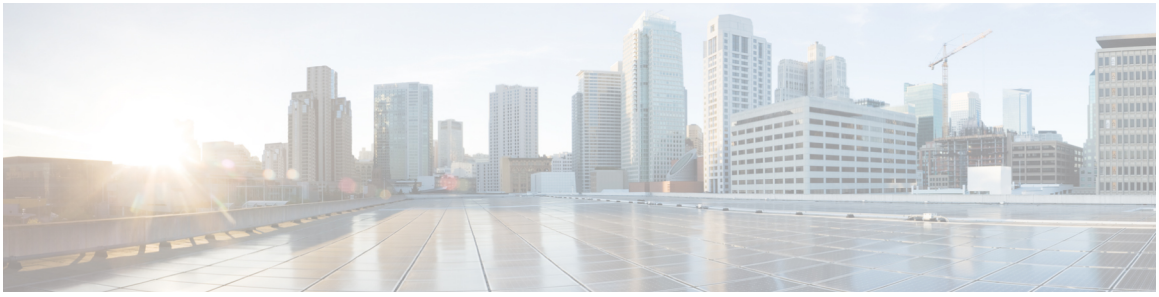
Cisco Catalyst IW9165 Rugged Series Configuration Guide, Release 17.13.x

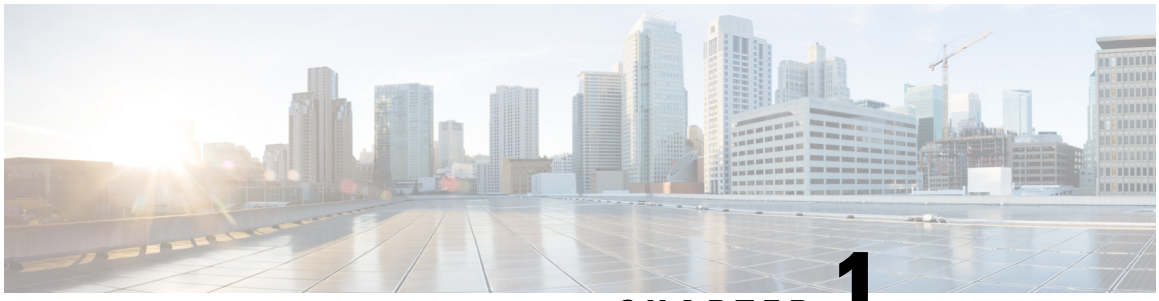
First Published: 2023-12-15

Last Modified: 2024-11-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

Introduction

Overview of the Access Point

The Cisco Catalyst IW9165E Rugged Access Point and Wireless Client (hereafter referred to as *IW9165E*) is designed to add ultrareliable wireless connectivity to moving vehicles and machines. The IW9165E can operate as Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) starting from Cisco Unified Industrial Wireless Software Release 17.12.1, which delivers high availability, low latency, and zero packet loss with seamless handoffs.

Starting from Cisco Unified Industrial Wireless Software Release 17.13.1, the IW9165E can also operate as a Wi-Fi client in Workgroup Bridge (WGB) mode, which allows it to connect to a Cisco access point infrastructure, and Universal WGB (uWGB) mode, which allows it to connect to a third-party access point infrastructure. Both of these modes help bridge the wired clients that are behind the WGB to the access point on the infrastructure side.

This document covers configuration of WGB and uWGB mode specific to the IW9165E access points.

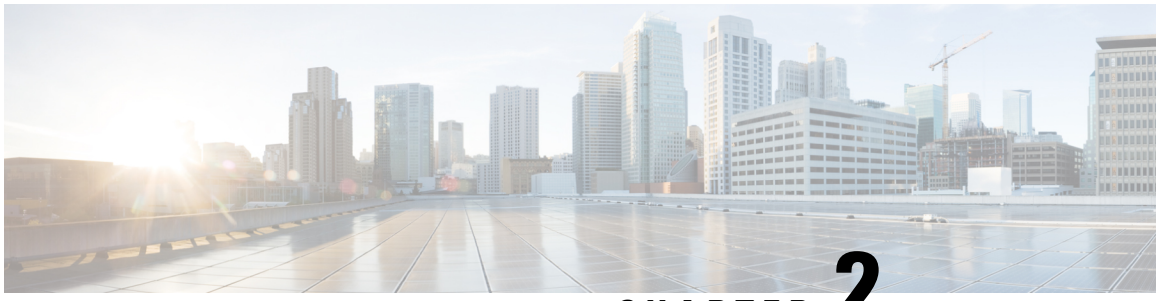
Related Documentation

To view all support information for the Cisco Catalyst IW9165 Rugged Series, see https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html.

In addition to the documentation available on the support page, you will need to refer to the following guides:

- For information about IW9165E hardware, see Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Hardware Installation Guide.
- A full listing of the AP's features and specifications is provided in Cisco Catalyst IW9165 Series Data Sheet.
- For information about Cisco URWB mode configuration, see the relevant documents at:

  https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html.



CHAPTER 2

Workgroup Bridges

Overview

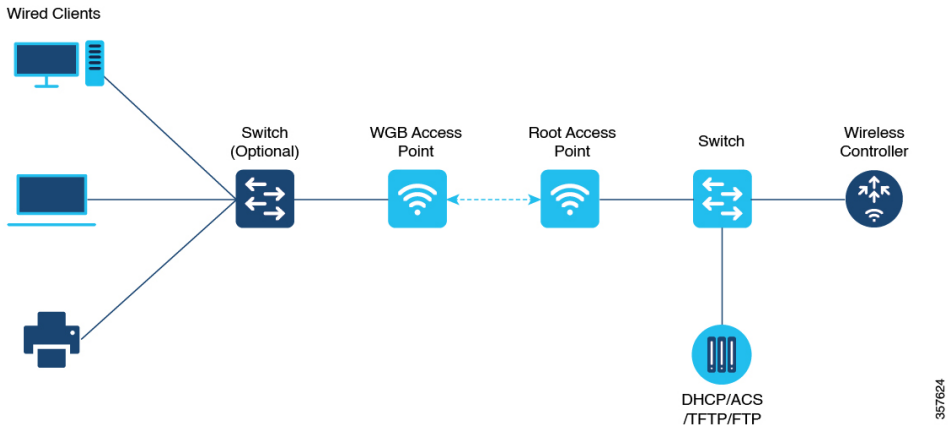
Workgroup bridge mode

Workgroup Bridge Mode (WGB) is a mode of an Access Point (AP) that provides wireless connectivity to the wired clients. These clients are connected to the Ethernet port of the WGB. The WGB bridges the wired network and a wireless segment. It perfoms this by learning the MAC addresses of its Ethernet-wired clients. The WGB then shares these identifiers with the Wireless LAN Controller (WLC) through an infrastructure AP using the Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which treats the WGB as a wireless client.

Universal workgroup bridge mode

Universal Workgroup Bridge (uWGB) is a complementary mode to the WGB. It acts as a wireless bridge between the wired client connected to the uWGB and the wireless infrastructure. This infrastructure includes both Cisco and non-Cisco wireless networks. One of the wireless interfaces is used to connect with the access point. The radio MAC is used to associate with the AP.

Figure 1: WGB Example



Starting from Cisco Unified Industrial Wireless Software Release 17.13.1, WGB is supported on the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client.

Limitations and Restrictions

This section provides the limitations and restrictions of both WGB and uWGB modes.

WGB mode limitations and restrictions

- The WGB can associate only with Cisco lightweight APs.
- In a Meraki wireless infrastructure that uses WPA1 security, uWGB do not associate with any SSIDs.
- Speed and duplex are automatically negotiated based on the capabilities of the locally connected endpoint. They cannot be manually configured on the AP's wired 0 and wired 1 interfaces.
- Spanning Tree Protocol (STP) and Per-VLAN Spanning Tree (PVST) packets are used to detect and prevent loops in the wired and wireless switching networks. WGB transparently bridges STP packets between two wired segments. Incorrect or inconsistent configuration of STP in the wired segments can cause the connected switch(es) to block the WGB wireless link to the connected AP or WGB. This can cause WGB to lose connection with the AP or the AP to lose connection with the controller. This prevents wired clients from getting IP addresses because STP blocks the switch port in the wired network.If you want to stop STP bridging between wired segments by the WGB, you are recommended to disable STP on the switches directly connected in the wireless network.
- These features do not work with a WGB:
  - Idle timeout
  - Web authentication

- In Layer 3 roaming, if you connect a wired client to the WGB network, when the WGB has roamed to a different controller such as a foreign controller, the wired client's IP address displays only on the anchor controller, but not on the foreign controller.
- When you deauthenticate a WGB record from a controller, it clears all entries of the wired clients connected to that WGB.
- Wired clients connected to a WGB do not support these features:
  - MAC filtering
  - Link tests
  - Idle timeout
- You can't associate a WGB to a WLAN that is configured with Adaptive 802.11r.
- Although IPv4 is enabled, the WGB supports only IPv6. This does notaffect any WGB wired clients IPv6 traffic.
- WGB IPv6 management does not work, even upon a successful WGB uplink association. Although the WGB can obtain an IPv6 address, IPv6 pings do not work to or from the WGB. Additionally, SSH to the WGB management IPv6 address using wireless or wired clients does not work. The workaround to resolve this issue is to re-enable IPv6, even though it has already been enabled and the IPv6 address has been assigned.
- Even though the infrastructure AP operates on a non-dynamic frequency selection (non-DFS) channel and changes its channel bandwidth, the WGB remains connected to the infrastructure AP using the original channel bandwidth.

Note Ensure that the WGB should connect to the AP using the correct channel bandwidth. Use the `<wgb-wireless-client-mac-address> deauthenticate` command on the wireless controller to deauthenticate the WGB wireless client.

uWGB mode limitations and restrictions

- The uWGB can associate with both Cisco and third-party APs.
- The uWGB mode does not support TFTP or SFTP. Software upgrade should be done in WGB mode only. For more information, see uWGB Image Upgrade.
- uWGB mode supports wired clients connected to the wired0 interface. It does not support wired clients connected to the wired1 interface.
- In uWGB mode, you should configure an arbitrary non-routable IP address for uWGB. If you configure uWGB with a static or dynamic IP address in the same range as the end device, it may cause unexpected behavior.
- From UIW Release 17.13.1, an AP in uWGB mode is managed using SSH. An image upgrade can be performed when no wired clients are connected to the AP.
  - When a wired client is detected, the AP in uWGB mode remains in the same uWGB mode. You cannot upgrade the image of AP.

- When a wired client is not detected, AP in uWGB mode switches to WGB mode. You can manage as well as upgrade the image of AP.

Guidelines to Reset the Login Credentials in Day0

You should configure new login credentials for WGB or uWGB after the first login. The username and password should follow these rules:

- The username length must be from 1 to 32.
- The password length must be from 8 to 120.
- The password must include:
  - at least one uppercase character,
  - one lowercase character,
  - one digit, and
  - one punctuation mark.
- The password can include:
  - alphanumeric characters
  - special characters (ASCII decimal code from 33 to 126)
- The password must exclude:
  - " (double quote),
  - ' (single quote), and
  - ? (question mark).
- The password cannot contain:
  - Three consecutive characters in sequence (ABC/ CBA).
  - Three consecutive identical characters (AAA).
  - The same as or the reverse of the username.
- Your new password must contain at least four characters that are different from your current password.

Default credentials:

- Username: Cisco
- Password: Cisco
- Enable password: Cisco

Credentials example:

- username: demouser
- password: DemoP@ssw0rd
- enable password: DemoE^aP@ssw0rd

```
User Access Verification
Username: Cisco
Password: Cisco

% First Login: Please Reset Credentials

Current Password:Cisco
Current Enable Password:Cisco
New User Name:demouser
New Password:DemoP@ssw0rd
Confirm New Password:DemoP@ssw0rd
New Enable Password:DemoE^aP@ssw0rd
Confirm New Enable Password:DemoE^aP@ssw0rd

% Credentials changed, please re-login

[*04/18/2023 23:53:44.8926] chpasswd: password for user changed
[*04/18/2023 23:53:44.9074]
[*04/18/2023 23:53:44.9074] Management user configuration saved successfully
[*04/18/2023 23:53:44.9074]


User Access Verification
Username: demouser
Password: DemoP@ssw0rd
APFC58.9A15.C808>enable
Password:DemoE^aP@ssw0rd
APFC58.9A15.C808#
```

Note In the above example, all passwords appear in plain text for clarity. In real scenarios, they are hidden with asterisks (*).

Configure Controller and WLAN Settings for WGB Association

For a WGB to join a wireless network, configure following settings on the WLAN and related policy profile on the controller.

Follow these steps to configure the Cisco Client Extensions option and set the support of Aironet IE in the WLAN:

1. Use the **wlan** *profile-name* command to enter WLAN configuration submode.

```
Device#wlan profile-name
```

Note Here the *profile-name* is the name of the configured WLAN.

2. Use the **ccx aironet-iesupport** command to configure the Cisco Client Extensions option and set the Aironet IE support on the WLAN.

```
Device#ccx aironet-iesupport
```

Note This configuration is mandatory for WGB to associate with the AP.

Configure WLAN policy profile for WGB

1. Use the **wireless profile policy** *profile-policy* command to enter wireless policy configuration mode.

```
Device#wireless profile policy profile-policy
```

2. Use the **vlan** *vlan-id* command to assign the profile policy to the VLAN.

```
Device#vlan vlan-id
```

3. Use the **wgb vlan** command to configure WGB VLAN client support.

```
Device#wgb vlan
```

uWGB Image Upgrade

uWGB mode does not support TFTP or SFTP. Convert uWGB to WGB mode to upgrade the software.

Procedure

Step 1 Connect a TFTP or SFTP server to wired 0 port of uWGB.

Step 2 Use the **configure Dot11Radio** *slot_id* **disable** command to disable the radio interface.

```
Device#configure Dot11Radio slot_id disable
```

Step 3 Convert uWGB to WGB mode.

Use the **configure Dot11Radio** *slot_id* **mode wgb ssid-profile** *ssid_profile_name* command to reboot the device with the downloaded configuration.

```
Device#configure Dot11Radio slot_id mode wgb ssid-profile ssid_profile_name


This command will reboot with downloaded configs.
Are you sure you want continue? <confirm>
```

Note
For *ssid_profile_name*, use any existing configured SSID profile.

Step 4 When device reboots, assign a static IP address to the WGB.

Use the **configure ap address ipv4 static** *IPv4_address netmask Gateway_IPv4_address* command to assign a static IP address to the WGB.

```
Device#configure ap address ipv4 static 192.168.1.101 255.255.255.0 192.168.1.1
```

Step 5 Use the **ping***server_IP* command to view the ICMP ping.

```
Device#ping server_IP
```

Example:

```
Device#ping 192.168.1.20
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds

PING 192.168.1.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.858/0.932/1.001 ms
```

Step 6 Use the **archive download/reload** <**tftp | sftp | http**>://*server_ip*/*file_path* command to upgrade the software.

```
Device#archive download/reload <tftp | sftp | http >://server_ip /file_path
```

Step 7 Use the **configure Dot11Radio** *slot_id* **mode uwgb** *wired_client_mac_addr* **ssid-profile** *ssid_profile_name* command to convert AP's mode from WGB to uWGB mode.

```
Device#configure Dot11Radio slot_id mode uwgb wired_client_mac_addr ssid-profile ssid_profile_name
```

WGB Configuration

Perform these tasks for WGB configuration:

1. Create an SSID profile.
2. Configure radio in WGB mode, and associate the SSID profile to the radio.
3. Turn on the radio.

WGB uplink supports various security methods which includes:

- Open (unsecured)
- PSK
- Dot1x (LEAP, PEAP, FAST-EAP, and TLS.)

Dot1x FAST-EAP configuration example

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 1 mode wgb ssid-profile demo-FAST
configure dot11radio 1 enable
```

These sections provide detailed information on the WGB configuration procedure.

Configure a dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP dot1x profile.

```
Device#show wgb eap dot1x credential profile
```

Deauthenticate WGB wired client

Use the **clear wgb client** {**all** |**single** *mac-addr*} command to deauthenticate WGB wired client.

```
Device#clear wgb client {all |single mac-addr}
```

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

Step 1 Use the **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} command to configure the EAP profile.

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method: fast or leap or peap or tls.

Step 2 Use the **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} command to attach the CA trustpoint for TLS. By default, WGB uses the internal MIC certificate for authentication.

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* command to attach the dot1x-credential profile.

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

Step 4 [Optional] Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** command to create a trustpoint in WGB.

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and certificate signing request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* command to enroll a trustpoint in WGB using the server URL.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to enroll the trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the digitally signed certificate from the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* command to enable auto-enroll.

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

Note
Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll disable** command to disable the auto-enroll.

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

```
Device#show crypto pki timers
```

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and Certificate Signing Request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

This generates certificate request and sends the request to the TFTP server. The filename to be written is appended with the **.req** extension.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

The console terminal uses TFTP to import a certificate and the WGB tries to get the approved certificate from the TFTP. The filename to be written is appended with the **.crt** extension.

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 8 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

SSID configuration

Perform these tasks to configure SSID.

Create an SSID profile

Choose one of the following authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK dot11r authentication
   - PSK dot11w authentication
3. Dot1x authentication

Configure an SSID profile using open authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** *open* command to configure an SSID profile using open authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of the following authentication protocols to configure an SSID profile using PSK authentication:

- Configure an SSID profile using PSK WPA2 authentication
- Configure an SSID profile using PSK Dot11r authentication
- Configure an SSID profile using PSK Dot11w authentication

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}} command to configure an SSID profile using dot1x authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using dot1x EAP-PEAP authentication

The following example shows the configuration of an SSID profile using dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configure radio interface for WGB

IW9165E does not have 2.4 GHz radio. Only dot11radio 1 can be configured as uplink and operate in WGB mode.

Use the **configure dot11radio** *slot_id* **mode wgb ssid-profile** *ssid-profile-name* command to configure a radio interface to a WGB SSID profile.

```
Device#configure dot11radio 1 mode wgb ssid-profile ssid-profile-name
```

Enable radio interface for WGB

Use the **configure dot11radio** *slot_id* **enable** command to enable a radio interface.

```
Device#configure dot11radio 1 enable
```

Note Use the **configure dot11radio** *slot_id* **disable** command to disable a radio interface.

Configure WGB or uWGB timer

The timer configuration CLIs are common for both WGB and uWGB. Use these commands to configure timer:

- Use the **configure wgb association response timeout** *response-millisecs* command to configure the WGB association response timeout.

  ```
  Device#configure wgb association response timeout response-millisecs
  ```

  The default value is 100 milliseconds, and the valid range is between 100 and 5000 milliseconds.

- Use the **configure wgb authentication response timeout** *response-millisecs* command to configure the WGB authentication response timeout.

  ```
  Device#configure wgb authentication response timeout response-millisecs
  ```

  The default value is 100 milliseconds, and the valid range is between 100 and 5000 milliseconds.

- Use the **configure wgb eap timeout** *timeout-secs* command to configure the WGB EAP timeout.

  ```
  Device#configure wgb eap timeout timeout-secs
  ```

  The default value is 3 seconds, and the valid range is between 2 and 60 seconds.

- Use the **configure wgb bridge client timeout** *timeout-secs* command to configure the WGB bridge client response timeout.

  ```
  Device#configure wgb bridge client timeout timeout-secs
  ```

  The default timeout value is 300 seconds, and the valid range is between 10 and 1000000 seconds.

uWGB Configuration

The universal WGB is able to interoperate with non-Cisco access points using uplink radio MAC address, thus the universal workgroup bridge role supports only one wired client.

Most WGB configurations apply to uWGB. The only difference is that you configure wired client's MAC address with the following command:

configure dot11 <*slot_id*> **mode uwgb** <*uwgb_wired_client_mac_address*> **ssid-profile** <*ssid-profile*>

The following is an example of Dot1x FAST-EAP configuration:

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 1 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 1 enable
```

The following sections provide detailed information about uWGB configuration:

Configure a dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP dot1x profile.

```
Device#show wgb eap dot1x credential profile
```

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

Step 1 Use the **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} command to configure the EAP profile.

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method: fast or leap or peap or tls.

Step 2 Use the **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} command to attach the CA trustpoint for TLS. By default, WGB uses the internal MIC certificate for authentication.

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* command to attach the dot1x-credential profile.

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

Step 4 [Optional] Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** command to create a trustpoint in WGB.

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and certificate signing request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* command to enroll a trustpoint in WGB using the server URL.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to enroll the trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the digitally signed certificate from the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* command to enable auto-enroll.

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

Note
Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll disable** command to disable the auto-enroll.

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

```
Device#show crypto pki timers
```

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and Certificate Signing Request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

This generates certificate request and sends the request to the TFTP server. The filename to be written is appended with the **.req** extension.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

The console terminal uses TFTP to import a certificate and the WGB tries to get the approved certificate from the TFTP. The filename to be written is appended with the **.crt** extension.

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 8 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 14
2. Configuring Radio Interface for uWGB, on page 22

Create an SSID profile

Choose one of the following authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK dot11r authentication
   - PSK dot11w authentication
3. Dot1x authentication

Configure an SSID profile using open authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** *open* command to configure an SSID profile using open authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of the following authentication protocols to configure an SSID profile using PSK authentication:

- Configure an SSID profile using PSK WPA2 authentication
- Configure an SSID profile using PSK Dot11r authentication
- Configure an SSID profile using PSK Dot11w authentication

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**} } command to configure an SSID profile using dot1x authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using dot1x EAP-PEAP authentication

The following example shows the configuration of an SSID profile using dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configuring Radio Interface for uWGB

IW9165E does not have 2.4 GHz radio. Only slot 1 (dot11radio 1) can be configured as uplink.

- Map a radio interface to a WGB SSID profile by entering this command:

  # **configure dot11radio 1 mode uwgb** *client-mac-address* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  # **configure dot11radio 1** { **enable** | **disable** }

  Example

  ```
  # configure dot11radio 1 disable
  ```

Configure IP Address

Configure IPv4 address

- Use the **configure ap address** *ipv4 dhcp* command to configure IPv4 address using DHCP.

  ```
  Device#configure ap address ipv4 dhcp
  ```

- Use the **configure ap address** *ipv4 static ipv4_addr netmask gateway* command to configure the static IPv4 address. By doing so, you can manage the device using a wired interface without an uplink connection.

  ```
  Device#configure ap address ipv4 static ipv4_addr netmask gateway
  ```

Verify current IP configuration

Use **show ip interface brief** command to view the current IP address configuration.

```
Device#show ip interface brief
```

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. By doing so, you can manage the AP through a wired interface without uplink connection.

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

Enable IPv6 auto configuration

Use the **configure ap address ipv6 auto-config enable** command to enable the IPv6 auto configuration on the AP.

```
Device#configure ap address ipv6 auto-config enable
```

Note

- Use the **configure ap address ipv6 auto-config disable** command to disable the IPv6 auto configuration on the AP.
- Use the **configure ap address ipv6 auto-config enable** command to enable IPv6 SLAAC. Note that SLAAC does not apply to CoS of WGB. This command configures IPv6 address with DHCPv6 instead of SLAAC.

Configure IPv6 address using DHCP

Use the **configure ap address** *ipv6 dhcp* command to configure IPv6 address using DHCP.

```
Device#configure ap address ipv6 dhcp
```

Verify current IP configuration

Use the **show ipv6 interface brief** command to verify current IP address configuration.

```
Device#show ipv6 interface brief
```

Syslog

Overview of syslog

yslog is a common protocol, used to send event data logs to a central location for storing. Currently, only UDP mode is supported. If you enable the debug command in WGB, it collects debug logs. All logs collected will be sent to the syslog server are in the kernel facility and at the warning level.

Enable or disable WGB syslog

Use the **logging host enable** <*server_ip*> **UDP** command to enable WGB syslog.

```
Device#logging host enable <server_ip> UDP
```

Note Use the **logging host disable** <*server_ip*> **UDP** command to disable default WGB syslog.

Verify WGB syslog

Use the **show running-config** command to view current syslog configuration.

```
show running-config
```

Conversion between WGB and uWGB modes

- Use the **configure dot11radio** <*radio_slot_id*> **mode uwgb** <*WIRED_CLIENT_MAC*> **ssid-profile** <*SSID_PROFILE_NAME*> command to convert from WGB to uWGB mode.

```
Device#configure dot11radio <radio_slot_id> mode uwgb <WIRED_CLIENT_MAC> ssid-profile
<SSID_PROFILE_NAME>
```

- Use the **configure dot11radio** <*radio_slot_id*> **mode wgb ssid-profile** <*SSID_PROFILE_NAME*> command to convert from uWGB to WGB mode. This conversion involves rebooting of the AP.

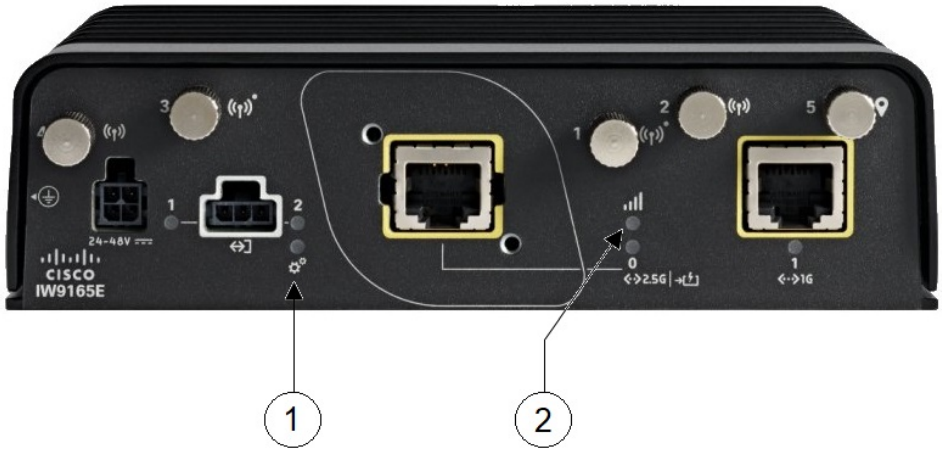
```
Device#configure dot11radio 1 mode wgb ssid-profile <SSID_PROFILE_NAME>

 This command will reboot with downloaded configs.
 Are you sure you want continue? [confirm]
```

LED Pattern

There are two LEDs located at the front of AP panel:

- System status LED
- RSSI status LED

Figure 2: IW9165E LEDs



1	System status LED • Blinking Red: When WGB is disassociated. • Solid green: When WGB is associated with the parent AP.	2	RSSI status LED • Solid green: When RSSI value is >= -71dBm. • Blinking green: When RSSI value is between -81 dBm and -70 dBm. • Solid yellow: When RSSI value is between -95 dBm and -81 dBm. • Off: For all other RSSI values.

Configure Transmission Rate with High Throughput for WGB

During the configuration of WGB mode, in case of moving deployment, you can manually configure transmission rate limit. You can do this using a method called high throughput (HT) modulation and coding scheme (MCS).

Example of WGB configuration with transmission rate of 802.11n HT m4. m5. rate:

Config dot11radio [**1**|**2**] **802.11ax disable**

Config dot11radio [**1**|**2**] **802.11ac disable**

Config dot11radio [**1**|**2**] **speed ht-mcs m4. m5.**

Note WGB supports to configure legacy rate:

Config dot11radio [**1**|**2**] **speed legacy-rate basic-6.0 9.0 12.0 18.0 24.0**

802.11 management and control frames use legacy rates. WGB legacy rates should match with AP's legacy rates, or at least, it should overlap between these legacy rates. Otherwise, WGB association fails.

Use the **debug wgb dot11 rate** command to check WGB Tx MCS rate. The following example shows the output of this command.

```
JWGB1#debug wgb dot11 rate
[*10/14/2023 03:16:08.6175]
[*10/14/2023 03:16:08.6175]                MAC    Tx-Pkts    Rx-Pkts                Tx-Rate(Mbps)                Rx-Rate(Mbps)  RSSI Tx-Retries
[*10/14/2023 03:16:08.6175] 24:16:1B:F8:02:6E          0          0          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70          0
JWGB1#[*10/14/2023 03:16:09.6179] 24:16:1B:F8:02:6E        330          3          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         15
[*10/14/2023 03:16:10.6183] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         25
[*10/14/2023 03:16:11.6187] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:12.6190] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         13
[*10/14/2023 03:16:13.6194] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         21
[*10/14/2023 03:16:14.6198] 24:16:1B:F8:02:6E        331          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         16
[*10/14/2023 03:16:15.6202] 24:16:1B:F8:02:6E        328          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         24
[*10/14/2023 03:16:16.6206] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         21
[*10/14/2023 03:16:17.6210] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         22
[*10/14/2023 03:16:18.6214] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         22
[*10/14/2023 03:16:19.6218] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:20.6221] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         17
[*10/14/2023 03:16:21.6258] 24:16:1B:F8:02:6E        328          3          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         16
```

Radio Statistics Commands

To help troubleshooting radio connection issues, use the following commands:

- #**debug wgb dot11 rate**

```
#debug wgb dot11 rate
[*03/13/2023 18:00:08.7814]                MAC    Tx-Pkts    Rx-Pkts
  Tx-Rate(Mbps)                    Rx-Rate(Mbps)  RSSI   SNR Tx-Retries
[*03/13/2023 18:00:08.7814] FC:58:9A:17:C2:51          0          0
HE-20,2SS,MCS6,GI0.8 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
[*03/13/2023 18:00:09.7818] FC:58:9A:17:C2:51          0          0
HE-20,2SS,MCS6,GI0.8 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
```

In this example, FC:58:9A:17:C2:51 is the parent AP radio MAC.

- #**show interfaces dot11Radio** <*slot-id*> **statistics**

```
#show interfaces dot11Radio 1 statistics
Dot11Radio Statistics:
        DOT11 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx K Bytes:        965570/0        Host Tx K Bytes:       1611903/0
Unicasts Rx:            379274/0        Unicasts Tx:           2688665/0
Broadcasts Rx:         3166311/0        Broadcasts Tx:               0/0
Beacons Rx:          722130099/1631     Beacons Tx:          367240960/784
Probes Rx:           588627347/2224     Probes Tx:            78934926/80
Multicasts Rx:         3231513/0        Multicasts Tx:           53355/0
Mgmt Packets Rx:     764747086/1769     Mgmt Packets Tx:     446292853/864
Ctrl Frames Rx:        7316214/5        Ctrl Frames Tx:              0/0
RTS received:                0/0        RTS transmitted:             0/0
Duplicate frames:            0/0        CTS not received:            0/0
MIC errors:                  0/0        WEP errors:            2279546/0
FCS errors:                  0/0        Retries:                896973/0
Key Index errors:            0/0        Tx Failures:              8871/0
                                        Tx Drops:                    0/0

Rate Statistics for Radio::
[Legacy]:
6 Mbps:
 Rx Packets:     159053/0            Tx Packets:      88650/0
                                     Tx Retries:       2382/0
9 Mbps:
 Rx Packets:         43/0            Tx Packets:         23/0
                                     Tx Retries:         71/0
12 Mbps:
 Rx Packets:          1/0            Tx Packets:        119/0
                                     Tx Retries:        185/0
18 Mbps:
 Rx Packets:          0/0            Tx Packets:          5/0
                                     Tx Retries:        134/0
24 Mbps:
 Rx Packets:        235/0            Tx Packets:      20993/0
                                     Tx Retries:       5048/0
36 Mbps:
 Rx Packets:          0/0            Tx Packets:        781/0
                                     Tx Retries:        227/0
54 Mbps:
 Rx Packets:        133/0            Tx Packets:       9347/0
                                     Tx Retries:       1792/0

[SU]:
M0:
 Rx Packets:          7/0            Tx Packets:          0/0
                                     Tx Retries:          6/0
M1:
 Rx Packets:       1615/0            Tx Packets:      35035/0
                                     Tx Retries:       3751/0
M2:
```

```
 Rx Packets:      15277/0            Tx Packets:     133738/0
                                     Tx Retries:      22654/0
M3:
 Rx Packets:      10232/0            Tx Packets:       1580/0
                                     Tx Retries:      21271/0
M4:
 Rx Packets:     218143/0            Tx Packets:     190408/0
                                     Tx Retries:      36444/0
M5:
 Rx Packets:     399283/0            Tx Packets:     542491/0
                                     Tx Retries:     164048/0
M6:
 Rx Packets:    3136519/0            Tx Packets:     821537/0
                                     Tx Retries:     329003/0
M7:
 Rx Packets:    1171128/0            Tx Packets:     303414/0
                                     Tx Retries:     154014/0



Beacons missed: 0-30s 31-60s 61-90s 90s+
                     2      0      0    0
```

- **#show wgb dot11 uplink latency**

```
AP4C42.1E51.A050#show wgb dot11 uplink latency
Latency Group Total Packets Total Latency Excellent(0-8) Very Good(8-16) Good (16-32
ms) Medium (32-64ms) Poor (64-256 ms) Very Poor (256+ ms)
        AC_BK             0             0              0               0
 0                0               0                0
        AC_BE          1840       4243793           1809              10
14                7               0                0
        AC_VI             0             0              0               0
 0                0               0                0
        AC_VO            24         54134             24               0
 0                0               0                0
```

- **#show wgb dot11 uplink**

```
AP4C42.1E51.A050#show wgb dot11 uplink

HE Rates: 1SS:M0-11 2SS:M0-11
Additional info for client 8C:84:42:92:FF:CF
RSSI: -24
PS  : Legacy (Awake)
Tx Rate: 278730 Kbps
Rx Rate: 410220 Kbps
VHT_TXMAP: 65530
CCX Ver: 5
Rx Key-Index Errs: 0
              mac     intf TxData TxUC TxBytes TxFail TxDcrd TxCumRetries MultiRetries
 MaxRetriesFail RxData RxBytes RxErr               TxRt(Mbps)               RxRt(Mbps)
   LER PER stats_ago
8C:84:42:92:FF:CF wbridge1   1341 1341  184032      0      0          543           96
              0    317   33523     0 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8
(458) 27272   0  1.370000
Per TID packet statistics for client 8C:84:42:92:FF:CF
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s)
       0      35    1314            0             8
       1       0       0            0             0
       2       0       0            0             0
       3       0       0            0             0
       4       0       0            0             0
       5       0       0            0             0
       6     182      24            1             0
```

```
       7       3       3            0            0
Rate Statistics:
Rate-Index    Rx-Pkts    Tx-Pkts Tx-Retries
         0         99          3          0
         4          1          1          9
         5         21         39         35
         6         31        185         64
         7         26        124         68
         8         28        293         82
         9         77        401        151
        10         32        140         97
        11          2        156         37
```

Event Logging

For WGB field deployment, event logging will collect useful information (such as WGB state change and packets rx/tx) to analyze and provide log history to present context of problem, especially in roaming cases.

You can configure WGB trace filter for all management packet types, including probe, auth, assoc, eap, dhcp, icmp, and arp. To enable or disable WGB trace, use the following command:

#**config wgb event trace** {**enable**|**disable**}

Four kinds of event types are supported:

- **Basic event**: covers most WGB basic level info message
- **Detail event**: covers basic event and additional debug level message
- **Trace event**: recording wgb trace event if enabled
- **All event**: bundle trace event and detail event

The log format is [*timestamp*] *module*:*level* <*event log string*>.

When abnormal situations happen, the eventlog messages can be dumped manually to memory by using the following show command which also displays WGB logging:

#**show wgb event** [**basic**|**detail**|**trace**|**all**]

The following example shows the output of **show wgb event all**:

```
APC0F8.7FE5.F3C0#show wgb event all
[*08/16/2023 08:18:25.167578] UP_EVT:4 R1 IFC:58:9A:17:B3:E7] parent_rssi: -42 threshold:
-70
[*08/16/2023 08:18:25.329223] UP_EVT:4 R1 State CONNECTED to SCAN_START
[*08/16/2023 08:18:25.329539] UP_EVT:4 R1 State SCAN_START to STOPPED
[*08/16/2023 08:18:25.330002] UP_DRV:1 R1 WGB UPLINK mode stopped
[*08/16/2023 08:18:25.629405] UP_DRV:1 R1 Delete client FC:58:9A:17:B3:E7
[*08/16/2023 08:18:25.736718] UP_CFG:8 R1 configured for standard: 7
[*08/16/2023 08:18:25.989936] UP_CFG:4 R1 band 1 current power level: 1
[*08/16/2023 08:18:25.996692] UP_CFG:4 R1 band 1 set tx power level: 1
[*08/16/2023 08:18:26.003904] UP_DRV:1 R1 WGB uplink mode started
[*08/16/2023 08:18:26.872086] UP_EVT:4 Reset aux scan
[*08/16/2023 08:18:26.872096] UP_EVT:4 Pause aux scan on slot 2
[*08/16/2023 08:18:26.872100] SC_MST:4 R2 reset uplink scan state to idle
[*08/16/2023 08:18:26.872104] UP_EVT:4 Aux bring down vap - scan
[*08/16/2023 08:18:26.872123] UP_EVT:4 Aux bring up vap - serv
[*08/16/2023 08:18:26.872514] UP_EVT:4 R1 State STOPPED to SCAN_START
[*08/16/2023 08:18:26.8727091 SC_MST:4 R1 Uplink Scan Started.
[*08/16/2023 08:18:26.884054] UP_EVT:8 R1 CH event 149
```

Note It might take a long time to display the **show wgb event** command output in console. Using *ctrl+c* to interrupt the printing will not affect log dump to memory.

The following clear command erases WGB events in memory:

#**clear wgb event** [**basic**|**detail**|**trace**|**all**]

To save all event logs to WGB flash, use the following command:

#**copy event-logging flash**

The package file consists of four separate log files for different log levels.

You can also save event log to a remote server by using the following command:

#**copy event-logging upload** <**tftp**|**sftp**|**scp**>://A.B.C.D[/*dir*][/*filename.tar.gz*]

The following example saves event log to a TFTP server:

```
APC0F8.7FE5.F3C0#copy event-logging upload
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz
Starting upload of WGB config
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz ...
It may take a few seconds. If longer, please cancel command, check network and try again.
########################################################################## 100.0%
Config upload completed.
```

802.11v Support

802.11v is the Wireless Network Management standard for the IEEE 802.11 family of standards. One enhancement of 802.11v is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

By adding 802.11v support to WGB, WGB can be aware of imminent disconnection before disassociation happens, and then actively starts a roam and picks up an appropriate AP from a list of neighbor APs. WGB periodically queries for latest neighbor APs and associates to the optimal AP on next roam.

Since channel information of neighbor APs is included in Basic Service Set (BSS) Transition Request frame, roaming latency can be reduced for multiple channels deployment by scanning only the channels of neighboring APs.

The wireless controller can disassociate a client based on load balance, RSSI, and data rate on AP side. This disassociation can be notified to 802.11v client before it happens. Wireless controller can disassociate the client after a period of time, if the client does not re-associate to another AP within configurable period. To enable disassociating a client by network assisted roaming, the disassociation-imminent configuration can be turned on from wireless controller, which corresponds to the optional field (disassociation imminent) within BSS Transition Management Request frame.

For detailed information of 802.11v configuration on wireless controller, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-13/config-guide/b_wl_17_13_cg/m_802_11v_ewlc.html.

To configure 802.11v support on WGB, use the following command:

- To enable or disable 802.11v support on WGB, use the following command. By enabling 802.11v support, WGB scans only the channels learned from neighbor list.

configure wgb mobile station interface dot11Radio <*radio_slot_id*> **dot11v-bss-transition** [**enable**|**disable**]

- To configure the time interval that WGB sends BSS transition Query message to the parent AP, use the following command. Default value is 10 sec if not explicit configured. The timer is configured in seconds.

  # **configure wgb neighborlist-update-interval** <*1-900*>

- To check neighbor list received from associated AP, use the following command:

  # **show wgb dot11v bss-transition neighbour**

- To check channel list from dot11v neighbor, aux radio scanned, and residual channel scanned, use the following command:

  # **show wgb dot11v bss-transition channel**

- To clear neighbor list to provide error condition recover, use the following command:

  # **clear wgb dot11v bss-transition neighbor**

Configure Aux Scanning

The aux-scan mode can be configured as either scanning only or handoff mode on WGB radio 2 (5 GHz) to improve roaming performance.

Configuring Scanning-Only Mode

When slot 2 radio is configured as scanning only mode, slot 1 (5G) radio will always be picked as uplink. Slot 2 (5G) radio will keep scanning configured SSID based on the channel list. By defualt, the channel list contains all supported 5G channels (based on reg domain). The scanning list can be configured manually or learned by 802.11v.

When a roaming is triggered, the algorithm looks for candidates from scanning table and skips scanning phase if the table is not empty. WGB then makes assocaition to that candidate AP.

To configure scanning only mode, use the following command:

configure dot11Radio 2 mode scan only

To manually configure the channel list, using the following command:

configure wgb mobile station interface dot11Radio 1 scan <*channel*> [**add**|**delete**]

By default, candidate AP entries in scanning table ages out in 1200 ms. You can adjust the timer by the following command:

#**configure wgb scan radio 2 timeout**

<1-5000> Scanning ap expire time

Note AP selection algorithm picks candidate with best RSSI from the scanning table. In some cases, the RSSI values are out-of-date. This can lead to a failed roaming.

Check the scanning table by using the **show wgb scan** command:

```
#show wgb scan
Best AP expire time: 5000 ms

************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:E2:4F     84     136       1531
FC:58:9A:15:DE:4F     37     136       41

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4F    37     136       41
```

Configuring Aux-Scan Handoff Mode

When slot 2 radio is configured as handoff mode, both radio 1 and radio 2 are the uplink candidate. While one radio maintains wireless uplink, the other radio keeps scanning the channels. The scanning list can be configured manually or learned by 802.11v.

Radio 2 shares the same MAC address with radio 1, and supports the scanning function, association, and data serving. Both radios can work as **serving** or **scanning** role. When a roaming is triggered, the algorithm looks for the scanning database (internal tables), selects the best candidate AP and makes connection. The radio roles and traffic will dynamically switch between slot 1 and slot 2 after each roaming. WGB always uses the radio with operating role of **scanning** to complete the roaming association to a new AP. With this configuration, the roaming interruption time can be improved to 20-50 ms.

The following table is an example of aux-scan handoff radio mode configuration on IW9165E:

Slot 0 (2.4 G)	Slot 1 (5G)	Slot 2 (5G Only)	Slot 3 (Scanning radio)
N/A	WGB	Scan handoff	N/A

The following table compares roaming interruption time (3 channel case) in various mechanisms:

Roaming Interruption Time	Normal Channel Setting	Aux-scan Only	Aux-scan Handoff
Scanning	(40+20)*3=180 ms	0+40 ms	0 ms
Association	30-80 ms	30-80 ms	20-50 ms
Total	~210 ms	70-120 ms	20-50 ms

Use the following command to configure the WGB slot2 radio to aux-scan mode:

configure dot11Radio 2 mode scan handoff

Use the **show run** command to check your configuration:

```
#show run
...
Radio Id                    : 1
   Admin state              : ENABLED
   Mode                     : WGB
   Spatial Stream           : 1
   Guard Interval           : 800 ns
   Dot11 type               : 11n
   11v BSS-Neighbor         : Disabled
```

```
   A-MPDU priority         : 0x3f
   A-MPDU subframe number  : 12
   RTS Protection          : 2347(default)
   Rx-SOP Threshold        : AUTO
   Radio profile           : Default
   Encryption mode         : AES128
Radio Id                   : 2
   Admin state             : ENABLED
   Mode                    : SCAN - Handoff
   Spatial Stream          : 1
   Guard Interval          : 800 ns
   Dot11 type              : 11n
   11v BSS-Neighbor        : Disabled
   A-MPDU priority         : 0x3f
   A-MPDU subframe number  : 12
   RTS Protection          : 2347(default)
   Rx-SOP Threshold        : AUTO
   Radio profile           : Default
```

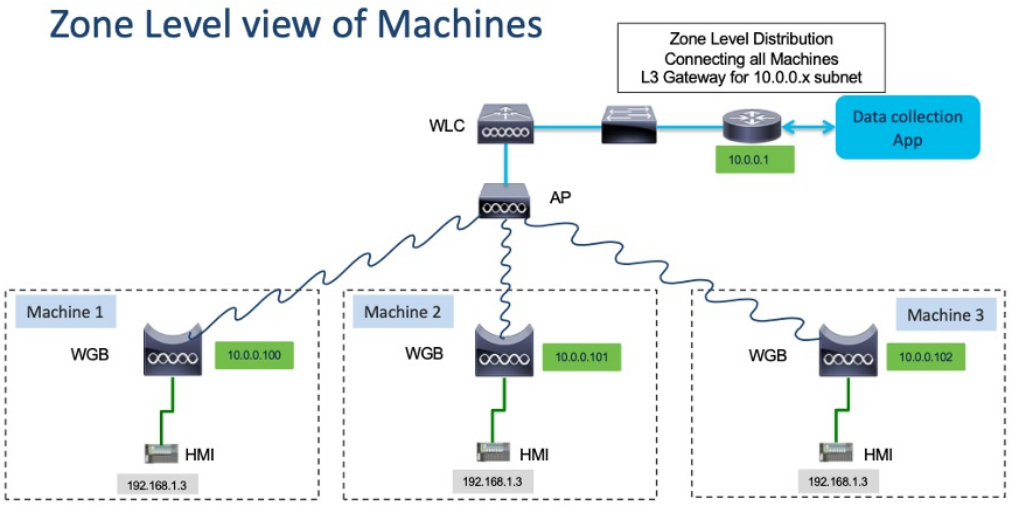
Use the **show wgb scan** command to display the current role of each radio and the aux scanning results:

```
APFC58.9A15.C808#show wgb scan
Best AP expire time: 2500 ms

Aux Scanning Radio Results (slot 2)
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     54     153       57
FC:58:9A:15:E2:4E     71     153       64

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    54     153       57

Aux Serving Radio Results
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     58     153       57
FC:58:9A:15:E2:4E     75     153       133

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    58     153       57
```

Configuring Layer 2 NAT

One-to-one (1:1) Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate with public network. Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined.

In the industrial scenario where the same firmware is programmed to every HMI (customer machine, such as a Robot), firmware duplication across machines means IP address is reused across HMIs. This feature solves the problem of multiple end devices with the same duplicated IP addresses in the industrial network communicating with the public network.



The following table provides the commands to configure Layer 2 NAT:

Table 1: Layer 2 NAT Configuration Commands

Command	Description
#**configure l2nat** {**enable**|**disable**}	Enables or disables L2 NAT.
#**configure l2nat default-vlan** <*vlan_id*>	Specifies the default vlan where all NAT rules will be applied. If *vlan_id* is not specified, all NAT rules will be applied to vlan 0.
#**configure l2nat** {**add**|**delete**} **inside from host** <*original_ip_addr*> **to** <*translated_ip_addr*>	Adds or deletes a NAT rule which translates a private IP address to a public IP address. • *original_ip_addr*—Private IP address of the wired client connected to WGB Ethernet port. • *translated_ip_addr*—Public IP address that represents the wired client at public network.
#**configure l2nat** {**add**|**delete**} **outside from host** <*original_ip_addr*> **to** <*translated_ip_addr*>	Adds or deletes a NAT rule which translates a public IP address to a private IP address. • *original_ip_addr*—Public IP address of an outside network host. • *translated_ip_addr*—Private IP address which represents the outside network host at private network.

Command	Description
#**configure l2nat** {**add**|**delete**} **inside from network** <*original_nw_prefix*> **to** <*translated_nw_prefix*> <*subnet_mask*>	Adds or deletes a NAT rule which translates a private IP address subnet to a public IP address subnet. • *original_nw_prefix*—Private IP network prefix. • *translated_nw_prefix*—Public IP network prefix.
#**configure l2nat** {**add**|**delete**} **outside from network** <*original_nw_prefix*> **to** <*translated_nw_prefix*> <*subnet_mask*>	Adds or deletes a NAT rule which translates a public IP address subnet to a private IP address subnet. • *original_nw_prefix*—Public IP network prefix. • *translated_nw_prefix*—Private IP network prefix.

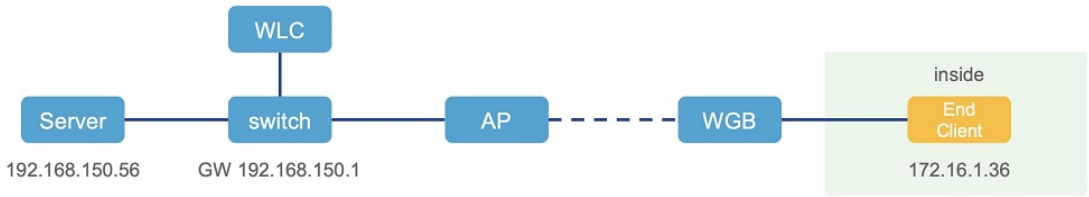
The following table provides the show and debug commands to verify and troubleshoot your Layer 2 NAT configuration:

Table 2: Layer 2 NAT Show and Debug Commands

Command	Description
#**show l2nat entry**	Displays the Layer 2 NAT running entries.
#**show l2nat config**	Displays the Layer 2 NAT configuration details.
#**show l2nat stats**	Displays the Layer 2 NAT packet translation statistics.
#**show l2nat rules**	Displays the Layer 2 NAT rules from the configuration.
#**clear l2nat statistics**	Clears packet translation statistics.
#**clear l2nat rule**	Clears Layer 2 NAT rules.
#**clear l2nat config**	Clears Layer 2 NAT configuration.
#**debug l2nat**	Enables debugging of packet translation process.
#**debug l2nat all**	Prints out the NAT entry match result when a packet arrives. **Caution** This debug command may create overwhelming log print in console. Console may lose response because of this command, especially when Syslog service is enabled with a broadcast address.
#**undebug l2nat**	Disables debugging of packet translation process.

Configuration Example of Host IP Address Translation

In this scenario, the end client (172.16.1.36) connected to WGB needs to communicate with the server (192.168.150.56) connected to the gateway. Layer 2 NAT is configured to provide an address for the end client on the outside network (192.168.150.36) and an address for the server on the inside network (172.16.1.56).



The following table shows the configuration tasks for this scenario.

Command	Purpose
#configure l2nat add inside from host 172.16.1.36 to 192.168.150.36 **#configure l2nat add outside from host 192.168.150.56 to 172.16.1.56**	Adds NAT rules to make inside client and outside server communicate with each other.
#configure l2nat add inside from host 172.16.1.1 to 192.168.150.1 **#configure l2nat add inside from host 172.16.1.255 to 192.168.150.255**	Adds NAT for gateway and broadcast address.

The following show commands display your configuration.

- The following command displays the Layer 2 NAT configuration details. In the output, I2O means "inside to outside", and O2I means "outside to inside".

```
#show l2nat config
L2NAT Configuration are:
================================
Status: enabled
Default Vlan: 0
The Number of L2nat Rules: 4
Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

- The following command displays the Layer 2 NAT rules.

```
#show l2nat rule
Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

- The following command displays Layer 2 NAT running entries.

```
#show l2nat entry
Direction           Original            Substitute            Age    Reversed
inside-to-outside   172.16.1.36@0       192.168.150. 36@0     -1     false
inside-to-outside   172.16.1.56@0       192.168.150. 56@0     -1     true
inside-to-outside   172.16.1.1@0        192.168.150. 1@0      -1     false
```

```
inside-to-outside    172.16.1.255@0       192.168.150. 255@0     -1     false
outside-to-inside    192.168.150.36@0     172.16.1.36@0          -1     true
outside-to-inside    192.168.150.56@0     172.16.1.56@0          -1     false
outside-to-inside    192.168.150.1@0      172.16.1.1@0           -1     true
outside-to-inside    192.168.150.255@0    172.16.1.255@0         -1     true
```

- The following command displays the WGB wired clients over the bridge.
  - Before Layer 2 NAT is enbled:

```
#show wgb bridge
    ***Client ip table entries***
                mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0      172.16.1.36     0.360000       true
24:16:1B:F8:05:0F   0 wbridge1       0           0.0.0.0  3420.560000       true
```

  - After Layer 2 NAT is enbled:

```
#show wgb bridge
    ***Client ip table entries***
                mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0   192.168.150.36     0.440000       true
24:16:1B:F8:05:0F   0 wbridge1       0           0.0.0.0  3502.220000       true
```

  If there are E2E traffic issues for wired client in NAT, restart the client register process by using the following command:

```
#clear wgb client single B8:AE:ED:7E:46:EB
```

- The following command displays the Layer 2 NAT packet translation statistics.

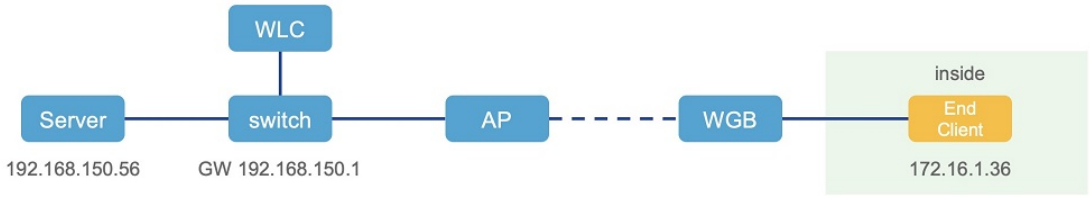
```
#show l2nat stats
Direction          Original              Substitute            ARP  IP   ICMP UDP  TCP
inside-to-outside  172.16.1.1@2660       192.168.150.1@2660    1    4    4    0    0
inside-to-outside  172.16.1.36@2660      192.168.150.36@2660   3    129  32   90   1
inside-to-outside  172.16.1.56@2660      192.168.150.56@2660   2    114  28   85   1
inside-to-outside  172.16.1.255@2660     192.168.150.255@2660  0    0    0    0    0
outside-to-inside  192.168.150.1@2660    172.16.1.1@2660       1    4    4    0    0
outside-to-inside  192.168.150.36@2660   172.16.1.36@2660      3    39   38   0    1
outside-to-inside  192.168.150.56@2660   172.16.1.56@2660      2    35   34   0    1
outside-to-inside  192.168.150.255@2660  172.16.1.255@2660     0    0    0    0    0
```

  To reset statistics number, use the following command:

```
#clear l2nat stats
```

Configuration Example of Network Address Translation

In this scenario, Layer 2 NAT is configured to translate the inside addresses from 172.16.1.0 255.255.255.0 subnet to addresses in the 192.168.150.0 255.255.255.0 subnet. Only the network prefix will be replaced during the translation. The host bits of the IP address remain the same.



The following command is configured for this scenario:

```
#configure l2nat add inside from network 172.16.1.0 to 192.168.150.0 255.255.255.0
```

Configuring Native VLAN on Ethernet Ports

A typical deployment of WGB is that a single wired client connects directly to the WGB Ethernet port. As a result, wired client traffic must be on the same VLAN as the WGB (or WLC/AP/WGB) management VLAN. If you need the wired client traffic to be on a different VLAN other than the WGB management VLAN, you should configure native VLAN on the Ethernet port.

Note Configuring native VLAN ID per Ethernet port is not supported. Both Ethernet ports share the same native VLAN configuration.

Note When WGB broadcast tagging is enabled and a single wired passive client connects directly to the WGB Ethernet port, it may hit the issue that infrastructure DS side client fails to ping this WGB behind the passive client. The workaround is to configure the following additional commands: **configure wgb ethport native-vlan enable** and **configure wgb ethport native-vlan id X**, where X is the same VLAN as the WGB (or WLC/AP/WGB) management VLAN.

The following table provides the commands to configure native VLAN:

Table 3: Native VLAN Configuration Commands

Command	Description
#**config wgb ethport native-vlan** {**enable**|**disable**} **Example:** `#config wgb ethport native-vlan enable`	Enables or disables native VLAN configuration.
#**config wgb ethport native-vlan id** <*vlan-id*> **Example:** `#config wgb ethport native-vlan id 2735`	Specifies native VLAN ID.

To verify your configuration, use the **show wgb ethport config** or **show running-config** command.

Low Latency Profile

IEEE 802.11 networks have a great role to play in supporting and deploying the Internet of Things (IoT) for the low latency and QoS requirement by applying the Enhanced Distributed Channel Access (EDCA), aggregated MAC protocol data unit (AMPDU), and aggregated or non-aggregated packet retry.

Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

Configuring WGB optimized-video EDCA Profile

To configure optimized low latency profile for video use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-video** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-video
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 4 10 11 0 0
AC_BK L 6 10 11 0 0
AC_VI L 3 4 2 94 0
AC_VO L 2 3 1 47 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Configuring WGB optimized-automation EDCA Profile

To configure optimized low latency profile for automation use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-automation** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-automation
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 7 10 12 0 0
AC_BK L 8 10 12 0 0
AC_VI L 7 7 3 0 0
AC_VO L 3 3 1 0 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Configuring WGB customized-wmm EDCA profile

To configure customized Wi-Fi Multimedia (WMM) profile, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile customized-wmm** {**enable** | **disable**}

To configure customized WMM profile parameters, use the following command:

#**configure dot11Radio** {**0**|**1**|**2**} **wmm** {**be** | **vi** | **vo** | **bk**} {**cwmin** <*cwmin_num*> | **cwmax** <*cwmax_num*> | **aifs** <*aifs_num*> | **txoplimit** <*txoplimit_num*>}

Parameter descriptions:

- be—best-effort traffic queue (CS0 and CS3)
- bk—background traffic queue (CS1 and CS2)
- vi—video traffic queue (CS4 and CS5)
- vo—voice traffic queue (CS6 and CS7)
- aifs—Arbitration Inter-Frame Spacing, <1-15> in units of slot time
- cwmin—Contention Window min, <0-15> 2^n-1, in units of slot time
- cwmax—Contention Window max, <0-15> 2^n-1, in units of slot time
- txoplimit—Transmission opportunity time, <0-255> integer number, in units of 32us

Configuring Low Latency Profile on WGB

Use the following command to configure low latency profile on WGB:

AP# **configure dot11Radio** <*radio_slot_id*> **profile low-latency** [**ampdu** <*length*>] [**sifs-burst** {**enable** | **disable**}] [**rts-cts** {**enable** | **disable**}] [**non-aggr** <*length*>] [**aggr** <*length*>]

Use the following command to display iot-low-latency profile EDCA detailed parameters:

```
#show controllers dot11Radio 1 | beg EDCA
EDCA config
L: Local C:Cell A:Adaptive EDCA params
  AC   Type  CwMin  CwMax Aifs Txop ACM
AC_BE     L      4      6   11    0   0
AC_BK     L      6     10   11    0   0
AC_VI     L      3      4    1    0   0
AC_VO     L      0      2    0    0   1
AC_BE     C      4     10   11    0   0
AC_BK     C      6     10   11    0   0
AC_VI     C      3      4    2   94   0
AC_VO     C      2      3    1   47   1
```

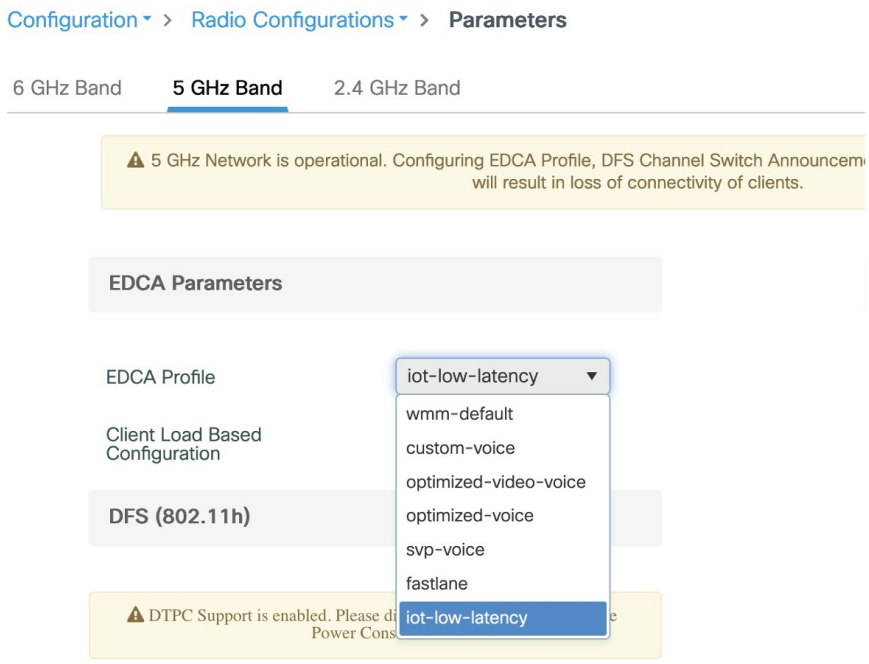
Configuring EDCA Parameters (Wireless Controller GUI)

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters**. Using this page, you can configure global parameters for 6 GHz, 5 GHz, and 2.4 GHz radios.

Note
You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the **Configuration > Radio Configurations > Network** page before you proceed.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.



Step 3 Click **Apply**.

Configuring EDCA Parameters (Wireless Controller CLI)

Procedure

Step 1 Enters global configuration mode.

configure terminal

Example:

```
Device# configure terminal
```

Step 2 Disables the radio network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

```
Device(config)# ap dot11 5ghz shutdown
```

Step 3 Enables iot-low-latency EDCA profile for the 5 GHz, 2.4 GHz, or 6 GHz network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency**

Example:

```
Device(config)# ap dot11 5ghz edca-parameters iot-low-latency
```

Step 4 Enables the radio network.

no ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

```
Device(config)# no ap dot11 5ghz shutdown
```

Step 5 Returns to privileged EXEC mode.

end

Example:

```
Device(config)# end
```

Step 6 Displays the current configuration.

show ap dot11 {**5ghz** | **24ghz** | **6ghz**} **network**

Example:

```
Device(config)# show ap dot11 5ghz network
EDCA profile type check                   : iot-low-latency
```

Configuring A-MPDU

Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).

The A-MPDU parameters define the size of an aggregated packet and define the proper spacing between aggregated packets so that the receive side WLAN station can decode the packet properly.

To configure profiled based A-MPDU under 2.4G, 5G and 6G radio, use the following commands:

WLC(config)# **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** <*profile-name*>

WLC(config-rf-profile)# [**no**] **dot11n a-mpdu tx block-ack window-size** <*1-255*>

Global configuration is a special profile which can also be configured bu using the following command:

WLC(config)#[**no**] **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** <*1-255*>

To bind different RF profiles with the radio RF tag, use the following command:

WLC(config)# **wireless tag rf** <*rf-tag-name*>

WLC (config-wireless-rf-tag)# **5ghz-rf-policy** <*rf-profile-name*>

Note RF profile level configured **a-mpdu tx block-ack window-size** value takes preference over globally configured value.

To display configured a-mpdu length value, use the following command:

show controllers dot11Radio <*radio_slot_id*>

```
AP# show controllers dot11Radio 1
Radio Aggregation Config:
=========================

TX A-MPDU Priority: 0x3f
TX A-MSDU Priority: 0x3f
TX A-MPDU Window:   0x7f
```

Import and Export WGB Configuration

You can upload the current configuration of an existing WGB to a server and then you can download it for newly deployed WGBs.

- Use the **copy configuration upload** <**sftp:**|**tftp:**> *ip-address* [*directory*] [*file-name*] command to upload the working configuration of an existing WGB to a server.

  ```
  Device#copy configuration upload <sftp:|tftp:> ip-address [directory] [file-name]
  ```

- Use the **copy configuration download** <**sftp:**|**tftp:**> *ip-address* [*directory*] [*file-name*] command to download a sample configuration to all WGBs in the deployment.

  ```
  Device#copy configuration download <sftp:|tftp:> ip-address [directory] [file-name]
  ```

Note When you execute the **copy configuration download** command, the AP starts to reboot. The new configuration takes effect after this reboot.

Verify the WGB and uWGB configuration

Use the **show run** command to check whether the AP is in WGB mode or uWGB mode.

- WGB:

  ```
  Device#show run
  AP Name              : APFC58.9A15.C808
  AP Mode              : WorkGroupBridge
  CDP State            : Enabled
  Watchdog monitoring  : Enabled
  ```

```
SSH State            : Disabled
AP Username          : admin
Session Timeout      : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
--------------------------
1           WGB           myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
   Mode              : WGB
   Dot11 type        : 11ax
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
```

- uWGB:

```
Device#show run
AP Name              : APFC58.9A15.C808
AP Mode              : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring  : Enabled
SSH State            : Disabled
AP Username          : admin
Session Timeout      : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
--------------------------
1           UWGB          myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
   Mode              : UWGB
   Uclient mac       : 0009.0001.0001
   Current state     : WGB
   UClient timeout   : 0 Sec
   Dot11 type        : 11ax
Radio Id             : NA
```

```
Admin state       : NA
Mode              : NA
```

Use the **show wgb dot11 associations** command to view the WGB and uWGB configuration.

- WGB:

```
Device#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:99:9A:15:B4:91
SSID Name : roam-m44-open
Parent AP Name : APFC58.9A15.C964
Parent AP MAC : 00:99:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Dot11 type : 11ax
Channel : 100
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 86/86 Mbps
Max Datarate : 143 Mbps
RSSI : 53
IP : 192.168.1.101/24
Default Gateway : 192.168.1.1
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```

- uWGB:

```
Device#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:09:00:01:00:01
SSID Name : roam-m44-open
Parent AP MAC : FC:58:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Uclient mac : 00:09:00:01:00:01
Current state : UWGB
Uclient timeout : 60 Sec
Dot11 type : 11ax
Channel : 36
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 77/0 Mbps
Max Datarate : 143 Mbps
RSSI : 60
IP : 0.0.0.0
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```