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.

*Figure 1: WGB Example*
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:

```plaintext
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.

**Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs**

Cisco Wireless LAN Controller (WLC) Release 8.3 provides an enhancement to broadcast traffic support on multiple 802.1Q VLAN workgroup bridge (WGB) deployments that traverse mesh networks and in Local mode. Specifically, support for WGB downstream broadcasts over multiple VLANs (to differentiate and prioritize traffic); and, bridging of VLAN traffic to wired clients connected to the WGB. Applications for this functionality are commonly found in the transportation and mining industries. For more information, see CSCub87583.

Supported platforms:
• Access point (AP) and WGB support:
  • IW3700 Series
  • 1552H/SA/SD Series

Supported AP mode:
• Local mode
• Bridge mode
Prerequisites

You need to create the dynamic interfaces and bind them to the interface group before you proceed with the configuration.

1. Create the dynamic interfaces, by choosing \texttt{CONTROLLER > Interfaces > New} on WLC. Add any dynamic interface that needs to support the downstream broadcast on Multiple VLANs feature into the interface group.

2. Bind the dynamic interfaces with Interface Groups, by choosing \texttt{CONTROLLER > Interface Groups > Add Group} on WLC.

3. Bind the Interface Groups to WLAN. Choose \texttt{WLAN}. Under the specific WLAN General confirmation tab, choose the proper interface group.

Cisco Wireless Controller Configuration (CLI Only)

To enable or disable the downlink broadcast packet VLAN tagging on a WLAN (new command):

\begin{verbatim}
(Cisco Controller) \texttt{>config wlan wgb broadcast-tagging \{enable | disable\} wlan-id}
\end{verbatim}

\textbf{Note}

This feature is disabled by default.

\textbf{Note}

To enable this feature, you need to enable \texttt{Broadcast Forwarding} on WLC, by choosing \texttt{Controller > General} and choose \texttt{Enabled} from the \texttt{Broadcast Forwarding} drop-down list.
To enable this feature, you should also configure the AP Multicast Mode to Multicast rather than Unicast, by clicking **Controller > General > AP Multicast Mode** and choosing **Multicast**, and then assign Multicast Group Address.

**WGB Configuration (CLI Only)**

You can configure the following on Workgroup Bridges:

- Broadcast Tagging
- Native VLANs

By default, Broadcast Tagging is disabled.

By default, only Native VLAN broadcasts can be forwarded to wired clients in Native VLANs.

You use the no command to disable VLAN configurations on the WGB as shown in the examples below.

When you have multiple VLAN configurations on WGB, you need to configure the encryption cipher mode and keys as the following example shows:

```
encryption vlan 861 mode ciphers aes-ccm
encryption vlan 862 mode ciphers aes-ccm
encryption vlan 864 mode ciphers aes-ccm
```

Then, you should configure the encryption cipher mode globally on the multicast or broadcast interface by entering the following command:

```
encryption mode ciphers aes-ccm
```

**VLAN Broadcast Tagging Configuration**

- To enable broadcast tagging on a VLAN (new command):
  ```
  (WGB) (config)# workgroup-bridge unified-vlan-client broadcast-tagging
  ```

- To disable broadcast tagging on a VLAN:
  ```
  (WGB) (config)# no workgroup-bridge unified-vlan-client broadcast-tagging
  ```

The **no workgroup-bridge unified-vlan-client broadcast-tagging** command will disable **workgroup-bridge unified-vlan-client** as well. Make sure you have **workgroup-bridge unified-vlan-client** configured properly to enable the multiple vlan feature.
Parallel Redundancy Protocol Enhancement on AP and WGB

Cisco Wireless Release 8.4 provides the Parallel Redundancy Protocol (PRP) enhancement to improve wireless network availability for wired clients behind Workgroup Bridge (WGB), and improve the roaming performance by allowing wired clients to have dual wireless connections.

PRP allows a data communication network to prevent data transmission failures by providing two alternate paths for the traffic to reach its destination. Two Ethernet networks (LANs) with similar topology are completely separated.

A device that requires protection for data across the network connects to the two independent networks (LAN-A and LAN-B) is called a Dual Attached Node implementing PRP (DANP). A DANP source sends two frames simultaneously on both LANs. A DANP destination receives both frames and discards the duplicating. If one LAN fails, a DANP destination can still receive a frame from the other LAN.

Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs). A Redundancy Box (RedBox) is used when a single interface node must be attached to both networks. Such a node can communicate with all other nodes. The switch implements RedBox functionality is a PRP switch.

To implement the PRP function for this release, you need to connect the AP and WGB to a PRP switch. The PRP switch is to offload PRP processing. AP or WGB is to keep dual wireless connections. You can have two WGBs interconnected through an external PRP switch and wirelessly connected to a single fixed AP or two fixed APs. Two WGBs can roaming between APs. Redundant packet transmissions can be supported over either single or both 2.4 GHz and 5 GHz. The infrastructure side also needs a PRP switch for AP side.

For the application where both WGBs may roam at the same time, the roaming coordination feature is introduced to avoid roaming gaps and guarantee staggered roaming. In this release, only dual radio links roaming coordination across two WGBs is supported for roaming coordination.

Supported platforms and AP mode:

- WLC and AP on the infrastructure side—FlexConnect AP mode (central authentication, local switching), the following IOS based platforms are supported: IW3702, 2700, 3700, and 1570 series.
- WGB on the client side—Only supported for IW3700 Series
- Roaming coordination—Only supported for IW3700 Series

Sample Network Configuration

General guidelines for this configuration:

- Separation of expected redundancy in the network:
  - Traffic expecting redundancy mapped to two reserved SSID A and SSID B each with specified VLAN.
  - Each WGB is configured to connect either SSID A or SSID B.
  - Others traffic without expectation of redundancy is recommended to be mapped to other SSID.

- WGB supports unified VLAN function and it is recommended that wired clients not to use VLANs assigned to SSID A or SSID B.

- Wired clients connected to WGB are source and recipients of redundancy traffic.
The following figure shows a topology of concurrent wireless transmission via two WGBs paired with one PRP switch, commonly used in train transportation.

On the train side, the PRP switch (in this example, Cisco IE2000U) duplicates upstream packets and sends both packets simultaneously via two different ports, Gi0/1 and Gi0/2. The dual packets will pass from different WGBs or APs, to ensure that at least one packet reaches the destination. On the track side, one more PRP switch is added to each aggregating endpoint along the track. The PRP switch on the track side will remove the duplicating for upstream packets. The same redundancy for downstream packet is also available by the pair of PRP switches.

The throughput of this solution depends on the network elements depicted in the diagram. Each element along the wired and wireless transmission path should validate its throughput to avoid being the throughput bottleneck.

**Figure 3: Concurrent Wireless Transmission via Two WGBs Paired With One PRP Switch**

**WLC Configuration (CLI Only)**

To enable or disable PRP on a WLAN (new command):

```
(Cisco Controller)> config wlan wgb prp {enable|disable} <wlan id>
```

- **enable**: Enable Parallel Redundancy Protocol (PRP) feature on a WLAN
- **disable**: Disable Parallel Redundancy Protocol (PRP) feature on a WLAN

This feature is disabled by default.

This CLI will enable two WLANs to allow dual associations in flex-connect mode. It will also enable the AP to forward packets to or from WGB wired clients with double tags in flex-connect mode.

**Note**

To enable unified VLANs in the WGB, the existing command `config wgb vlan enable` should also be executed. You should configure the inner VLAN (VLAN for wired client) on WLC as well.
**WGB Configuration for Roaming Coordination (CLI Only)**

For Parallel Redundancy Protocol (PRP), wired client traffic will be duplicated to transmit in dual radio links in two WGBs. Dual radio links without any radio link coordination have the possibility to trigger roaming at the same time, so that the traffic will be broken in a short window time.

The following figure is a typical PRP scenario of train transportation. AP like IW3702 has two physical Ethernet ports. Gig0 will be exclusively used to bridge PRP traffic. Gig1 will be used for internal communication. Gig 1 will connect to a non-PRP port on the PRP switch or connect to a peer Gig1 port directly.

*Figure 4: Peer Link Between Two WGBs*

**Configuration of Dual Radio Coordination on Two WGBs**

Follow these steps to configure dual radio coordination on two WGBs:

1. **Configure service VLAN.**
   
   Use the following command to enable the service VLAN traffic that will be punted to local handling process for sub interface on Gig0 or Gig1.
   
   ```
   WGB(config)# workgroup-bridge service-vlan <vlan id>
   ```

2. **Configure peer coordinator address.**
   
   Use the following commands to set peer coordinator address and create the coordination communication process. For example, if you have configured the service VLAN to 50, you should configure the local/peer coordinator address under sub interface 50.
   
   ```
   WGB(config)# interface GigabitEthernet1.50
   WGB(config-subif)# encapsulation dot1q 50
   WGB(config-subif)# ip coordinator peer-addr <addr>
   ```

3. **Configure dot11 radio coordinator on two WGBs.**
   
   Use the following commands to create dot11 coordinator process, and enable dot11 roaming coordinator service on radio 0 or radio 1.
   
   ```
   WGB(config)# dot11 coordinator uplink single [radio 0|radio 1]
   ```

4. **Configure dot11 coordination roaming waiting timer.**
   
   Use the following command to set the dot11 coordination roaming waiting timer. The default is 100ms.
   
   ```
   WGB(config)# dot11 coordinator timeout roam-wait [value]
   ```

5. **Configure Dot11 roaming coordination bypass.**
   
   Use the following command to bypass roaming coordination decision on WGB. When configured, it is used to collect WGB’s roaming conflict statistics, and will not affect the current roaming behavior.
WGB(config)# dot11 coordinator bypass

6. Configure to avoid bridge loop.

Wired network on WGB side can introduce a bridge loop if you connect the Gig1 port of WGBs directly or via a switch. The following sample configurations can avoid the bridge loop.

---

**Note**

The coordination traffic is forwarded on service VLAN and will not be blocked.

- To avoid bridge loop when connecting the Gig1 port of WGBs directly, configure the following on both WGBs:

  ```
  WGB(config)# access-list 700 deny 0000.0000.0000 ffff.ffff.ffff
  WGB(config)# interface gigabitEthernet 1
  WGB(config-if)# l2-filter bridge-group-acl
  WGB(config-if)# bridge-group 1
  WGB(config-if)# bridge-group 1 output-address-list 700
  ```

- To avoid traffic loop when connecting two WGBs via a switch, configure the following on the switch port:

  ```
  interface GigabitEthernet0/3
  switchport trunk allowed vlan 50
  switchport mode trunk

  interface GigabitEthernet0/4
  switchport trunk allowed vlan 50
  switchport mode trunk
  ```

---

**WLC Configuration**

**Note**

For more information about WLC configuration for FlexConnect, see the FlexConnect Chapter in the *Cisco Wireless Controller Configuration Guide*.

Follow these steps to configure the wireless controller for FlexConnect:

1. Create two WLANs with the SSID PRP1 and PRP2.

2. Enable local switching for each WLAN.

**Note**

For any wired client within the service VLAN, you need to create a corresponding dynamic interface with the same service VLAN on WLC.

---

**Configuration of AP**

1. Configure AP to FlexConnect mode and join WLC.

2. Enable VLAN support on each AP, and make sure PRP SSID is included.
Configuration of WGBs

- WGB1 Configuration

```plaintext
hostname WGB1
dot11 ssid PRP1
  vlan 801
  authentication open
interface Dot11Radio1
  no ip address
  ssid PRP1
  antenna gain 0
  stbc
  beamform ofdm
  station-role workgroup-bridge
interface Dot11Radio1.800
  encapsulation dot1Q 800
  bridge-group 2
  bridge-group 2 spanning-disabled
interface Dot11Radio1.801
  encapsulation dot1Q 801 native
  bridge-group 1
  bridge-group 1 spanning-disabled
interface GigabitEthernet0
  no ip address
  duplex auto
  speed auto
interface GigabitEthernet0.800
  encapsulation dot1Q 800
interface GigabitEthernet0.801
  encapsulation dot1Q 801 native
interface BVI1
  mac-address 4c00.821a.c0b0
  ip address dhcp
  ipv6 address dhcp
  ipv6 address autoconfig
  ipv6 enable
  bridge 1 route ip
workgroup-bridge unified-vlan-client
```

- WGB2 Configuration

```plaintext
hostname WGB2
dot11 ssid PRP2
  vlan 802
  authentication open
interface Dot11Radio1
  no ip address
interface Dot11Radio1
  ssid PRP2
  antenna gain 0
  stbc
```
beamform ofdm
station-role workgroup-bridge

interface Dot11Radio1.800
  encapsulation dot1q 800
  bridge-group 2
  bridge-group 2 spanning-disabled

interface Dot11Radio1.802
  encapsulation dot1q 802 native
  bridge-group 1
  bridge-group 1 spanning-disabled

interface GigabitEthernet0
  no ip address
duplex auto
  speed auto

interface GigabitEthernet0.800
  encapsulation dot1q 800

interface GigabitEthernet0.802
  encapsulation dot1q 802 native
  bridge-group 1

interface BVI1
  mac-address f872.eae4.a4d8
  ip address dhcp
  ipv6 address dhcp
  ipv6 address autoconfig
  ipv6 enable
  bridge 1 route ip
  workgroup-bridge unified-vlan-client

Aggregated Switch Configuration

Agg-SW# show run int fa 1/0/1
description ***AP1***
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 201
  switchport trunk allowed vlan 201,801,802
  switchport mode trunk

Agg-SW# show run int fa 1/0/3
Building configuration...

Current configuration : 196 bytes

Agg-SW# show run int fa 1/0/7
Building configuration...
Current configuration : 178 bytes
!
interface FastEthernet1/0/7
  description ***PRP-Track-SW***
  switchport access vlan 801
  switchport trunk encapsulation dot1q
  switchport mode dot1q-tunnel
  no cdp enable
end

Agg-SW# show run int fa 1/0/8
Building configuration...

Current configuration : 178 bytes
!
interface FastEthernet1/0/8
  description ***PRP-Track-SW***
  switchport access vlan 802
  switchport trunk encapsulation dot1q
  switchport mode dot1q-tunnel
  no cdp enable

PRP Switch Configuration

interface PRP-channel1
  switchport mode trunk
interface GigabitEthernet0/1
  switchport mode trunk
  no ptp enable
  no cdp enable
  prp-channel-group 1
!
interface GigabitEthernet0/2
  switchport mode trunk
  no ptp enable
  no cdp enable
  prp-channel-group 1

Note

Verifying the PRP Configurations

Follow these steps to verify the PRP configurations:

Before you begin

- Create an SVI interface on the train side PRP switch with service vlan: 800.
- Configure the SVI interface on the track side PRP switch with service vlan: 800, and create the DHCP pool.
**Procedure**

**Step 1**
On the train side PRP switch, use the following command to check whether an IP address has been assigned to Vlan 800 from the DHCP pool on the track side.

**Example:**

```
PRP-Train-SW# show ip int bri
Interface   IP-Address  OK? Method Status   Protocol
Vlan1       unassigned  YES NVRAM administratively down down
Vlan800     10.10.80.67 YES DHCP    up
```

**Step 2**
On the track side PRP switch, use the following command to display ingress packet statistics. In this example, LAN A and LAN B both have one packet.

**Example:**

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
  ingress pkt lan a: 1
  ingress pkt lan b: 1
  ingress crc lan a: 0
  ingress crc lan b: 0
  ingress danp pkt acpt: 0
  ingress danp pkt dscrd: 0
  ingress supfrm rcv a: 0
  ingress supfrm rcv b: 0
  ingress over pkt a: 0
  ingress over pkt b: 0
  ingress pri over pkt_a: 0
  ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
  ingress pkt_lan a: 0
  ingress pkt_lan b: 0
  ingress crc lan a: 0
  ingress crc lan b: 0
  ingress danp pkt acpt: 0
  ingress danp pkt dscrd: 0
  ingress supfrm rcv a: 0
  ingress supfrm rcv b: 0
  ingress over pkt a: 0
  ingress over pkt b: 0
  ingress pri over pkt a: 0
  ingress pri over pkt b: 0
```

**Step 3**
On the train side PRP switch, ping the track side with the following command, to send 5 packets from the train to the track side:

**Example:**

```
PRP-Train-SW# ping 10.10.80.1
<= issue ping from train to track side, 5 pkts
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.80.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```
Step 4  
On the track side PRP switch, use the following command to display the number of packets that LAN A and LAN B have received, and the number of duplicated packets that have been discarded. In this example, after receiving 5 packets, both LAN A and LAN B have 6 packets in total.

Example:

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
ingress pkt lan a: 6 <= LAN A receives 5 pkts
ingress pkt lan b: 6 <= LAN B receives 5 pkts
ingress crc lan a: 0
ingress crc lan b: 0
ingress danp pkt acpt: 5
ingress danp pkt dscrd: 5 <= discard 5 duplicate pkts
ingress supfrm rcv a: 0
ingress supfrm rcv b: 0
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt_a: 0
ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
ingress pkt_lan a: 0
ingress pkt_lan b: 0
ingress crc lan a: 0
ingress crc lan b: 0
ingress danp pkt acpt: 0
ingress danp pkt dscrd: 0
ingress supfrm rcv a: 0
ingress supfrm rcv b: 0
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt_a: 0
ingress pri over pkt_b: 0
```

---

**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静态_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:

```plaintext
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**

**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)**

**Procedure**

**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 a 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`

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

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.