



Using Cisco Workgroup Bridges

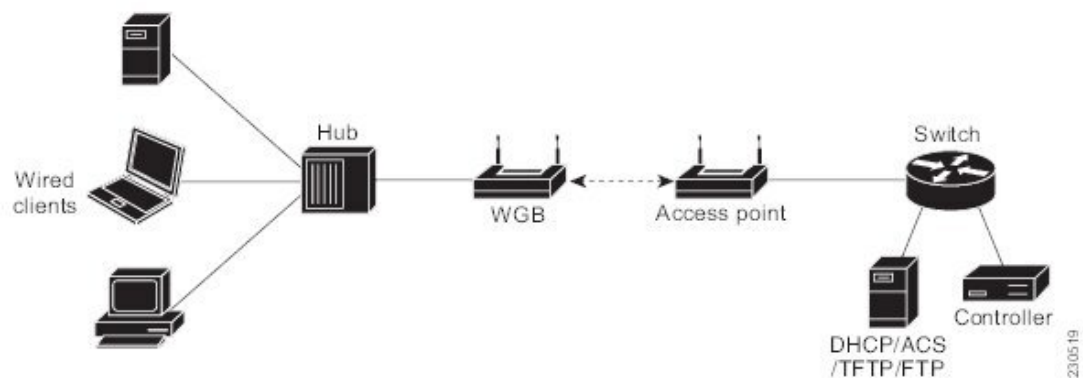
- [Information About Cisco Workgroup Bridges, on page 1](#)
- [Guidelines and Restrictions for Cisco Workgroup Bridges, on page 3](#)
- [WGB Configuration Example, on page 4](#)
- [Viewing the Status of Workgroup Bridges \(GUI\), on page 4](#)
- [Viewing the Status of Workgroup Bridges \(CLI\), on page 5](#)
- [Debugging WGB Issues \(CLI\), on page 5](#)

Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point. The lightweight access point treats the WGB as a wireless client.

A Cisco IOS AP as a WGB using the Cisco IOS 15.2 or later releases support Protected Extensible Authentication Protocol (PEAP) with the controller.

Figure 1: WGB Example





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

The following are some guidelines for Cisco Workgroup Bridges:

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. 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.

Enable the workgroup bridge mode on the WGB as follows:

- On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.
 - On the WGB access point CLI, enter the **station-role workgroup-bridge** command.
-



Note See the sample WGB access point configuration in the [WGB Configuration Example](#) section.

- The following features are supported for use with a WGB:
 - Guest N+1 redundancy
 - Local EAP
 - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, and EAP-TLS authentication modes
- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.
- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must disable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

Guidelines and Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with Cisco lightweight access points.
- The following features are not supported for use with a WGB:
 - Idle timeout
 - Web authentication
- Aironet WGBs are not supported if the parent AP is configured for FlexConnect local switching with local authentication, if the parent AP is a Wave 2 AP (that is, 802.11ac Wave 2 or 802.11ax). For more information, see [CSCvh22645](#).
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB 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.
- If a wired client does not send traffic for an extended period of time, the WGB 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 WGB to a large value using the following Cisco IOS commands on the WGB:

```
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.

- When you deauthenticate a WGB record from a controller, all of the WGB wired clients' entries are also deleted.
- These features are not supported for wired clients connected to a WGB:
 - MAC filtering
 - Link tests
 - Idle timeout
- The broadcast forwarding toward wired WGB clients works only on the native VLAN. If additional VLANs are configured, only the native VLAN forwards broadcast traffic.
- Associating a WGB to a WLAN that is configured for Adaptive 802.11r is not supported.

WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

```
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# dot11 ssid WGB_with_static_WEP
ap(config-ssid)# authentication open
ap(config-ssid)# guest-mode
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
ap(config)# station-role workgroup-bridge
ap(config-if)# encry mode wep 40
ap(config-if)# encry key 1 size 40 0 1234567890
ap(config-if)# ssid WGB_with_static_WEP
ap(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

show dot11 association

Information similar to the following appears:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address      IP address      Device          Name           Parent          State
000b.8581.6aee  10.11.12.1     WGB-client     map1           -               Assoc
ap#
```

Viewing the Status of Workgroup Bridges (GUI)

Step 1 Choose **Monitor > Clients** to open the Clients page.

The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB” if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

Step 3 See the details of any wired clients that are connected to a particular WGB as follows:

- a) Click **Back** on the Clients > Detail page to return to the Clients page.
- b) Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

Note If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

- c) Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB Client,” and the rest of the text boxes on this page provide additional information for this client.

Viewing the Status of Workgroup Bridges (CLI)

Step 1 See any WGBs on your network by entering this command:

```
show wgb summary
```

Step 2 See the details of any wired clients that are connected to a particular WGB by entering this command:

```
show wgb detail wgb_mac_address
```

Debugging WGB Issues (CLI)

Before you begin

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
 - **debug iapp all enable**—Enables debugging for IAPP messages.
 - **debug iapp error enable**—Enables debugging for IAPP error events.
 - **debug iapp packet enable**—Enables debugging for IAPP packets.
- Debug an roaming issue by entering this command:
debug mobility handoff enable
- Debug an IP assignment issue when DHCP is used by entering these commands:
 - **debug dhcp message enable**
 - **debug dhcp packet enable**
- Debug an IP assignment issue when static IP is used by entering these commands:
 - **debug dot11 mobile enable**
 - **debug dot11 state enable**

