Workgroup Bridges

Cisco Workgroup Bridges

A workgroup bridge (WGB) is an Access Point (AP) mode to provide wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP. 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 WLC through infrastructure AP using Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

Figure 1: Example of a WGB
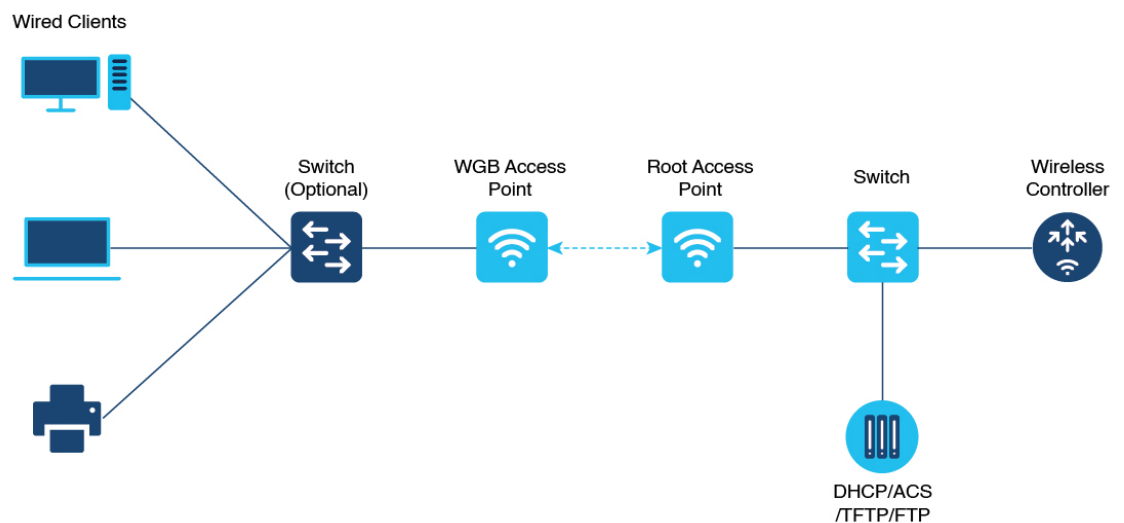
The mode supported in WGB for Embedded Wireless Controller is:

- Flex Mode: Central authentication and local switching.

✎

Note Cenral authentication is supported on Wave 1 and Wave 2 APs, whereas local switching is supported only on Wave 2 APs.

The following features are supported for use with a WGB:

Table 1: WGB Feature Matrix

Feature	Cisco Wave 1 APs	Cisco Wave 2
802.11r	Supported	Supported
QOS	Supported	Supported
UWGB mode	Supported	Supported on Wave 2 APs
IGMP Snooping or Multicast	Supported	Supported
802.11w	Supported	Supported
PI support (without SNMP)	Supported	Not supported
IPv6	Supported	Supported
VLAN	Supported	Supported
802.11i (WPAv2)	Supported	Supported
Broadcast tagging/replicate	Supported	Supported
Unified VLAN client	Implicitly supported (No CLI required)	Supported
WGB client	Supported	Supported
802.1x – PEAP, EAP-FAST, EAP-TLS	Supported	Supported
NTP	Supported	Supported
Wired client support on all LAN ports	Supported in Wired-0 and Wired-1 interfaces	Supported in all Wired-0, 1 and LAN ports 1, 2, and 3

Table 2: Supported Access Points and Requirements

Access Points	Requirements
Cisco Aironet 2700, 3700, and 1572 Series	Requires autonomous image.

Access Points	Requirements
Cisco Aironet 2800, 3800, 4800, 1562, and Cisco Catalyst 9105, 9115, IW6300 and ESW6300 Series	CAPWAP image starting from Cisco AireOS 8.8 release.

- MAC filtering is not supported for wired clients.

- Idle timeout is not supported for both WGB and wired clients.

- Session timeout is not applicable for wired clients.

- Web authentication is not supported.

- WGB supports only up to 20 clients.

- If you want to use a chain of certificates, copy all the CA certificates to a file and install it under a trust point on the WGB, else server certificate validation may fail.

- 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 root AP, create a WLAN and make sure that Aironet IE is enabled under the Advanced settings.

Configuring Workgroup Bridge on a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan wlan-profile`	Enters WLAN configuration submode. The *wlan-profile* is the profile name of the configured WLAN.
Step 3	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Restarts the WLAN.

Verifying the Status of Workgroup Bridges

- To verify the number of WGBs, use the following command:

  show wireless wgb summary

  The following is a sample output:

  ```
  Device#show wireless wgb summary
  Number of WGBs: 1
  MAC Address     AP Name                          WLAN State          Clients
  -------------------------------------------------------------------------------
  7070.8b7a.7030 Ed2-JFW-AP1                       1     Run           1
  ```

- To verify WGB details, use the following command:

  show wireless wgb mac-address *MAC-address* **detail**

  The following is a sample output:

  ```
  Device#show wireless wgb mac-address 7XXX.8XXa.7XXX detail

  Work Group Bridge

  MAC Address        : 7XXX.8XXa.7XXX
  AP Name            : Ed2-JFW-AP1
  WLAN ID            : 1
  State              : Run

  Number of Clients: 1

  MAC Address
  ------------
  d8XX.97XX.bXXX
  ```

- To view the client details on the controller, use the following command:

  show wireless client mac-address *MAC-address* **detail**

  The following is a sample output:

  ```
  Device#show wireless client mac-address 7XXX.8bXX.70XX detail

  Workgroup Bridge
  Wired Client count : 1
  ```

- The following is a sample output:

  ```
  Device#show wireless client mac-address d8XX.97XX.b0XX detail
  Workgroup Bridge Client
  WGB MAC Address : 7XXX.8bXX.70XX
  ```

Information About Simplifying WGB Configuration

From Cisco IOS XE Cupertino 17.8.1, it is possible to configure WGB in multiple Cisco access points (APs) simultaneously. By importing a running configuration, you can deploy multiple WGBs in a network and make them operational quicker. When new Cisco APs are added to the network, you can transfer an existing or

working configuration to the new Cisco APs to make them operational. This enhancement eliminates the need to configure multiple Cisco APs using CLIs, after logging into them.

A network administrator can onboard Cisco APs using either of the following methods:

- Upload the working configuration from an existing Cisco AP to a server and download it to the newly deployed Cisco APs.

- Send a sample configuration to all the Cisco APs in the deployment.

This feature is supported only on the following Cisco APs:

- Cisco Aironet 1562 Access Points

- Cisco Aironet 2800 Access Points

- Cisco Aironet 3800 Access Points

- Cisco Catalyst 9105 Access Points

- Cisco Catalyst 9115 Access Points

- Cisco Catalyst 9120 Access Points

- Cisco Catalyst IW6300 Series Heavy Duty Access Points

For latest support information on various features in Cisco Wave 2 and 802.11ax (Wi-Fi 6) Access Points in Cisco IOS XE releases, see the Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points document.

Configuring Multiple WGBs (CLI)

Perform the following procedure on the APs in WGB mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**copy configuration upload**{**sftp:**| **tftp:**} *ip-address* [*directory*] [*file-name*] **Example:** `Device# copy configuration upload sftp: 10.10.10.1 C:sample.txt`	Creates upload configuration file and uploads to the SFTP or TFTP server using the specified path.
Step 3	**copy configuration download**{**sftp:**| **tftp:**} *ip-address* [*directory*] [*file-name*] **Example:** `Device# copy configuration download sftp: 10.10.10.1 C:sample.txt`	Downloads the configuration file and replaces the old configuration in the AP and reboots the WGB. When the device restarts, new configuration is applied.

	Command or Action	**Purpose**
Step 4	**show wgb dot11 association**	Lists the WGB uplink information.
	Example:	
	`Device# show wgb dot11 association`	
Step 5	**show version**	Displays the AP software information.
	Example:	
	`Device# show version`	

Verifying WGB Configuration

After completing the configuration download and reboot of the AP, the WGB rejoins the network. Use the **show logging** command to list and verify the download events that are captured in the debug logs:

```
Device# show logging

Jan 13 18:19:17 kernel: [*01/13/2022 18:19:17.4880] WGB - Applying download config...
Jan 13 18:19:18 download_config: configure clock timezone UTC
Jan 13 18:19:18 download_config: configure dot1x credential dot1x_profile username wifiuser
 password U2FsdGVkX1+8PWmAOnFO8BXyk5EAphMy2PmhPPhWV0w=
Jan 13 18:19:18 download_config: configure eap-profile eap_profile method PEAP
Jan 13 18:19:18 download_config: configure eap-profile eap_profile dot1x-credential
dot1x_profile
Jan 13 18:19:18 chpasswd: password for user changed
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7260] chpasswd: password for user changed
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]  Management user configuration saved
successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]  Dot1x credential configuration has
been saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]  EAP profile configuration has been
saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]  EAP profile configuration has been
saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7830] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7830]
Jan 13 18:19:18 download_config: configure ssid-profile psk ssid alpha_psk authentication
psk U2FsdGVkX18meBfFFeiC4sgkEmbGPNH/ul1dne6h/m8= key-management wpa2
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]  EAP profile configuration has been
saved successfully
```

```
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]
Jan 13 18:19:18 download_config: configure ssid-profile open ssid alpha_open authentication
 open
Jan 13 18:19:18 download_config: configure ssid-profile openax ssid alpha_open_ax
authentication open
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.8650]  SSID-Profile dot1xpeap has been saved
 successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.8650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.9270]  SSID-Profile psk has been saved
successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.9270]
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]  SSID-Profile open has been saved
successfully
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]  SSID-Profile openax has been saved
successfully
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]
Jan 13 18:19:22 download_config: configure wgb broadcast tagging disable
Jan 13 18:19:22 download_config: configure wgb packet retries 64 drop
Jan 13 18:19:22 kernel: [*01/13/2022 18:19:22.9710] Broadcast tagging 0 successfully
Jan 13 18:19:22 kernel: [*01/13/2022 18:19:22.9710]
Jan 13 18:19:23 download_config: configure dot11Radio 1 mode wgb ssid-profile open
Jan 13 18:19:23 download_config: configure dot11Radio 1 enable
Jan 13 18:19:23 download_config: configure ap address ipv6 disable
```