



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

**First Published:** 2023-12-15

**Last Modified:** 2024-10-09

### **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 1**

Overview of the Access Point 1

Related Documentation 1

---

**CHAPTER 2**

**Workgroup Bridges 3**

Overview 3

Limitations and Restrictions 4

Configuring Strong Password in Day0 5

Controller Configuration for WGB 7

uWGB Image Upgrade 7

WGB Configuration 8

Configuring a Dot1X Credential 9

Deauthenticating WGB Wired Client 9

Configuring an EAP Profile 9

Configuring Manual Enrollment of a Trustpoint for Terminal 10

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge 11

Configuring Manual Certificate Enrollment Using TFTP Server 12

SSID configuration 13

Creating an SSID Profile 13

Configuring Radio Interface for Workgroup Bridges 13

Configuring WGB or uWGB Timer 14

uWGB Configuration 14

Configuring a Dot1X Credential 15

Configuring an EAP Profile 15

Configuring Manual Enrollment of a Trustpoint for Terminal 16

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge	17
Configuring Manual Certificate Enrollment Using TFTP Server	18
SSID configuration	18
Creating an SSID Profile	19
Configuring Radio Interface for uWGB	19
Configuring IP Address	20
Configuring IPv4 Address	20
Configuring IPv6 Address	20
Configuring Syslog	20
Converting Between WGB and uWGB	21
LED Pattern	21
Configuring HT Speed Limit	22
Radio Statistics Commands	22
Event Logging	25
802.11v Support	26
Configure Aux Scanning	27
Configuring Scanning-Only Mode	27
Configuring Aux-Scan Handoff Mode	28
Configuring Layer 2 NAT	29
Configuration Example of Host IP Address Translation	32
Configuration Example of Network Address Translation	33
Configuring Native VLAN on Ethernet Ports	34
Low Latency Profile	34
Configuring WGB optimized-video EDCA Profile	35
Configuring WGB optimized-automation EDCA Profile	35
Configuring WGB customized-wmm EDCA profile	36
Configuring Low Latency Profile on WGB	36
Configuring EDCA Parameters (Wireless Controller GUI)	37
Configuring EDCA Parameters (Wireless Controller CLI)	37
Configuring A-MPDU	38
Importing and Exporting WGB Configuration	39
Verifying the Configuration of WGB and uWGB	39





# CHAPTER 1

## Introduction

---

- [Overview of the Access Point, on page 1](#)
- [Related Documentation, on page 1](#)

## 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, on page 3](#)
- [Limitations and Restrictions, on page 4](#)
- [Configuring Strong Password in Day0, on page 5](#)
- [Controller Configuration for WGB, on page 7](#)
- [uWGB Image Upgrade, on page 7](#)
- [WGB Configuration, on page 8](#)
- [uWGB Configuration, on page 14](#)
- [Configuring IP Address, on page 20](#)
- [Configuring Syslog, on page 20](#)
- [Converting Between WGB and uWGB, on page 21](#)
- [LED Pattern, on page 21](#)
- [Configuring HT Speed Limit, on page 22](#)
- [Radio Statistics Commands, on page 22](#)
- [Event Logging, on page 25](#)
- [802.11v Support, on page 26](#)
- [Configure Aux Scanning, on page 27](#)
- [Configuring Layer 2 NAT, on page 29](#)
- [Configuring Native VLAN on Ethernet Ports, on page 34](#)
- [Low Latency Profile, on page 34](#)
- [Importing and Exporting WGB Configuration, on page 39](#)
- [Verifying the Configuration of WGB and uWGB, on page 39](#)

## Overview

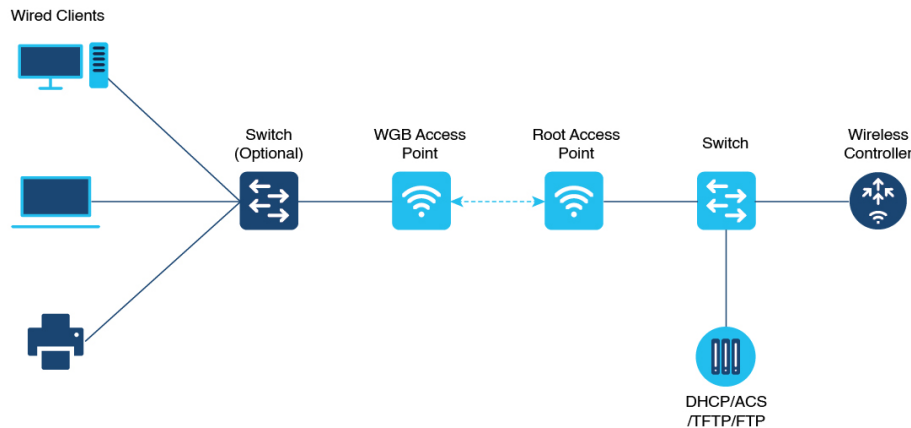
### Workgroup Bridge Mode

Workgroup Bridge Mode (WGB) is an Access Point (AP) mode that provides wireless connectivity to the wired clients. These clients are connected to the Ethernet port of the WGB AP. The WGB works like a bridge between the wired network and the single wireless segment. It does this by learning the MAC addresses of its wired clients on the Ethernet. 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) mode is a complementary mode of the WGB feature. 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: Example of a WGB



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 limitations and restrictions for WGB and uWGB modes.

- The WGB can associate only with Cisco lightweight access points. The uWGB can associate to a third party access point.
- Speed and duplex are automatically negotiated based on the capabilities of the locally connected endpoint and cannot be manually configured on the AP's wired 0 and wired 1 interfaces.
- Per-VLAN Spanning Tree (PVST) and packets are used to detect and prevent loops in the wired and wireless switching networks. WGB transparently bridge STP packets. WGB can bridge STP packets between two wired segments. Incorrect or inconsistent configuration of STP in the wired segments can cause WGB wireless link to be blocked by the connected switch(es) to Access Point or WGB. This could cause WGB to disconnect from AP or AP disconnection to Controller to drop, and wired clients not receiving IP addresses, as STP begins to block switch port in the wired network. If administrator needs to disable bridging of STP between the wired segments by the WGB, we recommend disabling the STP on the directly connected switches in the wireless network.
- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication



- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- When you deauthenticate a WGB record from a controller, all of the WGB wired clients' entries are also deleted.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
  - Idle timeout
- Associating a WGB to a WLAN that is configured for Adaptive 802.11r is not supported.
- WGB supports IPv6 only when IPv4 is enable. But there is no impact on WGB wired clients IPv6 traffic.
- WGB management IPv6 does not work after WGB uplink association is completed. WGB can get an IPv6 address when the association is successful. But IPv6 ping will not be passed from or to WGB. SSH from wireless or wired client to WGB management IPv6 is not working. The workaround to bypass the pingable issue is to re-enable IPv6, even though IPv6 has already been enabled and the IPv6 address has been assigned.
- The uWGB mode does not support TFTP or SFTP. For software upgrade, you should perform it from WGB mode. For more information, see [uWGB Image Upgrade, on page 7](#).
- 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 Cisco Unified Industrial Wireless Software Release 17.13.1, AP in uWGB mode supports to be managed by SSH, and image upgrade can be implemented when no wired client is detected.
  - When wired client is detected, AP in uWGB mode changes to uWGB state and AP cannot be managed.
  - When no wired client is detected, AP in uWGB mode changes to WGB state and AP can be managed.
- When the infrastructure AP operates on a non-DFS (Dynamic Frequency Selection) channel and changes its channel bandwidth, the WGB stays connected to the infrastructure AP using the original channel bandwidth.

To make sure the WGB connects to the AP with the correct channel bandwidth. Use **wireless client mac-address** *<wgb-wireless-client-mac-address>* **deauthenticate** command on the wireless controller to deauthenticate the WGB wireless client.

## Configuring Strong Password in Day0

It is required to set a strong password for WGB/uWGB after first login. The username and strong password should follow these rules:

1. Username length is between 1 and 32 characters.
2. Password length is between 8 to 120 characters.
3. Password must contain at least one uppercase character, one lowercase character, one digit, and one punctuation.
4. Password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not permitted: " (double quote), ' (single quote), ? (question mark).
5. Password cannot contain three sequential characters.
6. Password cannot contain three same characters consecutively.
7. Password cannot be the same as or reverse of the username.
8. New password must have at least four different characters compared to the current password.

For example, by default, the credential is

- username: Cisco
- password: Cisco
- enable password: Cisco

To reset the credential with the following strong password:

- 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 above example, all passwords are displayed in plain text for demonstration purpose. In real case, they are hidden by asterisks (\*).

---

## Controller Configuration for WGB

For a WGB to join a wireless network, you need to configure specific 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. Enter WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

```
#wlan profile-name
```

2. Configure the Cisco Client Extensions option and set the support of Aironet IE on the WLAN.

```
#ccx aironet-iesupport
```



---

**Note** Without this configuration, WGB is not able to associate to AP.

---

Follow these steps to configure WLAN policy profile:

1. Enter wireless policy configuration mode.

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

2. Assign the profile policy to the VLAN.

```
#vlan vlan-id
```

3. Configure WGB VLAN client support.

```
#wgb vlan
```

## uWGB Image Upgrade

uWGB mode does not support TFTP or SFTP. To perform a software upgrade, follow these steps:

### Procedure

---

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

**Step 2** Turn radio interfaces into Administratively Down state.

```
configure Dot11Radio slot_id disable
```

**Example:**

```
#configure Dot11Radio 1 disable
```

**Step 3** Convert uWGB to WGB mode.

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

**Example:**

```
#configure Dot11Radio 1 mode wgb ssid-profile a_uwgb_demo_ssid
```

This command will reboot with downloaded configs.

Are you sure you want continue? <**confirm**>

**Note** *ssid\_profile\_name* can be any existing SSID profile configured by users.

**Step 4** After rebooting, assign a static IP address to the WGB.

```
configure ap address ipv4 static IPv4_address netmask Gateway_IPv4_address
```

**Example:**

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

**Step 5** Verify the ICMP ping works.

```
ping server_IP
```

**Example:**

```
#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** Upgrade the software.

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

**Step 7** Convert WGB back to uWGB.

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

**Example:**

```
#configure Dot11Radio 1 mode uwgb 00b4.9e00.a891 ssid-profile a_uwgb_demo_ssid
```

## WGB Configuration

The typical WGB configuration involves the following steps:

1. Create an SSID profile.
2. Configure radio as workgroup, and associate the SSID profile to the radio.
3. Turn on the radio.

WGB uplink supports various security methods, including:

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

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 wgb ssid-profile demo-FAST
configure dot11radio 1 enable
```

The following sections provide detailed information about WGB configuration:

## Configuring a Dot1X Credential

Configure a dot1x credential by entering this command:

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

View the WGB EAP dot1x profile summary by entering this command:

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

## Deauthenticating WGB Wired Client

Deauthenticate WGB wired client by entering this command:

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

## Configuring an EAP Profile

Follow these steps to configure the EAP profile:

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

### Procedure

- 
- Step 1** Configure the EAP profile method type by entering this command:
- ```
# configure eap-profile profile-name method {fast | leap | peap | tls}
```
- Step 2** Attaching the CA Trustpoint for TLS by entering the following command. With the default profile, WGB uses the internal MIC certificate for authentication.
- ```
# configure eap-profile profile-name trustpoint {default | name trustpoint-name}
```

- Step 3** Bind dot1x-credential profile by entering this command:  
**# configure eap-profile** *profile-name* **dot1x-credential** *profile-name*
- Step 4** [Optional] Delete an EAP profile by entering this command:  
**# configure eap-profile** *profile-name* **delete**
- Step 5** View summary of EAP and dot1x profiles by entering this command:  
**# show wgb eap profile all**
- 

## Configuring Manual Enrollment of a Trustpoint for Terminal

### Procedure

---

- Step 1** Create a Trustpoint in WGB by entering this command:  
**# configure crypto pki trustpoint** *ca-server-name* **enrollment terminal**

- Step 2** Authenticate a Trustpoint manually by entering this command:  
**# configure crypto pki trustpoint** *ca-server-name* **authenticate**  
 Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

**Note** User has to import complete certificate chains in the trustpoint if intermediate certificate is used.

#### Example:

```
#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** Configure a private key size by entering this command:  
**# configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length*
- Step 4** Configure the subject-name by entering this command:  
**# configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [Optional] *2ltr-country-code state-name locality org-name org-unit email*
- Step 5** Generate a private key and Certificate Signing Request (CSR) by entering this command:  
**# configure crypto pki trustpoint** *ca-server-name* **enroll**

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

- Step 6** Import the signed certificate in WGB by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* import certificate**  
Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.
- Step 7** [Optional] Delete a Trustpoint by entering this command:  
**# configure crypto pki trustpoint *trustpoint-name* delete**
- Step 8** View the Trustpoint summary by entering this command:  
**# show crypto pki trustpoint**
- Step 9** View the content of the certificates that are created for a Trustpoint by entering this command:  
**# show crypto pki trustpoint *trustpoint-name* certificate**
- 

## Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge

### Procedure

---

- Step 1** Enroll a Trustpoint in WGB using the server URL by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* enrollment url *ca-server-url***
- Step 2** Authenticate a Trustpoint by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* authenticate**  
This command will fetch the CA certificate from CA server automatically.
- Step 3** Configure a private key size by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* key-size *key-length***
- Step 4** Configure the subject-name by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* subject-name *name* [Optional] *2ltr-country-code state-name locality org-name org-unit email***
- Step 5** Enroll the Trust point by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* enroll**  
Request the digitally signed certificate from the CA server.
- Step 6** Enable auto-enroll by entering this command:  
**# configure crypto pki trustpoint *ca-server-name* auto-enroll enable *renew-percentage***  
You can disable auto-enrolling by using the disable syntax in the command.
- Step 7** [Optional] Delete a Trustpoint by entering this command:

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

**Step 8** View the Trustpoint summary by entering this command:

```
# show crypto pki trustpoint
```

**Step 9** View the content of the certificates that are created for a Trustpoint by entering this command:

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

**Step 10** View the PKI timer information by entering this command:

```
# show crypto pki timers
```

## Configuring Manual Certificate Enrollment Using TFTP Server

### Procedure

- Step 1** Specify the enrollment method to retrieve the CA certificate and client certificate for a Trustpoint in WGB by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```
- Step 2** Authenticate a Trustpoint manually by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name authenticate
```
- Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension “.ca” to the specified filename.
- Step 3** Configure a private key size by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name key-size key-length
```
- Step 4** Configure the subject-name by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code state-name  
locality org-name org-unit email
```
- Step 5** Generate a private key and Certificate Signing Request (CSR) by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name enroll
```
- Generates certificate request and writes the request out to the TFTP server. The filename to be written is appended with the extension “.req”.
- Step 6** Import the signed certificate in WGB by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name import certificate
```
- Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The WGB will attempt to retrieve the granted certificate via TFTP using the same filename and the file name append with “.crt” extension.
- Step 7** View the Trustpoint summary by entering this command:



```
# show crypto pki trustpoint
```

**Step 8** View the content of the certificates that are created for a Trustpoint by entering this command:

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

---

## SSID configuration

SSID configuration consists of the following two parts:

### Creating an SSID Profile

Choose one of the following authentication protocols for the SSID profile:

#### Configuring an SSID profile with Open Authentication

Use the following command to configure an SSID profile with Open Authentication:

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

#### Configuring an SSID profile with PSK Authentication

Use the following command to configure an SSID profile with PSK WPA2 Authentication:

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

Use the following command to configure an SSID profile with PSK Dot11r Authentication:

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

Use the following command to configure an SSID profile with PSK Dot11w Authentication:

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

#### Configuring an SSID Profile with Dot1x Authentication

Use the following commands to configure an SSID profile with Dot1x authentication:

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

The following example configures an SSID profile with Dot1x EAP-PEAP authentication:

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

## Configuring Radio Interface for Workgroup Bridges

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

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

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

#### Example

```
#configure dot11radio 1 mode wgb ssid-profile psk_ssid
```

- Configure a radio interface by entering this command:

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

#### Example

```
#configure dot11radio 1 disable
```

## Configuring WGB or uWGB Timer

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

- Configure the WGB association response timeout by entering this command:

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

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

- Configure the WGB authentication response timeout by entering this command:

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

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

- Configure the WGB EAP timeout by entering this command:

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

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

- Configure the WGB bridge client response timeout by entering this command:

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

Default timeout value is 300 seconds. 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:

## Configuring a Dot1X Credential

Configure a dot1x credential by entering this command:

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

View the WGB EAP dot1x profile summary by entering this command:

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

## Configuring an EAP Profile

Follow these steps to configure the EAP profile:

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

### Procedure

---

- Step 1** Configure the EAP profile method type by entering this command:
- ```
# configure eap-profile profile-name method { fast | leap | peap | tls }
```
- Step 2** Attaching the CA Trustpoint for TLS by entering the following command. With the default profile, WGB uses the internal MIC certificate for authentication.
- ```
# configure eap-profile profile-name trustpoint { default | name trustpoint-name }
```
- Step 3** Bind dot1x-credential profile by entering this command:
- ```
# configure eap-profile profile-name dot1x-credential profile-name
```
- Step 4** [Optional] Delete an EAP profile by entering this command:
- ```
# configure eap-profile profile-name delete
```
- Step 5** View summary of EAP and dot1x profiles by entering this command:
- ```
# show wgb eap profile all
```
-

# Configuring Manual Enrollment of a Trustpoint for Terminal

## Procedure

**Step 1** Create a Trustpoint in WGB by entering this command:

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

**Step 2** Authenticate a Trustpoint manually by entering this command:

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

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

**Note** User has to import complete certificate chains in the trustpoint if intermediate certificate is used.

### Example:

```
#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** Configure a private key size by entering this command:

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

**Step 4** Configure the subject-name by entering this command:

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

**Step 5** Generate a private key and Certificate Signing Request (CSR) by entering this command:

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

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

**Step 6** Import the signed certificate in WGB by entering this command:

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

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

**Step 7** [Optional] Delete a Trustpoint by entering this command:

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

**Step 8** View the Trustpoint summary by entering this command:

```
# show crypto pki trustpoint
```

**Step 9** View the content of the certificates that are created for a Trustpoint by entering this command:

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

---

## Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge

### Procedure

---

**Step 1** Enroll a Trustpoint in WGB using the server URL by entering this command:

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

**Step 2** Authenticate a Trustpoint by entering this command:

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

This command will fetch the CA certificate from CA server automatically.

**Step 3** Configure a private key size by entering this command:

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

**Step 4** Configure the subject-name by entering this command:

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

**Step 5** Enroll the Trust point by entering this command:

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

Request the digitally signed certificate from the CA server.

**Step 6** Enable auto-enroll by entering this command:

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

You can disable auto-enrolling by using the disable syntax in the command.

**Step 7** [Optional] Delete a Trustpoint by entering this command:

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

**Step 8** View the Trustpoint summary by entering this command:

```
# show crypto pki trustpoint
```

**Step 9** View the content of the certificates that are created for a Trustpoint by entering this command:

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

**Step 10** View the PKI timer information by entering this command:

```
# show crypto pki timers
```

---

# Configuring Manual Certificate Enrollment Using TFTP Server

## Procedure

- 
- Step 1** Specify the enrollment method to retrieve the CA certificate and client certificate for a Trustpoint in WGB by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```
- Step 2** Authenticate a Trustpoint manually by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name authenticate
```
- Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension “.ca” to the specified filename.
- Step 3** Configure a private key size by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name key-size key-length
```
- Step 4** Configure the subject-name by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code state-name locality org-name org-unit email
```
- Step 5** Generate a private key and Certificate Signing Request (CSR) by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name enroll
```
- Generates certificate request and writes the request out to the TFTP server. The filename to be written is appended with the extension “.req”.
- Step 6** Import the signed certificate in WGB by entering this command:
- ```
# configure crypto pki trustpoint ca-server-name import certificate
```
- Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The WGB will attempt to retrieve the granted certificate via TFTP using the same filename and the file name append with “.crt” extension.
- Step 7** View the Trustpoint summary by entering this command:
- ```
# show crypto pki trustpoint
```
- Step 8** View the content of the certificates that are created for a Trustpoint by entering this command:
- ```
# show crypto pki trustpoint trustpoint-name certificate
```
- 

## SSID configuration

SSID configuration consists of the following two parts:

1. [Creating an SSID Profile, on page 13](#)
2. [Configuring Radio Interface for uWGB, on page 19](#)

## Creating an SSID Profile

Choose one of the following authentication protocols for the SSID profile:

### Configuring an SSID profile with Open Authentication

Use the following command to configure an SSID profile with Open Authentication:

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

### Configuring an SSID profile with PSK Authentication

Use the following command to configure an SSID profile with PSK WPA2 Authentication:

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

Use the following command to configure an SSID profile with PSK Dot11r Authentication:

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

Use the following command to configure an SSID profile with PSK Dot11w Authentication:

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

### Configuring an SSID Profile with Dot1x Authentication

Use the following commands to configure an SSID profile with Dot1x authentication:

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

The following example configures an SSID profile with Dot1x EAP-PEAP authentication:

```
configure dot1x credential c1 username wgbusr password cisco123456
configure eap-profile p1 dot1x-credential c1
configure eap-profile p1 method peap
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
```

# Configuring IP Address

## Configuring IPv4 Address

Configure the IPv4 address of the AP by entering the following commands:

- To configure IPv4 address by DHCP, use the following command:

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

- To configure the static IPv4 address, use the following command. By doing so, you can manage the device via wired interface without uplink connection.

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

- To display current IP address configuration, use the following command:

```
#show ip interface brief
```

## Configuring IPv6 Address

Configure the IPv6 address of the AP by entering the following commands:

- To configure the static IPv6 address, use the following command. By doing so, you can manage the device via wired interface without uplink connection.

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

- #configure ap address ipv6 auto-config {enable|disable}



---

**Note** The **configure ap address ipv6 auto-config enable** command is designed to enable IPv6 SLAAC. However, SLAAC is not applicable for cos WGB. This CLI will configure IPv6 address with DHCPv6 instead of SLAAC.

---

- To configure IPv6 address by DHCP, use the following command:

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

- To display current IP address configuration, use the following command:

```
#show ipv6 interface brief
```

## Configuring Syslog

Syslog is a common protocol that the device uses to send event data logs to a central location for storing. Currently, only UDP mode is supported. Additional debug log will be collected if debug command is enabled in WGB. All collected log sent to syslog server will be in "kernel" facility and "warning" level.

- To enable WGB syslog, use the following command:



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

- To disable WGB syslog (default), use the following command:

```
# logging host enable 0.0.0.0 UDP
```

- To display current syslog configuration, use the following command:

```
# show running-config
```

## Converting Between WGB and uWGB

To convert from WGB to uWGB, use the following command:

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

To convert from uWGB to WGB, use the following command. This conversion involves a reboot of the AP.

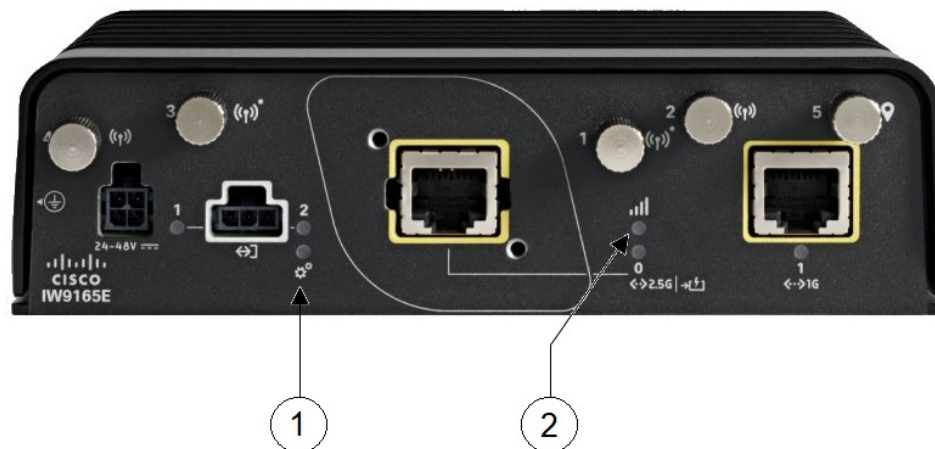
```
#configure Dot11Radio 1 mode wgb ssid-profile <SSID_PROFILE_NAME>
```

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

## LED Pattern

There are two LEDs located at the AP front panel, a system status LED and an RSSI LED, as shown in the following figure.

Figure 2: IW9165E LEDs



|   |                                                                                                                                                                                                                                           |   |                                                                                                                                                                                                                                                                                                                                                  |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <p>System Status LED</p> <ul style="list-style-type: none"> <li>• When WGB is in disassociated state, the System LED is blinking RED.</li> <li>• When WGB makes association to parent AP, the System LED turns to solid GREEN.</li> </ul> | 2 | <p>RSSI Status LED</p> <ul style="list-style-type: none"> <li>• When RSSI <math>\geq</math> -71dBm, the RSSI LED is solid GREEN.</li> <li>• When -81 dBm <math>\leq</math> RSSI &lt; -70 dBm, the RSSI LED is blinking GREEN.</li> <li>• When -81 dBm &lt; RSSI &lt; -95 dBm, the RSSI LED is solid YELLOW.</li> <li>• Otherwise Off.</li> </ul> |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Configuring HT Speed Limit

In WGB field moving case deployment, you can manually set a transmission rate limit with High Throughput (HT) Modulation and Coding Scheme (MCS) .

The following is an example to configure WGB to transmit with 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 also supports to configure legacy rate:

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

Legacy rate is used by 802.11 management frame and control frame. WGB legacy rates should match AP's legacy rates, or at least, having overlap between these two rate sets. Otherwise, WGB association will be rejected due to mismatched rates.

To check WGB Tx MCS rate, use the **debug wgb dot11 rate** command. 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] 24:16:18:F8:02:6E MAC Tx-Pkts Rx-Pkts Tx-Rate(Mbps) Rx-Rate(Mbps) RSSI Tx-Retries
JWGB1#[*10/14/2023 03:16:09.6179] 24:16:18:F8:02:6E 330 2 3 HT-20,1SS,MCS5,(52) HT-20,1SS,MCS5,SGI(57) -70 0
[*10/14/2023 03:16:10.6183] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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] 24:16:18: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]
Tx-Rate (Mbps) MAC Tx-Pkts Rx-Pkts
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          0
AC_BE          1840      4243793      1809          10
14             7          0          0          0
AC_VI          0          0          0          0
0              0          0          0          0
AC_VO          24          54134        24          0
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 0 543 96
(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

```

| 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`:

```
APCOF8.7FE5.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:

```
APCOF8.7FE5.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](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 default, 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 association 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 **servicing** 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

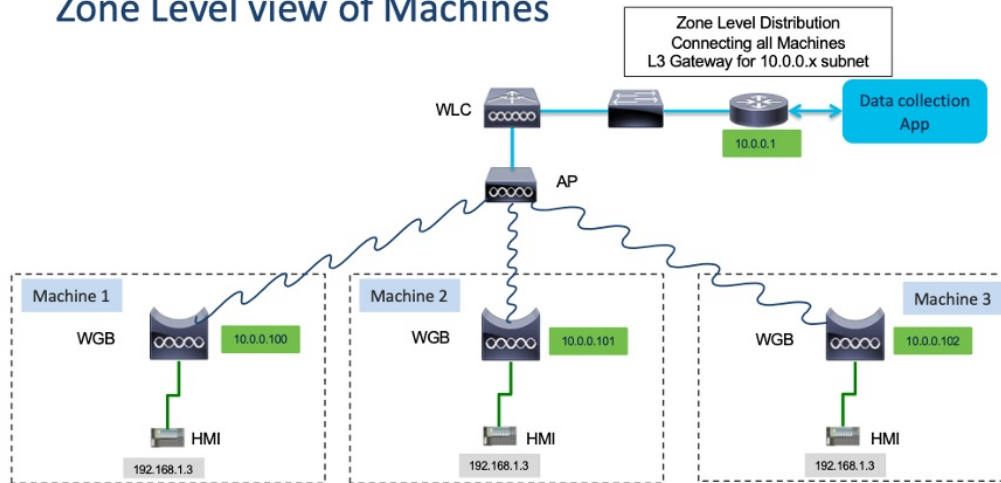
```

## 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.

## Zone Level view of Machines



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

**Table 1: Layer 2 NAT Configuration Commands**

| Command                                                                                                             | Description                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>#configure l2nat {enable disable}</code>                                                                      | Enables or disables L2 NAT.                                                                                                                                                                                                                                                                                                                            |
| <code>#configure l2nat default-vlan &lt;vlan_id&gt;</code>                                                          | Specifies the default vlan where all NAT rules will be applied. If <i>vlan_id</i> is not specified, all NAT rules will be applied to vlan 0.                                                                                                                                                                                                           |
| <code>#configure l2nat {add delete} inside from host &lt;original_ip_addr&gt; to &lt;translated_ip_addr&gt;</code>  | Adds or deletes a NAT rule which translates a private IP address to a public IP address. <ul style="list-style-type: none"> <li>• <i>original_ip_addr</i>—Private IP address of the wired client connected to WGB Ethernet port.</li> <li>• <i>translated_ip_addr</i>—Public IP address that represents the wired client at public network.</li> </ul> |
| <code>#configure l2nat {add delete} outside from host &lt;original_ip_addr&gt; to &lt;translated_ip_addr&gt;</code> | Adds or deletes a NAT rule which translates a public IP address to a private IP address. <ul style="list-style-type: none"> <li>• <i>original_ip_addr</i>—Public IP address of an outside network host.</li> <li>• <i>translated_ip_addr</i>—Private IP address which represents the outside network host at private network.</li> </ul>               |

| Command                                                                                                                      | Description                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>#configure l2nat {add delete} inside from network</b><br><original_nw_prefix> to <translated_nw_prefix><br><subnet_mask>  | Adds or deletes a NAT rule which translates a private IP address subnet to a public IP address subnet. <ul style="list-style-type: none"> <li>• <i>original_nw_prefix</i>—Private IP network prefix.</li> <li>• <i>translated_nw_prefix</i>—Public IP network prefix.</li> </ul> |
| <b>#configure l2nat {add delete} outside from network</b><br><original_nw_prefix> to <translated_nw_prefix><br><subnet_mask> | Adds or deletes a NAT rule which translates a public IP address subnet to a private IP address subnet. <ul style="list-style-type: none"> <li>• <i>original_nw_prefix</i>—Public IP network prefix.</li> <li>• <i>translated_nw_prefix</i>—Private IP network prefix.</li> </ul> |

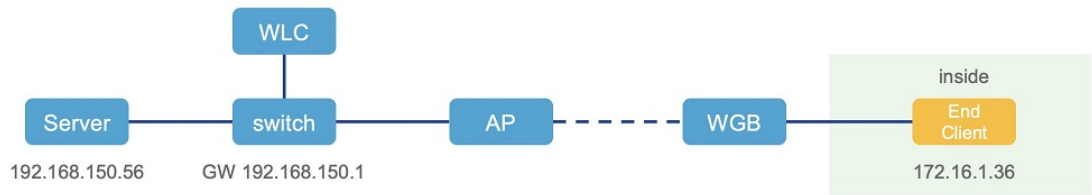
The following table provides the show and debug commands to verify and troubleshoot your Layer 2 NAT configuration:

**Table 2: Layer 2 NAT Show and Debug Commands**

| Command                        | Description                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>#show l2nat entry</b>       | Displays the Layer 2 NAT running entries.                                                                                                                                                                                                                                  |
| <b>#show l2nat config</b>      | Displays the Layer 2 NAT configuration details.                                                                                                                                                                                                                            |
| <b>#show l2nat stats</b>       | Displays the Layer 2 NAT packet translation statistics.                                                                                                                                                                                                                    |
| <b>#show l2nat rules</b>       | Displays the Layer 2 NAT rules from the configuration.                                                                                                                                                                                                                     |
| <b>#clear l2nat statistics</b> | Clears packet translation statistics.                                                                                                                                                                                                                                      |
| <b>#clear l2nat rule</b>       | Clears Layer 2 NAT rules.                                                                                                                                                                                                                                                  |
| <b>#clear l2nat config</b>     | Clears Layer 2 NAT configuration.                                                                                                                                                                                                                                          |
| <b>#debug l2nat</b>            | Enables debugging of packet translation process.                                                                                                                                                                                                                           |
| <b>#debug l2nat all</b>        | Prints out the NAT entry match result when a packet arrives. <p><b>Caution</b> 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.</p> |
| <b>#undebug l2nat</b>          | 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                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <pre>#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</pre> | Adds NAT rules to make inside client and outside server communicate with each other. |
| <pre>#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</pre>  | 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 enabled:

```

#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 enabled:

```

#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

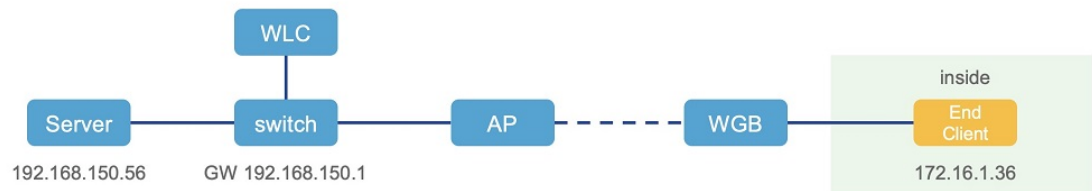
```

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                                    |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>#config wgb ethport native-vlan {enable disable}</b><br><b>Example:</b><br><pre>#config wgb ethport native-vlan enable</pre>    | Enables or disables native VLAN configuration. |
| <b>#config wgb ethport native-vlan id &lt;vlan-id&gt;</b><br><b>Example:</b><br><pre>#config wgb ethport native-vlan id 2735</pre> | 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
=====
wbridgel A-MPDU Priority 0: Enabled
wbridgel A-MPDU Priority 1: Enabled
wbridgel A-MPDU Priority 2: Enabled
wbridgel A-MPDU Priority 3: Enabled
wbridgel A-MPDU Priority 4: Disabled
wbridgel A-MPDU Priority 5: Disabled
wbridgel A-MPDU Priority 6: Disabled
wbridgel A-MPDU Priority 7: Disabled
wbridgel A-MPDU subframe number: 3
wbridgel 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
=====
wbridgel A-MPDU Priority 0: Enabled
wbridgel A-MPDU Priority 1: Enabled
wbridgel A-MPDU Priority 2: Enabled
wbridgel A-MPDU Priority 3: Enabled
wbridgel A-MPDU Priority 4: Disabled
wbridgel A-MPDU Priority 5: Disabled
wbridgel A-MPDU Priority 6: Disabled
wbridgel A-MPDU Priority 7: Disabled
wbridgel A-MPDU subframe number: 3
wbridgel 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} {cwmmin <cwmmin_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
- cwmmin—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.

Configuration > Radio Configurations > Parameters

6 GHz Band    **5 GHz Band**    2.4 GHz Band

⚠ 5 GHz Network is operational. Configuring EDCA Profile, DFS Channel Switch Announcement will result in loss of connectivity of clients.

#### EDCA Parameters

EDCA Profile

iot-low-latency ▾

Client Load Based Configuration

wmm-default

custom-voice

optimized-video-voice

optimized-voice

svp-voice

fastlane

DFS (802.11h)

⚠ DTPC Support is enabled. Please disable DTPC Support to improve Power Consumption.

iot-low-latency

**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 by 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
```

## Importing and Exporting WGB Configuration

You can upload the working configuration of an existing WGB to a server, and then download it to the new deployed WGBs.

To upload the configuration to a server, use the following command:

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

To download a sample configuration to all WGBs in the deployment, use the following command:

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

The access point will reboot after the **copy configuration download** command is executed. The imported configuration will take effect after the rebooting.

## Verifying the Configuration of WGB and uWGB

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

- WGB:

```
#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:

```

#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 verify the configuration of WGB and uWGB.

- WGB:

```

#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:

```
#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
```



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

