```

This example shows how to set a timeout of 60 seconds for the parent list:

```
AP(config-if)# parent timeout 60
```

This example shows how to disable the timeout value for the parent list:

```
AP(config-if)# no parent timeout
```

Aligning Antennas

When an access point is configured as a repeater, you can align its antenna with another remote antenna using the **dot11 antenna-alignment** CLI command.

The command invokes an alignment test. The radio disassociates from its parent, probes adjacent wireless devices, and records the MAC addresses and signal strengths of responses it receives. After the timeout, the radio reassociates with its parent.

Follow these steps to run an antenna alignment test:

	Command	Purpose
Step 1	**enable**	Enter privileged EXEC mod
Step 2	**dot11 dot11radio** { **0** | **1** } **antenna-alignment timeout** *timeout-in-seconds*	Enter interface configuration mode for the radio interface. • 0—For the 2.4-GHz radio and the 2.4-GHz 802.11n radio • 1—For the 5-GHz radio and the 5-GHz 802.11n radio. • *timeout-in-seconds*—Enter the time in seconds that the antenna alignment test runs before timing out. The default is 5 seconds.

Use the **show dot11 antenna-alignment** command to list the MAC addresses and signal level for the last 10 devices that responded to the probe.

Verifying Repeater Operation

After you set up the repeater, if your repeater is functioning correctly, the repeater access point should appear associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a WPA2 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 WPA2-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA2 client:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ssid** *ssid-string*	Associate the SSID to the radio interface.
Step 3	**authentication open**	Enable open authentication for the SSID.
Step 4	**authentication key-management wpa**	Enable WPA authenticated key management for the SSID.
Step 5	**infrastructure ssid**	Designate the SSID as the SSID that the repeater uses to associate to other access points.
Step 6	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	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 7	**exit**	Exit the SSID configuration sub-mode.
Step 8	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 9	**encryption mode ciphers aes-ccm**	Enable AES CCMP encryption on the radio interface.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Setting Up a Repeater As a EAP-FAST 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 can authenticate to your network, through the root AP, using user credentials.

Setting up a repeater as a EAP-FAST, or other 802.1x/EAP authentication-method client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure the authentication method to be supported 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 11, "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 802.1x/EAP client for the chosen method. The following example shows EAP-FAST configuration:

	Command	Purpose
Step 1	**eap profile** *profile-name*	Enter the name of a profile, that will be used by the repeater to determine which authentication method should be used.
Step 2	**method fast**	Configure EAP-FAST as the method to be used.
Step 3	**dot1x credentials** *name*	Configure user credentials that the repeater will use to authenticate to the wireless infrastructure.
Step 4	**username** *user-name*	Configure a username within the dot1x credentials.
Step 5	**password 0** *password*	Configure the password to use when the repeater will authenticate to the infrastructure.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**dot11 ssid** *ssid-name*	Create a new SSID.
Step 8	**authentication open eap eap_methods**	Allow Open+ EAP authentication (EAP-FAST or other).
Step 9	**authentication network-eap eap_methods**	Allow LEAP authentication. LEAP is not the method of choice in this example, but LEAP is the default method. You need to enable LEP to trigger the 802.1x/EAP process. The EAP profile will determine which method should actually be used.
Step 10	**authentication key-management wpa version 2**	Set key management to WPA version 2.
Step 11	**dot1x credentials** *name*	Use the dot1x credentials created in for when the repeater authenticates to the wireless infrastructure. The credentials defined in the dot1x credentials profile will be used.
Step 12	**dot1x eap profile EAP-only**	Use the EAP-only profile created above for when the repeater authenticates to the wireless infrastructure. The method defined in the eap profile, EAP-FAST in this example, will be used

	Command	Purpose
Step 13	**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 14	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 15	**ssid** *ssid-string*	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 16	**end**	Return to privileged EXEC mode.
Step 17	**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.

The standby access point monitors another access point in a device-to-device relationship, not in an interface-to-interface relationship. For example, you cannot configure the standby access point's 5-GHz radio to monitor the 5-GHz radio in access point alpha and the standby's 2.4-GHz radio to monitor the 2.4-GHz radio in access point bravo. You also cannot configure one radio in a dual-radio access point as a standby radio and configure the other radio to serve client devices.

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. If necessary, reconfigure the standby unit to use the BSSID's new MAC address.

Note Hot standby is not supported on the BR1410 configured for AP mode.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter radio mac address of the access point that the standby unit will monitor. To monitor access points with two radios, you need both radios MAC addresses. 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
- Security settings
- Authentication types and authentication servers
- Radios configuration and status

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 Chapter 20, "Working with Configuration Files," 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** *mac-address*	Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point. **Note** When you configure an access point with two radios to monitor an 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. If necessary, reconfigure the standby unit to use the BSSID's new MAC address. **Note** Hot standby is not supported on the BR1410 configured for AP mode.
Step 3	**iapp standby poll-frequency** *seconds*	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.
Step 4	**iapp standby timeout** *seconds*	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 5	**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.

	Command	Purpose
Step 6	**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, *no iapp standby mac-address* appears.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**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 19-2 lists the standby status messages that can appear.

Table 19-2 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.
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 access points as workgroup bridges, also termed as WGBs. In workgroup bridge (WGB) mode, the unit 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 Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network.

If your access point has two radios, either the 2.4-GHz radio or the 5-GHz radio can function in workgroup bridge mode. When you configure one radio interface as a workgroup bridge, the other radio remains up. However, both radios cannot be configured to operate simultaneously as a workgroup bridge. The other radio can either be disabled (shutdown), or be in root (access point or bridge), scanner, or spectrum mode.

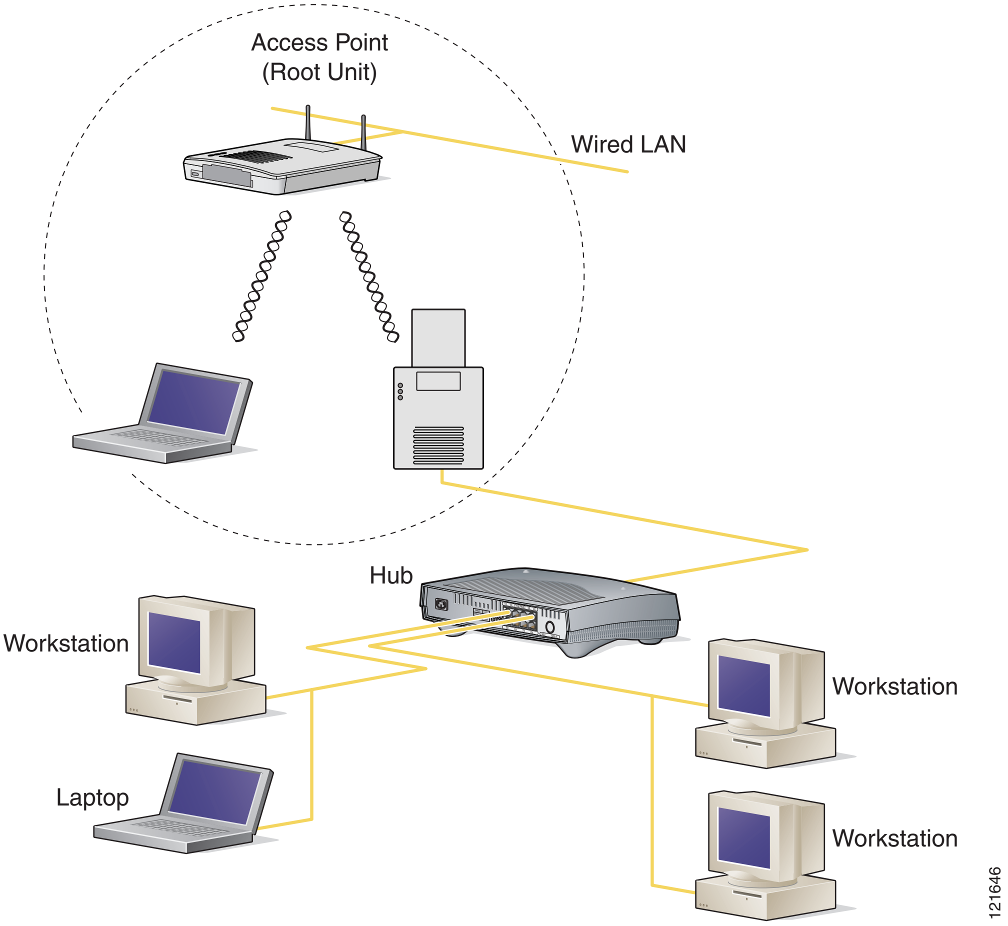
Caution An access point in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

Note 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. If necessary, reconfigure the workgroup bridge to use the BSSID's new MAC address.

Note Although it functions as a bridge, an access point in workgroup bridge mode has a limited radio range. Workgroup bridges do not support the **distance** setting, which enables you to configure wireless bridges to communicate across several kilometers.

Figure 19-2 shows an access point in workgroup bridge mode.

Figure 19-2 Access Point in Workgroup Bridge Mode



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 wired clients of workgroup bridges at the edge of the access point coverage area may not receive all multicast frames. 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

Please notice that the **(no) infrastructure client** command is entered on the access point to which the workgroup bridge associates. This command determines whether the access point should add unicast copies of each multicast frames, sent in a reliable (unicast with acknowledgment) fashion to each workgroup bridge in the cell.

When infrastructure client is configured on the access point, each workgroup bridge potentially receives both the multicast initial frame and the unicast copy. Processing both frames (carrying the same upper layer content) creates processing inefficiency on the workgroup bridge. You can configure the workgroup bridge to consider the multicast frame and discard the unicast copy (default), or consider the unicast frame and discard the multicast original frame. To configure this behavior on the workgroup bridge radio, use the command **station-role workgroup-bridge multicast mode {client | infrastructure}**. The client option considers the multicast frame and discards the unicast copy. The infrastructure option echoes the Infrastructure Client configuration on the main access point, and sets the workgroup bridge to consider the unicast copies of multicast frames, and not process the multicast frames.

Configuring a Workgroup Bridge for Roaming

By default, workgroup bridges are expected to be static. Therefore, once they are associated to an access point SSID, they do not scan for other access points.

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:

```
ap(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.

```
ap(config-if)#mobile station minimum-rate <data rate>
```

This is a configurable parameter to control when WGB triggers a new roaming event. If this cli is configured and if the current data rate is lower than the configured value, the new roaming process will be triggered. This will reduce unnecessary roaming and allows to have an expected rate value.

You can also configure the periodicity of scans. When the connection conditions deteriorate, the workgroup bridge scans for a better access point to connect to. If the scan does not allow the workgroup bridge to find a better connection point, use the **mobile station period** *number-of-seconds* command to determine the interval to the next scanning cycle.

Configuring a Workgroup Bridge for Limited Channel Scanning

In mobile environments such as railroads, a workgroup bridge instead of scanning all the channels will be restricted to scan only a set of limited channels in order to reduce the hand-off delay when the workgroup bridge roams from one access point to another. By limiting the number of channels the workgroup bridge scans to only those required, the mobile workgroup bridge achieves and maintains a continuous wireless LAN connection with fast and smooth roaming.

Configuring the Limited Channel Set

This limited channel set is configured using the **mobile station scan <set of channels>** CLI command to invoke scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels a radio can support. When executed, the workgroup bridge only scans this limited channel set. This limited channel feature also affects the known channel list that the workgroup bridge receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also a part of the limited channel set.

The following example shows how the command is used. In the example, channels 1, 6, and 11 are specified to scan:

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

Use the **no mobile station scan** command to restore scanning to all the channels.

Ignoring the CCX Neighbor List

In addition, the workgroup bridge updates its known channel list using CCX reports such as the AP Adjacent report or Enhanced Neighbor List report. However, when a workgroup bridge is configured for limited channel scanning, it does not need to process the CCX reports to update its known channel list. Use the **mobile station ignore neighbor-list** command to disable processing of CCX neighbor list reports. This command is effective only if the workgroup bridge is configured for limited scanning channel scanning. The following example shows how this command is used

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

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.

Workgroup Bridge VLAN Tagging

The Workgroup-Bridge (WGB) VLAN tagging feature enables segregation of VLAN traffic based on the VLAN numbers for Unified WGB solution.

When this feature is enabled, the WGB removes the 802.1q header while sending the packet from a VLAN client to the wireless LAN controller (WLC). WGB gets the packet to a VLAN client without 802.1q header and WGB code has to be modified to add the 802.1q header while forwarding the frame to the switch behind WGB.

WGB updates the WLC with the wired-client VLAN information in the Internet Access Point Protocol (IAPP) Association message. WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source-mac-address.

In the upstream direction, WGB removes the 802.1q header from the packet while sending to the WLC. In the downstream direction while forwarding the packet to the switch connecting the wired-client, the WLC sends the packet to WGB without the 802.1q tag and WGB adds a 4-byte 802.1q header based on the destination mac-address. (For detailed information on VLANs, refer to Chapter 14, "Configuring VLANs".)

Enter this command to enable WGB VLAN tagging:

```
WGB(config)#workgroup-bridge unified-vlan-client ?
        -replicate  Enable WGB broadcast to all vlans
        <cr>
```

Configuring Workgroup Bridge Mode

Beginning in privileged EXEC mode, follow these steps to configure an access point 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.

	Command	Purpose
Step 3	**station-role workgroup-bridge [universal** *mac-address***]**	Set the radio role to workgroup bridge. (Optional) When configured as a workgroup bridge, the access point sends specific messages to the primary access point to inform it about the MAC addresses of wired clients relayed through the workgroup bridge radio. When the primary access point is not a Cisco access point, these messages are not understood. To allow the workgroup bridge to successfully associate and communicate with a non-Cisco access point, you can use the **universal** optional argument. A restriction of this mode is that only one wired client is supported. When configuring this mode you need to configure the MAC address of the wired client, to which the traffic should be relayed through the workgroup bridge. Instead of sending the list of wired clients to the primary AP, the workgroup bridge will directly associate to the access point using the wired client's MAC address. If the wired client's MAC address is not found in the workgroup bridge's MAC address table, the workgroup bridge associates using its own MAC address. Then, when the wired client is connected and its MAC address appears in the workgroup bridge MAC address table, the WGB disassociates and then re-associates using the wired client's MAC address. This process supports non-Cisco access points that need a unique mapping between a wireless client and a MAC address.
Step 4	**station-role workgroup-bridge multicast mode {client | infrastructure}**	(Optional) When the primary access point is configured with the **infrastructure client** command, multicast frames are also sent to workgroup bridges via unicast. In such cases, the multicast frames relayed via unicast contain four MAC addresses in the header: Workgroup bridge unicast destination MAC address, Transmitting access point MAC address, Multicast destination MAC address, Original sender source MAC address). The original multicast frame header only contains three MAC addresses: Multicast destination MAC address, Transmitting access point MAC address, Original sender source MAC address. When using the **infrastructure client** command on the primary access point, use the station role workgroup-bridge multicast mode infrastructure to instruct the workgroup bridge to ignore the multicast frames and only process the relayed unicast copies of the multicast frames. Use the station role workgroup-bridge multicast mode client to instruct the workgroup bridge to only consider the standard frames, and ignore any relayed frame that would display four MAC addresses in the header. • client—Client-mode accepts only 3-MAC address header multicast packets • infrastructure—Infrastructure-mode accepts only 4-MAC address header multicast packets
Step 5	**ssid** *ssid-string*	Designates the SSID that the workgroup bridge should use to associate to a parent access point or a bridge.

	Command	Purpose
Step 6	**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 7	**authentication client username** *username* **password** *password*	(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 8	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 9	**parent** {*1-4*} *mac-address* [*timeout*]	(Optional) Enter the MAC address for the access point to which the workgroup bridge should associate. • You can enter MAC addresses for up to four parent access points, designated 1 to 4. The workgroup bridge always attempts to associate to the best access point from the list of its parent access points. The workgroup bridge does not associate with a MAC address that is not in its parent list unless you set the 'timeout' option. **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. • (Optional) You can enter a timeout value in seconds, which determines how long the workgroup bridge attempts to associate to an access point that is in its parent list. If the workgroup bridge fails to associate within the timeout period, it will try to associate to parent access points that are not from its parent list. You can enter a timeout value ranging from 0 to 65535 seconds.
Step 10	**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 11	**mobile station period** *number-of-seconds*	(Optional) When the signal to the access point to which the workgroup bridge is associated, deteriorates, the workgroup bridge scans for an alternate access point. If this scan is unsuccessful (i.e. no access point with a better signal was found), the number of seconds entered here will be the interval to the next scan attempt.

	Command	Purpose
Step 12	**mobile station minimum-rate** *rate*	(Optional) When a workgroup bridge scans for an alternate access point, this command determines the minimum data rate that should be achievable to the new access point in order for the workgroup bridge to consider the alternate access point as a potential connection point.
Step 13	**mobile station scan**	(Optional) Restricts the list of channels that the workgroup bridge should scan in search of an alternate access point.
Step 14	**mobile station ignore neighbor-list**	(Optional) When the workgroup bridge is configured to restrict the list of scanned channels, this command instructs the workgroup bridge to ignore the CCX neighbor list messages that indicate potential neighboring access points and their channel.
Step 15	**exit**	Exit radio configuration mode and return to global configuration mode.
Step 16	**workgroup-bridge client-vlan** *vlan-id*	(Optional) Specify the VLAN to which the devices that are connected to the workgroup bridge's Ethernet port are assigned.
Step 17	**end**	Return to privileged EXEC mode.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure an access point 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
```

This example shows how to set up a workgroup bridge with the parent access points, designated 1 and 2:

```
AP(config-if)# parent 1 0040.9631.81cf
AP(config-if)# parent 2 0040.9631.81da
```

This example shows how to remove a parent, here parent 2, from the parent list:

```
AP(config-if)# no parent 2
```

This example shows how to set a timeout of 60 seconds for the parent list:

```
AP(config-if)# parent timeout 60
```

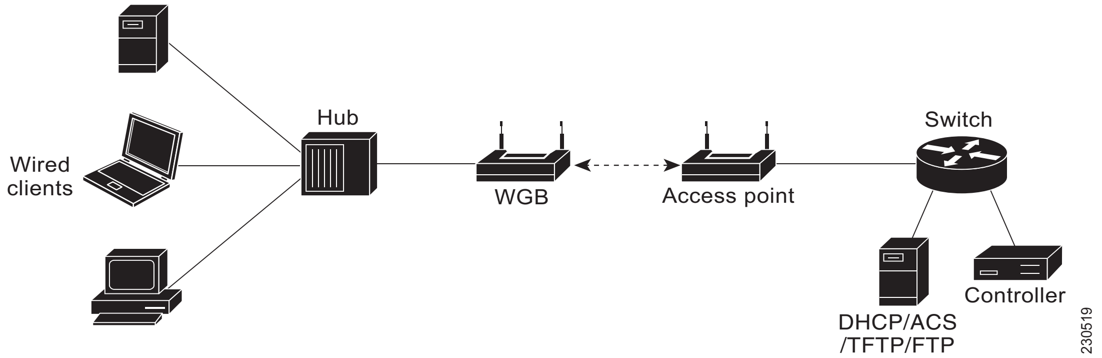
This example shows how to disable the timeout value for the parent list:

```
AP(config-if)# no parent timeout
```

Using Workgroup Bridges in a Lightweight Environment

You can configure an access point to operate as a workgroup bridge so that it can provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the workgroup bridge access point. A workgroup bridge connects to a wired network over a single wireless segment by learning the MAC address of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The workgroup bridge provides wireless access connectivity to wired clients by establishing a single connection to the lightweight access point. The lightweight access point treats the workgroup bridge as a wireless client.

Figure 19-3 Workgroup Bridge in a Lightweight Environment



Note If the lightweight access point fails, the workgroup bridge attempts to associate to another access point.

Guidelines for Using Workgroup Bridges in a Lightweight Environment

Follow these guidelines for using workgroup bridges on your lightweight network:

- The workgroup bridge can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release JA or greater (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or greater (on 16-MB access points). These access points include the AP1040, AP1140, and AP1260. Cisco IOS Releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

Note If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

Perform one of the following to enable the workgroup bridge mode on the workgroup bridge:

- On the workgroup bridge access point GUI, choose **Workgroup Bridge** for the role in radio network on the **Network > Network Interfaces > Radio0-802.11N 2.4GHz / Radio1-802.11N 5GHz > Settings** page.
  Alternatively, on the WGB access point CLI radio configuration submode, enter this command: **station-role workgroup-bridge**
- Only workgroup bridge in client mode (which is the default value) are supported. The lightweight access point will not relay multicast frames in a unicast fashion to associated workgroup bridges. Perform one of the following to enable client mode on the workgroup bridge:
  - On the radio configuration page, choose **Disabled** for the Reliable Multicast to workgroup bridge parameter.
  - From the radio configuration submode, enter this command: **no infrastructure client**.
- These lightweight features are supported for use with a workgroup bridge:
  - Guest N+1 redundancy
  - Local EAP
- These lightweight features are not supported for use with a workgroup bridge:
  - Cisco Centralized Key Management (CCKM)
  - Hybrid REAP
  - Idle timeout
  - Web authentication

Note If a workgroup bridge associates to a web-authentication WLAN, the workgroup bridge is added to the exclusion list, and all of the workgroup bridge wired clients are deleted.

- In a mesh network, a workgroup bridge can associate to any mesh access point, regardless of whether it acts as a root access point or a mesh access point.
- Wired clients connected to the workgroup bridge are not authenticated for security. Instead, the workgroup bridge is authenticated against the access point to which it associates. Therefore, We recommend that you physically secure the wired side of the workgroup bridge.
- With Layer 3 roaming, if you connect a wired client into the workgroup bridge network after the workgroup bridge has roamed to another controller (for example, to a foreign controller), the wired client’s IP address displays only on the anchor controller, not on the foreign controller.

- When you delete a workgroup bridge record from the controller, all of the workgroup bridge wired clients' records are also deleted.
- Wired clients connected to a workgroup bridge inherit the workgroup bridge's QoS and AAA override attributes.
- These features are not supported for wired clients connected to a workgroup bridge:
  - MAC filtering
  - Link tests
  - Idle timeout
- You do not need to configure anything on the controller to enable the workgroup bridge to communicate with the lightweight access point. However, to ensure proper communication, you should create a WLAN on the controller that matches the SSID and security method that was configured on the workgroup bridge.

Sample Workgroup Bridge Association Verification

To verify that the workgroup bridge is associated to an access point, enter this command on the workgroup bridge:

show dot11 association

If a wired client does not send traffic for an extended period of time, the workgroup bridge removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the workgroup bridge to a large value using the following IOS commands on the workgroup bridge:

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

where bridge-group-number is a value between 1 and 255, and seconds is a value between 10 and 1,000,000 seconds. We recommend configuring the seconds parameter to a value greater than the wired client's idle period.

Enabling VideoStream Support on Workgroup Bridges

VideoStream improves the reliability of an IP multicast stream by converting the multicast frame, over the air, to a unicast frame. Cisco IOS Releases 15.2(2)JA and later provide VideoStream support for wired devices connected to workgroup bridges. For access points running release 15.2(2)JA and later, the workgroup bridge is added to the wireless LAN controller (WLC) multicast table, and the workgroup bridge converts the VideoStream unicast frame into an Ethernet multicast frame and sends it out to its wired clients.

Enter this command on the WLC to enable VideoStream for workgroup bridges:

config media-stream wired-client enable

Configuring Workgroup Bridges for High-Speed Roaming

Consider the wireless network deployments which involve high-speed roaming of a workgroup bridge AP, such as in high-speed rail coaches. As the coaches move, the workgroup bridge AP in the coach roams from one parent AP (or root AP) to the next one mounted along the railway track. Such a scenario can involve trains moving at about 100 km/h, with the parent APs placed about 200-300m apart along the track.

For such scenarios ensure that the following configurations are done.

Note Configuring workgroup bridges for high-speed roaming scenarios is supported only on the Cisco Aironet 3600 and 3700 series, and the IW3700 series access points.

802.11v BSS Transition on the Wireless Controller

For high-speed roaming to work, on the wireless controller you must have 802.11v BSS Transition enabled. This allows for the workgroup bridge AP to request for and receive a neighbor list from the associated AP (i.e. the current parent AP). The workgroup bridge AP uses this list to identify the small set of channels on which it needs to scan to find the next parent AP.

Configuration on the WGB

To set how quickly a WGB detects that the current parent AP is suboptimal, while it is moving out of range, and that a roam needs to be initiated to discover the next parent AP, you can use the following command:
drssi roaming threshold *value* **period** *value* **packet** *value* **neighlist-update-interval** *value*

In this command:

- DRSSI roaming threshold is the RSSI threshold value. APs with RSSI values above this threshold are not considered for associating with.

  You are recommended to set the DRSSI roaming threshold to about 2 to 3 dBm below the average RSSI level in the middle point between two APs on the track. Note that a configured threshold of x, corresponding to -x dBm.
- Period controls how often the WGB decides to evaluate the quality of the link to the current parent. For example, if the train is moving very fast, you would like the WGB to evaluate the link quality more frequently. However if the speed is slow, the WGB can avoid frequent computations on evaluating the link quality.
- Packet is the threshold number of sample data packets from the current root AP that the WGB uses to keep track of the link quality with the AP. The WGB AP maintains a running average of the RSSI of the last received data packets from the root AP. If this running average falls below the threshold, the WGB initiates a roam. For example, if the train is moving very fast, a small number of samples can be used to decide when to switch.
- neighlist-update-interval is the time interval to update WGB neighbor list for roaming. It is used to trigger a periodic dot11v query to associated AP for that AP’s neighbor list. You can enter a value from 1 through 10000 in seconds. Default is 10 seconds.

As configured in the following example, a DRSSI roaming threshold value of 67, Period value of 1, and Packet value of 20 works well up to a speed of 100 km/h.

```
ap#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#int d0
ap(config-if)#drssi roaming threshold 67 period 1 packet 20
ap(config-if)#end
```

You can also set the workgroup bridge to scan only the neighbor list that is received from the last associated AP, using the following command:
drssi scan-only current-neighbor-list

You can also disable this above command so that the workgroup bridge ages out the neighbors list gradually - the age out factor is reduced by 1 for every roam. Default age is 2. To disable, use the command **no drssi scan-only current-neighbor-list**.

Note You can configure roaming by using either the **mobile station** command, or the **drssi** command. Make sure that you do not configure both commands at the same time.

Debug and Show commands

On the WGB, to view the current neighbor list table, use the following command:
show dot11 bss-trans neighbor-list

On the WGB, to enable debugging for 802.11v BSS transition:
debug dot11 dot11v {detail | errors | all}

Configuring Transparent Transporting of PROFINET Traffic

PROFINET is the PROFIBUS International (PI) open Industrial Ethernet Standard that uses TCP/IP and IT standards for automation control. PROFINET is particularly useful for industrial automation systems and process control networks. It emphasizes data exchange and defines communication paths to meet speed requirements.

PROFINET communication is scalable on three levels:

- Normal non-real-time communication uses TCP/IP and enables bus cycle times of approximately 100 ms. It is used for downloads, diagnostics, and management.
- Real-Time (RT): Real-time communication enables cycle times of approximately 10 ms. It is used to control traffic, time critical alarms and messaging. Real-time data are treated with a higher priority than TCP(UDP)/IP data. It uses the standard existing protocol components (using Ethernet with special frame etherType = 0x8892 and priority value in the VLAN tag) to achieve deterministic and cyclic data transfer.
- Isochronous Real-Time (IRT): Isochronous real-time communication enables cycle times of approximately 1 ms. The main focus of IRT is the ‘timing’ of the communication that requires precisely controlled communication. It is achieved using specialized hardware and the IEEE 1588-PTP protocol. IRT is out of the scope of this document.

PROFINET I/O is a modular communication framework for distributed automation applications. PROFINET I/O uses cyclic data transfer to exchange data, alarms, and diagnostic information with programmable controllers, input/output (I/O) devices, and other automation controllers (for example, motion controllers).

This feature implements the ability of transparent PROFINET RT traffic over wireless on the IW3700 Series. With this feature, PROFINET RT traffic, including PROFINET Class of Service (CoS) value, can be transparently relayed via Wi-Fi network.

Note Both flexconnect mode and autonomous mode are supported for this feature.

Figure 19-4 shows a topology of autonomous AP and WGB configuration.

Two vlans are configured on the autonomous AP. The native vlan (vlan 0) is used for the connection of autonomous AP. The PROFINET packets, between the IE Switch and autonomous AP, are transfered in vlan x. The wireless PROFINET traffic will be in the corresponding Access Category (AC) queue according to the CoS value. The WGB connects to the IO Device directly. The downstream is untagged, and the upstream uses vlan 0 to express the CoS priority.

Figure 19-4 Autonomous AP (root AP and WGB)

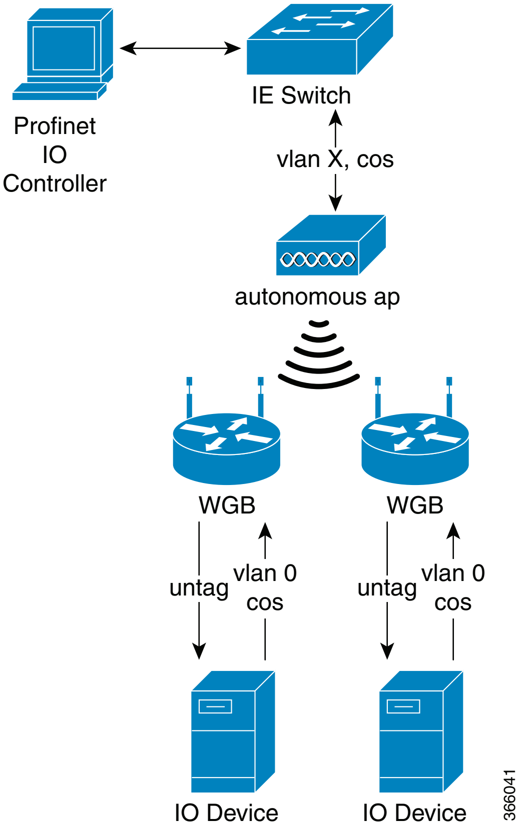
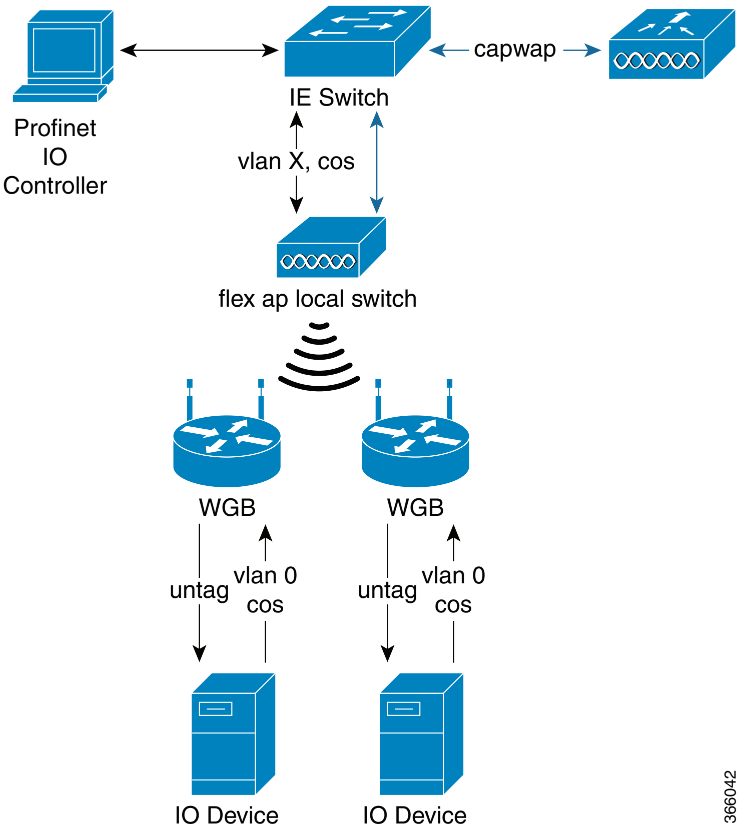


Figure 19-5 shows a topology of unified AP local switching configuration. The WLC communicates with the AP by capwap packets to exchange the control messages. The green lines and arrows are Profinet data flows. The black lines and arrows are capwap control packet flows.

Figure 19-5 Unified AP Local Switching



Configuration Examples

This section contains configuration examples for autonomous AP and WGB. In the following examples, native vlan 201 is used for control messages. Vlan 203 is used for Profinet.

Autonomous AP Configuration

Follow these steps to configure the autonomous AP:

Step 1 Create an ssid #Profinet in vlan 203.

```
ap(config)#dot11 ssid #Profinet
ap(config-ssid)#vlan 203
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii 0 12345678
ap(config-ssid)#exit
```

Step 2 Align the ssid #Profinet to dot11 5G.

```
ap(config)#interface d1
ap(config-if)#encryption vlan 203 mode ciphers aes-ccm
ap(config-if)#ssid #Profinet
ap(config-if)#station-role root
```

Step 3 Create a vlan bridge

```
ap(config)#interface Dot11Radio1.201
ap(config-subif)#encapsulation dot1Q 201 native
ap(config-subif)#exit

ap(config)#interface Dot11Radio1.203
ap(config-subif)#encapsulation dot1Q 203
ap(config-subif)#bridge-group 203
ap(config-subif)#exit

ap(config)#interface GigabitEthernet0.201
ap(config-subif)#encapsulation dot1Q 201 native
ap(config-subif)#exit

ap(config)#interface GigabitEthernet0.203
ap(config-subif)#encapsulation dot1Q 203
ap(config-subif)#bridge-group 203
ap(config-subif)#exit
```

WGB Configuration

Follow these steps to configure the WGB:

Step 1 Create the ssid #Profinet in the native vlan.

```
wgb(config)#dot11 ssid #Profinet
wgb(config-ssid)#authentication open
wgb(config-ssid)#authentication key-management wpa version 2
wgb(config-ssid)#wpa-psk ascii 0 12345678
wgb(config-ssid)#exit
```

Step 2 Align the ssid #Profinet to dot11.

```
wgb(config)#interface d1
wgb(config-if)#encryption mode ciphers aes-ccm
wgb(config-if)#ssid #Profinet
```