Cisco WGBs

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.
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.

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.

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.
Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with lightweight access points.
- Only WGBs in client mode (which is the default value) are supported. Those WGBs in infrastructure mode are not supported. Perform one of the following to enable client mode on the WGB:
  - On the WGB access point GUI, choose **Disabled** for the Reliable Multicast to WGB parameter.
  - On the WGB access point CLI, enter the **no infrastructure client** command.

  

  Note  
  VLANs are not supported for use with WGBs.

- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication

  

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

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.
- The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied.
- 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 delete a WGB record from the controller, all of the WGB wired clients’ records 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.

• Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the `config wgb vlan enable` command.

• The `dot11 arp-cache` global configuration command that you can enter on the access point that is in WGB mode is not supported.

• WGB clients do not show enc-cipher and AKM because they are wired clients. WGB APs, however, show correct values of enc-cipher and AKM.

**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-if)# 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)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Monitor &gt; 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the MAC address of the desired client. The Clients &gt; 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.</td>
</tr>
</tbody>
</table>
| 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.  
  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)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>See any WGBs on your network by entering this command: show wgb summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>See the details of any wired clients that are connected to a particular WGB by entering this command: show wgb detail wgb_mac_address</td>
</tr>
</tbody>
</table>

Debugging WGB Issues (CLI)

Before you begin

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
Third-Party WGBs and Client VMs

Information About Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller drops the following types of messages:

• ARP REQ from the distribution system for the WGB client
• ARP RPLY from the WGB client
• DHCP REQ from the WGB client
• DHCP RPLY for the WGB client

The following are some guidelines for non-Cisco workgroup bridges:

• The controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the work group bridge to the access point.

Note
For FlexConnect APs in local switching, non-Cisco workgroup-bridge clients in bridged mode are supported using the `config flexconnect group group-name dhcp overridden-interface enable` command.
• When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.

• If you have clients that use PC virtualization software such as VMware, you must enable this feature.

![Note](image)

We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

• You must enable the passive client functionality for all non-Cisco workgroup bridges.

• You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the `config dhcp proxy disable` command.
  - Enable DHCP boot broadcast by using the `config dhcp proxy disable bootp-broadcast enable` command.

### Restrictions for Non-Cisco Workgroup Bridges

- Only Layer 2 roaming is supported for WGB devices.
- Layer 3 security (web authentication) is not support for WGB clients.
- Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
- ARP poisoning detection does not work on a WLAN when the flag is enabled.
- VLAN select is not supported for WGB clients.
- Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the `config dhcp proxy disable` and `config dhcp proxy disable bootp-broadcast disable` commands.

The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.