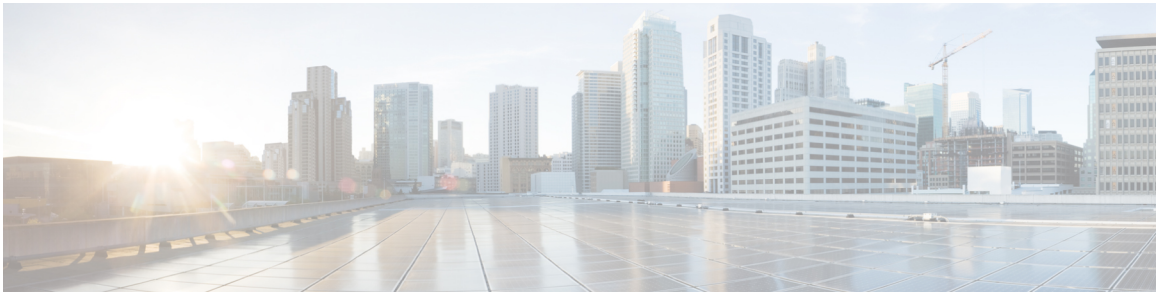


Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-28

Last Modified: 2024-11-16

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



CONTENTS

CHAPTER 1 **Introduction** 1

Overview of the Access Point 1

Determine Image on IW9167EH 2

Configuring AP to Boot up with Different Image Options 3

Upgrade IW9167EH with 17.9.x to Support WGB/uWGB 3

Related Documentation 4

CHAPTER 2 **AP Mode Configuration** 7

Configuring Indoor Deployment for -E Domain 7

802.11ax 1600ns and 3200ns Guard Interval Support 10

Configuring 802.11ax Long Guard Interval 10

GNSS Support 11

RAP Ethernet Daisy Chain 12

WSTP Overview 13

Comparison with Previous Release 13

RAP Ethernet Daisy Chain Configuration 14

Preconfiguring RAP Ethernet Daisy Chain Before Field Deployment 14

Enabling RAP Ethernet Daisy Chain 16

Configuring Super Root 17

Configuring Primary Ethernet Port 18

Configuring Ethernet Bridging and Ethernet Port 18

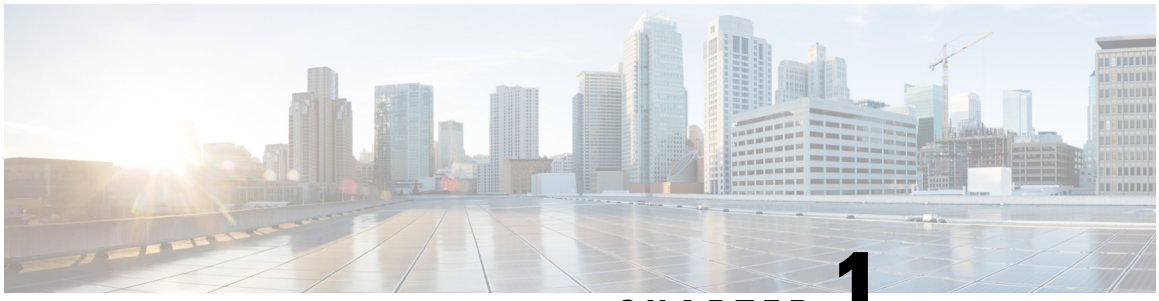
Show and Debug Command 21

CHAPTER 3 **Workgroup Bridges** 23

Overview 23

Limitations and Restrictions 24
Configuring Strong Password in Day0 25
Controller Configuration for WGB 26
uWGB Image Upgrade 27
WGB Configuration 28
Configure IP address 29
Configure IPv4 address 29
Configure IPv6 address 30
Configure a Dot1X credential 30
Deauthenticate WGB wired client 30
Configure an EAP profile 31
Configure trustpoint manual enrollment for terminal 31
Configure trustpoint auto-enrollment for WGB 33
Configure manual certificate enrollment using TFTP server 34
SSID configuration 35
Create an SSID profile 35
Configuring Radio Interface for Workgroup Bridges 36
Configuring WGB/uWGB Timer 37
uWGB Configuration 37
Configure IP address 38
Configure IPv4 address 38
Configure IPv6 address 38
Configure a Dot1X credential 39
Configure an EAP profile 39
Configure trustpoint manual enrollment for terminal 40
Configure trustpoint auto-enrollment for WGB 41
Configure manual certificate enrollment using TFTP server 42
SSID configuration 43
Create an SSID profile 43
Configuring Radio Interface for uWGB 44
Converting Between WGB and uWGB 45
Fast Roaming With Assistant Second 5G Radio 45
LED Pattern 46
Configuring WGB/uWGB Radio Parameters 46

Configuring WGB Radio Antenna 46
802.11ax 1600ns and 3200ns Guard Interval 47
Customized Transmit Power 47
Assign Country Code to WGB/uWGB With -ROW PID 47
Indoor Deployment for -E Domain and United Kingdom 47
Configuring WGB Roaming Parameters 48
Importing and Exporting WGB Configuration 48
Verifying the Configuration of WGB and uWGB 49



CHAPTER 1

Introduction

- Overview of the Access Point, on page 1
- Determine Image on IW9167EH, on page 2
- Configuring AP to Boot up with Different Image Options, on page 3
- Upgrade IW9167EH with 17.9.x to Support WGB/uWGB, on page 3
- Related Documentation, on page 4

Overview of the Access Point

The Cisco Catalyst IW9167E Heavy Duty Access Point provides reliable wireless connectivity for mission-critical applications in a state-of-the art platform. It can operate as Cisco Catalyst Wi-Fi (CAPWAP) mode or Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) mode starting from IOS XE Cupertino 17.9.3 Software Release. The IW9167EH access point has the flexibility to change the operating mode from Wi-Fi to Cisco URWB, and vice versa.

Starting from Cisco IOS XE Dublin 17.11.1, Workgroup Bridge (WGB) and Universal WGB (uWGB) are supported on the Cisco Catalyst IW9167E Heavy Duty Access Points.

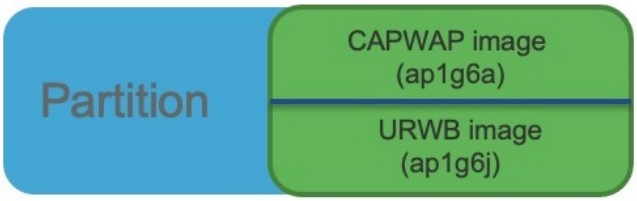
This document covers configuration of CAPWAP mode and WGB/uWGB mode specific to the IW9167EH access points.

For CAPWAP mode, the access points can operate in the following modes:

- Local
- Flexconnect
- Bridge
- Flexconnect + Bridge
- Sniffer
- Monitor
- Site survey

Determine Image on IW9167EH

Software images are stored under different folders on the same partition on IW9167EH.



You need to choose the image to boot up with according to the mode your AP is runnning, CAPWAP, Cisco URWB, or WGB/uWGB. The following table provides the software images of each mode:

Table 1: IW9167EH Software Images

IW9167EH Mode	Software Image
CAPWAP	**ap1g6a-k9w8-xxx.tar**
Cisco URWB	Unified Industrial Wireless image **ap1g6j-k9c1-xxx.tar**
WGB/uWGB	

To determine the image that your IW9167EH is running, use the **show version** command.

- If the **show version** output displays **Cisco AP Software, (ap1g6a)** as shown in the following example, it means that AP is running the CAPWAP image **ap1g6a-k9w8-xxx.tar**, which supports the CAPWAP mode.

```
Cisco AP Software, (ap1g6a), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Fri Jul 29 01:56:00 PDT 2022

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100

APFC58.9A16.E648 uptime is 0 days, 1 hours, 03 minutes
Last reload time   : Mon Sep 19 02:23:13 UTC 2022
Last reload reason : Image Upgrade

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1757076/1006864K bytes of memory.
```

- If the **show version** output displays **Cisco AP Software (ap1g6j)** as shown in the following example, it means that AP is running **ap1g6j-k9c1-xxx.tar** image, which supports the Cisco URWB mode or Cisco WGB/uWGB.

```
Cisco AP Software, (ap1g6j), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu Aug 18 01:01:29 PDT 2022

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100

APFC58.9A16.E464 uptime is 1 days, 3 hours, 58 minutes
```

```
Last reload time   : Wed Sep 7 11:17:00 UTC 2022
Last reload reason : reload command

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1759128/1091316K bytes of memory.
```

Configuring AP to Boot up with Different Image Options

To configure the access point to boot up with CAPWAP, URWB, or WGB/uWGB mode, follow these steps:

Note Switching between different modes performs full factory reset. Any configuration and data will be removed completely.

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure boot mode** {**capwap** | **urwb** | **wgb**}

Configures AP to CAPWAP, URWB, or WGB/uWGB mode. AP will reboot with specified mode.

Upgrade IW9167EH with 17.9.x to Support WGB/uWGB

If your IW9167EH is shipped with Cisco IOS XE Cupertino 17.9.3 software and operating as CAPWAP mode, and you want to upgrade your AP to Cisco IOS XE Dublin 17.11.1 to support WGB/uWGB mode, you need to switch your AP to Cisco URWB mode first, and then you can upgrade to 17.11.1.

To determine whether your IW9167EH is running CAPWAP mode or Cisco URWB mode, use the **show version** command.

- If the **show version** output displays **Cisco AP Software (ap1g6a)**, your AP is running as CAPWAP mode.
- If the **show version** output displays **Cisco AP Software (ap1g6j)**, your AP is running as Cisco URWB mode.

Cisco WGB/uWGB mode shares the same image with Cisco URWB. You cannot upgrade the **ap1g6j** image to 17.11.1 in CAPWAP mode (**ap1g6a**). Because the **archive download** command checks image type, upgrade gets aborted if image types mismatch.

Procedure

Step 1 Convert CAPWAP mode to Cisco URWB mode.

Example:

```
#configure boot mode urwb
       Before image swapping device need factory reset. Are you sure to proceed? (Y/N):y
       Converting to Cisco URWB Mode...
       <rebooting…>
```

Step 2 Log in with default credential (Cisco/Cisco/Cisco).

Step 3 Configure Cisco URWB, to make it work in **Offline** mode.

Example:

```
#configure iotod-iw offline
       Switching to IOTOD IW Offline mode...
       Will switch from Provisioning Mode to IOTOD IW offline Mode, device need to reboot: Y/N?  Y
       <rebooting…>
```

Step 4 Configure networking in Cisco URWB (IP/netmask/gateway, passphrase)

Example:

```
Cisco-23.174.76#configure wireless passphrase unit1
Cisco-23.174.76#configure ap address ipv4 static 192.168.1.200 255.255.255.0 192.168.1.1
Cisco-23.174.76#write
Cisco-23.174.76#reload
     <rebooting…>
```

Note
Passphrase is optional, but it is recommended to assign different passphrases if you are upgrading multiple units at the same time and they are connected to the same Layer 2 network. Because Cisco URWB forms MPLS network automatically if all nodes have the same passphrase, without further MPLS configuration, your IP service might not work properly.

Step 5 Upgrade to 17.11.1.

Example:

```
#archive download-sw /reload tftp://<TFTP_SERVER>/<ap1g6j-FILENAME>
          <rebooting…>
```

Step 6 Convert the AP from Cisco URWB mode to Cisco WGB/uWGB mode.

Example:

```
#configure boot mode wgb
           <rebooting…>
```

Related Documentation

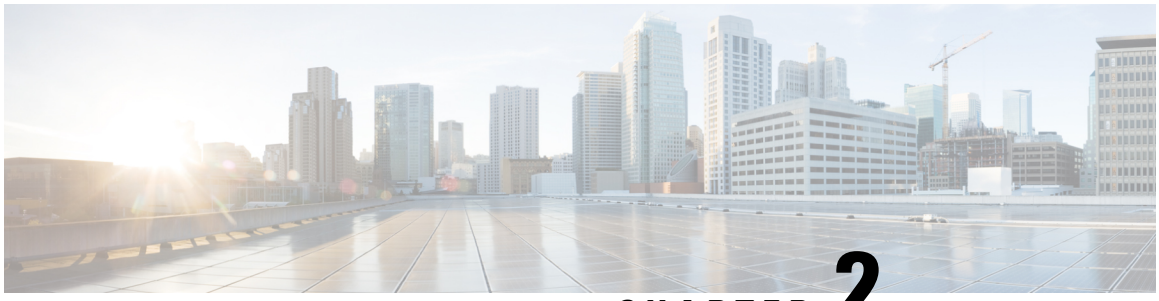
To view all support information for the Cisco Catalyst IW9167E Heavy Duty Access Point, see https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html.

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

- For information about IW9167EH hardware, see Cisco Catalyst IW9167E Heavy Duty Access Point Hardware Installation Guide.
- A full listing of the AP's features and specifications is provided in Cisco Catalyst IW9167E Heavy Duty Access Point Data Sheet.
- For more information about the configuration on Cisco Catalyst 9800 Series Wireless Controllers, see https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html.
- For information about Cisco URWB mode configuration, see the relevant documents at:

  https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html.
- For more information about Cisco IOS XE, see the relevant documents at:

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html



CHAPTER 2

AP Mode Configuration

- Configuring Indoor Deployment for -E Domain, on page 7
- 802.11ax 1600ns and 3200ns Guard Interval Support, on page 10
- GNSS Support, on page 11
- RAP Ethernet Daisy Chain, on page 12

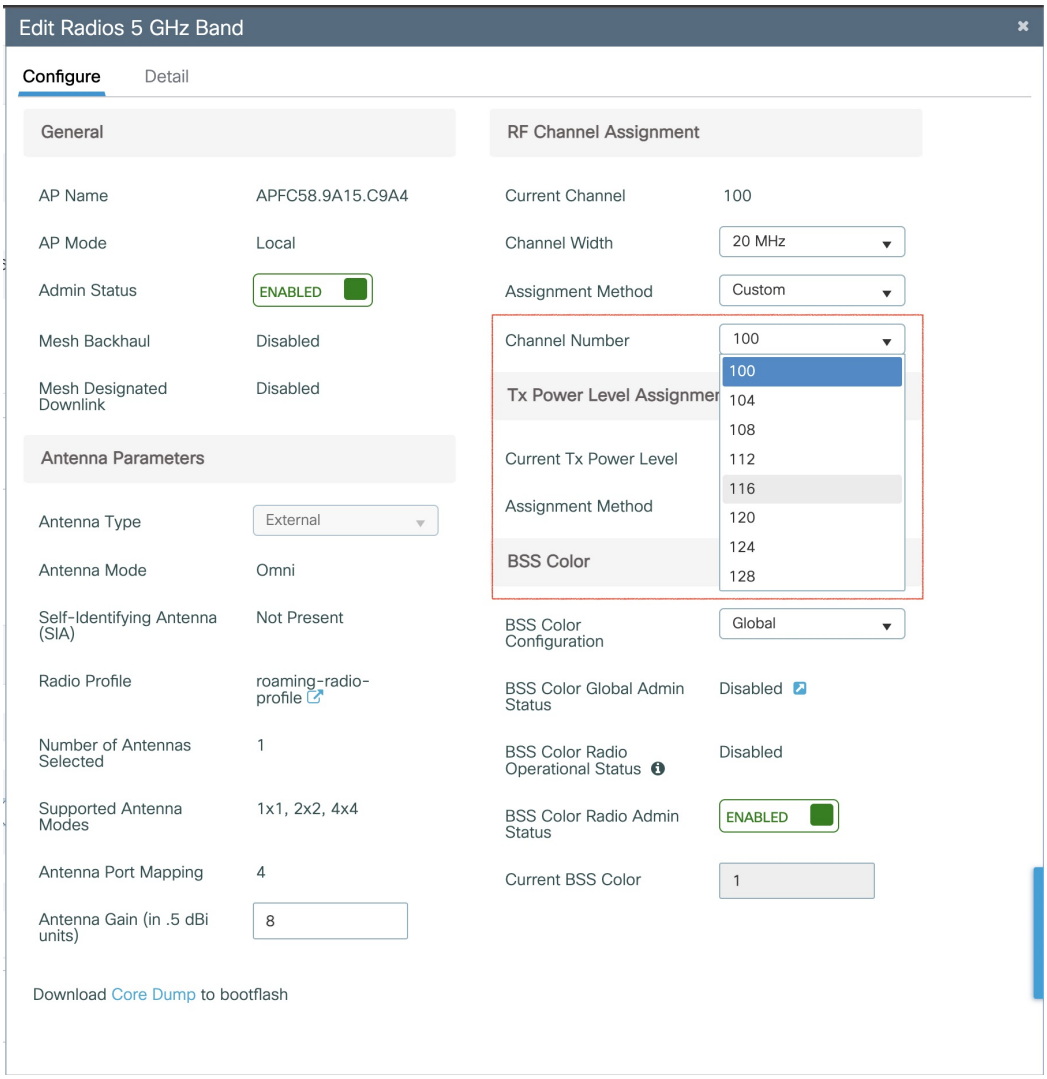
Configuring Indoor Deployment for -E Domain

IW9167EH supports indoor deployment for -E domain.

By default, indoor deployment is disabled, and the 5G radio supports channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140. After factory reset, indoor deployment configuration is reset to default, which is disabled.

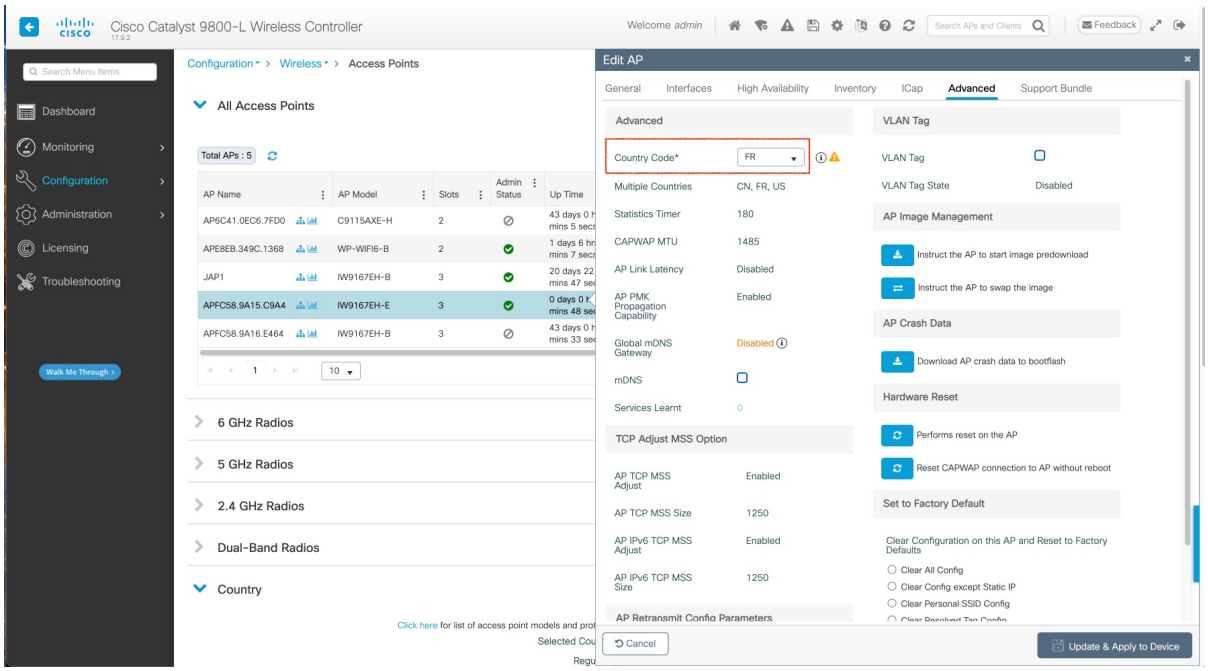
You can check AP mode by using the **show ap name <ap-name> config general | section Indoor** command. In the command output, "Enabled" means AP is in indoor mode, and "Disabled" means AP is in outdoor mode, as shown in the following example.

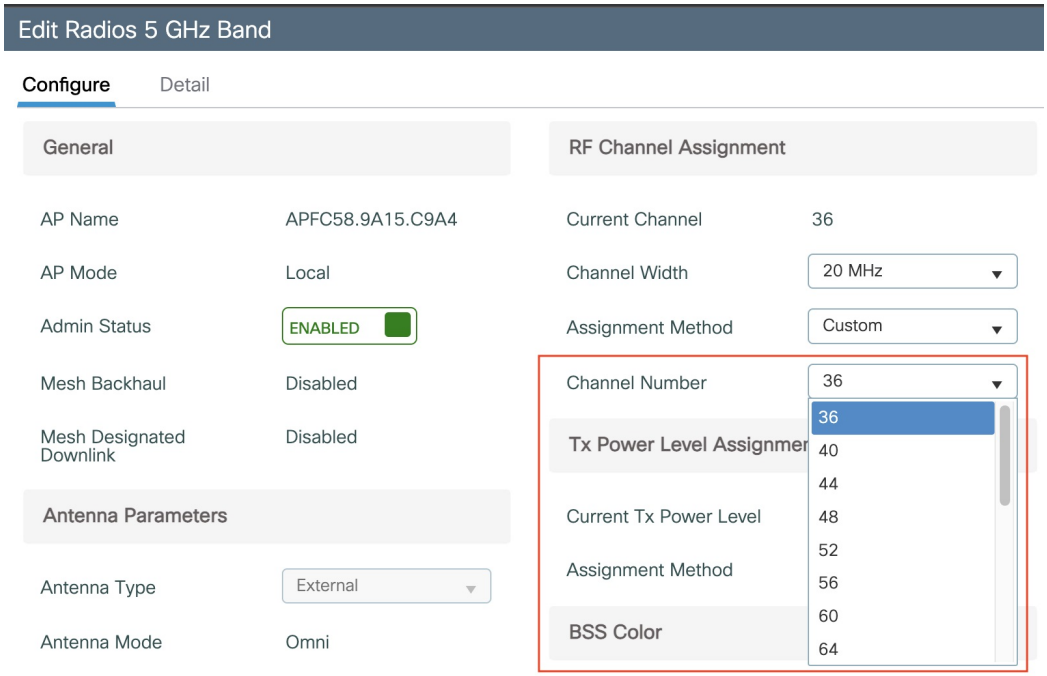
```
#show ap name APFC58.9A15.C9A4 config general | inc Indoor
    AP Indoor Mode                                  : Disabled
```



To configure the AP to indoor mode, use the **ap name** <*ap-name*> **indoor** command from wireless LAN controller. This command triggers an AP rebooting. After AP registers to the wireless LAN controller after rebooting, you need to assign corresponding country code to the AP. When indoor deployment is enabled, 5G radio supports channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Note To disable indoor deployment, use the **ap name** <*ap-name*> **no indoor** command.





Note Channel list extends from U-NII-2c to U-NII-1, U-NII-2a, U-NII-2c (channel 144 is excluded).

802.11ax 1600ns and 3200ns Guard Interval Support

802.11ac has two Guard Interval (GI) options – long GI (800ns) and short GI (400ns). 802.11ax introduces new guard interval options. It has three types of GI – 800ns, 1600ns, and 3200ns. Longer guard intervals provide improved performance in environments with multi-path and delay spread. It improves link reliability for longer-range outdoor deployments and helps to prevent inter-symbol interference in outdoor environments and therefore improve coverage and performance.

The following table compares 802.11ax to the previous two standards.

Table 2: 802.11ax Guard Interval Comparing With Previous Standards

Capabilities	802.11n	802.11ac	802.11ax
Physical Layer (PHY)	High Throughput (HT)	Very High Throughput (VHT)	High-Efficiency (HE)
Guard Interval	800/400 ns	800/400 ns	800/1600/3200 ns

Configuring 802.11ax Long Guard Interval

HE mode guard intervals should be configured in RF profiles.

Procedure

Step 1 Enters global configuration mode.

```
Device#configure terminal
```

Example:

```
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2 Configures RF profile and enters RF profile configuration mode

ap dot11 {**24ghz**|**5ghz**} **rf-profile** *<profile-name>*

Example:

```
Device(config)#ap dot11 24ghz rf-profile 24G-RF-profile
```

Step 3 Configures guard interval for the RF profile.

guard-interval {**GUARD_INTERVAL_1600NS** | **GUARD_INTERVAL_3200NS** | **GUARD_INTERVAL_400NS** | **GUARD_INTERVAL_800NS**}

Example:

```
Device(config-rf-profile)#guard-interval GUARD_INTERVAL_1600NS
```

- GUARD_INTERVAL_1600NS: Set 1600 ns guard interval (only in HE mode)
- GUARD_INTERVAL_3200NS: Set 3200 ns guard interval (only in HE mode)

- GUARD_INTERVAL_400NS: Set 400 ns guard interval (HT VHT mode)
- GUARD_INTERVAL_800NS: Set 800 ns guard interval

Note
Valid guard interval values are 800, 1600, and 3200 ns for HE mode. By default, GI is 800 ns.

Step 4 Exit global configuration mode.

end

Example:

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

Use the following command to verify the configuration on wireless controller:

```
#show ap rf-profile name Demo-24G-RF-profile detail | inc Guard
Guard Interval        : 1600ns
#show ap rf-profile name Demo-5G-RF-profile detail | inc Guard
Guard Interval        : 3200ns
```

Example

1. Define GI in RF profile

```
ap dot11 24ghz rf-profile Demo-24G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_1600NS
no shutdown
ap dot11 5ghz rf-profile Demo-5G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_3200NS
no shutdown
```

2. Associate RF profile to RF tag

```
wireless tag rf Demo-Guard-Interval-RF-tag
24ghz-rf-policy Demo-24G-RF-profile
5ghz-rf-policy Demo-5G-RF-profile
```

3. Associate RF tag to AP

```
ap fc58.9a15.c83c
rf-tag Demo-Guard-Interval-RF-tag
```

GNSS Support

From Cisco IOS XE Dublin 17.11.1, GNSS is supported on IW9167EH. The AP tracks GPS information for devices deployed in the outdoor environment and sends the GNSS information to the wireless controller.

Use the following command to display the GNSS information on the AP:

ap# **show gnss info**.

Use the following commands to display the GPS location of the AP:

controller# **show ap geolocation summary**

controller# **show ap name** <*Cisco AP*> **geolocation detail**

RAP Ethernet Daisy Chain

The RAP Ethernet Daisy Chain feature enhances the existing Ethernet bridging functionality. It forces the bridge AP to stick to the Ethernet link, and block the selecting of wireless link for uplink backhaul. Even the Ethernet link failure happens, the access point will never select a parent over wireless backhaul.

The following figure shows an example of RAP Ethernet Daisy Chain topology. Standalone DC power source is provided to each RAP.

Figure 1: RAP Ethernet Daisy Chain Topology

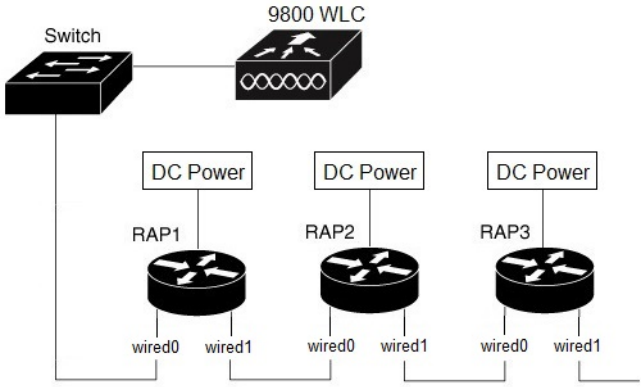


Table 3: Port Mapping

Panel Label	SW Interface
mGig POE-IN port	wired 0
SFP	wired 1

Note The supported SFP module for this feature is the 1000BASE-T rugged SFP (Cisco PID: GLC-T-RGD).

Follow these guidelines when you configure this feature:

- All APs in daisy chain is operating in mesh bridge mode or Flex+Bridge mode with Root AP role. The PoE-IN (wired0) and SFP (wired1) port can be used as uplink port and the PoE-IN (wired0) port has the higher priority than SFP (wired1).
- VLAN transparency should be disabled on all daisy-chained RAPs.
- To enable VLAN support on each root AP:
  - For bridge mode APs, use the **ap name name-of-rap mesh vlan-trunking [native] vlan-id** command to configure a trunk VLAN on the corresponding RAP.
  - For Flex+Bridge APs, you must configure the native VLAN ID under the corresponding flex profile.

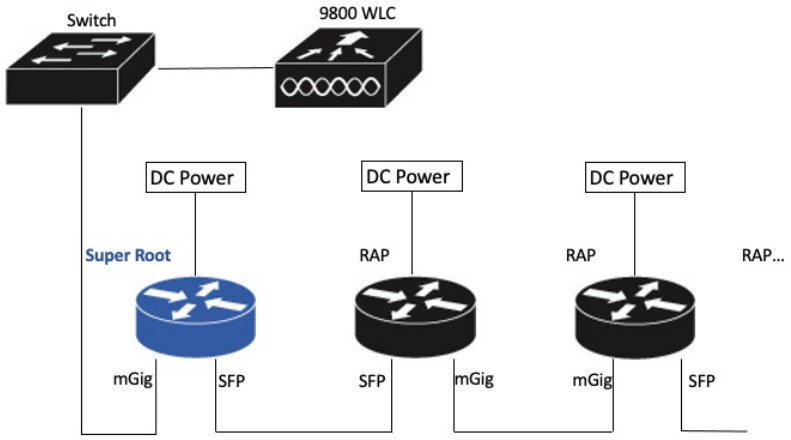
The RAP Ethernet Daisy Chain feature is already supported on Cisco IOS XE Cupertino 17.9.3, while it has the following limitations:

- Primary ethernet port (mGig port) must be used as uplink. In this case, SFP port to SFP port connection is not supported, which impacts network throughput (no 2.5Gbps or 5Gbps copper SFP available when SFP connect to mGig port).
- Reuse an existing command **persistant-ssid** to enable the RAP Ethernet Daisy Chain feature, which is misleading.

In Cisco IOS XE Dublin 17.11.1, the RAP Ethernet Daisy Chain feature is enhanced to support the following functions:

- Wireless Spanning Tree Protocol (WSTP) hello is enabled to support auto root port detection, so that RAP can use any port as its uplink. See the following topology.

Figure 2: RAP Ethernet Daisy Chain With WSTP Topology



- A separate and dedicated command **rap-eth-daisychain** is introduced to enable the feature.

WSTP Overview

Wireless LAN spanning tree protocol (WSTP) organizes a Cisco mesh network into a loop-free spanning tree topology. It quickly configure a mesh network into a stable, loop-free, optimal spanning tree topology, where an optimal topology provides least-cost paths to the primary Ethernet LAN. WSTP Hello messages are used to build the WSTP topology.

The WSTP super root is a single RAP that is elected as the highest level “super” root for the entire WSTP spanning tree. The super root is directly attached to the primary LAN. The super root transmits zero-cost WSTP SR Hello messages on its Ethernet root port to advertise the primary LAN to RAPs.

Comparison with Previous Release

The following table compares the daisy chain features in current release and prior to 17.11:

	Prior to Release 17.11.1	Release 17.11.1
Topology	**Fixed topology** RAP must use its mGig port as uplink in daisy chain topology	**Flexible topology** RAP can use either mGig port or SFP port as uplink in daisy chain topology by enabling WSTP on AP
Feature enablement	**Persistant-ssid** in AP profile [1]	**rap-eth-daisychain** in Mesh profile
Ring Topology	Not supported [2]	Not supported

[1] **Persistant-ssid** is still supported in 17.11, so that daisy chain function will not be impacted after upgrading from previous release to 17.11 with old configuration. But **Persistant-ssid** is not recommended in 17.11, and the new **rap-eth-daisychain** command is recommended.

[2] Supported only on IW6300 access point, by enabling **daisychain-stp-redundancy**. For more information, see the RAP Ethernet Daisy Chain Redundancy for STP Ring Topology section in Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide.

RAP Ethernet Daisy Chain Configuration

This section provides procedures for the RAP Ethernet daisy chain configuration.

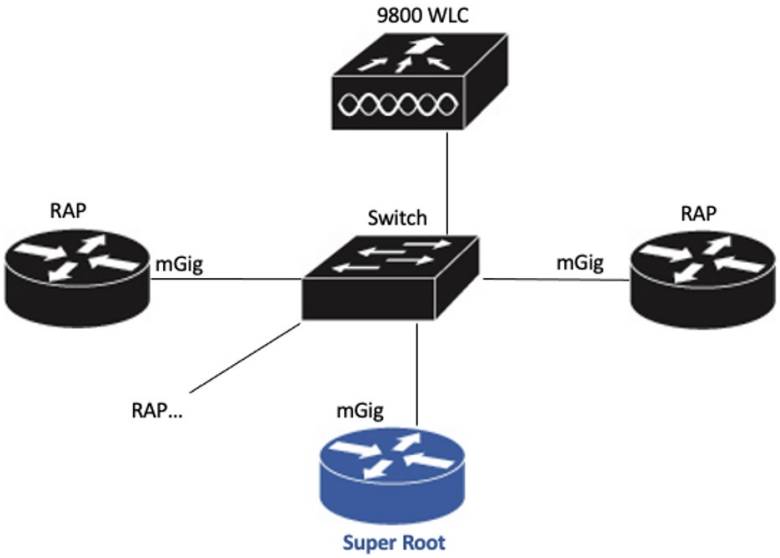
Preconfiguring RAP Ethernet Daisy Chain Before Field Deployment

This section provides the preconfiguration that you should complete in lab before you set up in field deployment.

Procedure

Step 1 Unpack, connect, and power on the AP.

Step 2 Join each AP to controller with mGig port. See the following figure for details.



Step 3 Configure AP to bridge mode and configure AP role to Root AP.

For detailed configuration procedures, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-11/config-guide/b_wl_17_eleven_cg/m_mesh_ewlc.html#task_pnb_bwy_mlb.

Step 4 Configuring RAP Ethernet Daisy Chain.

a) Create mesh profile and enable the Rap Ethernet Daisy chain feature.

See Enabling RAP Ethernet Daisy Chain, on page 16.

b) Attach the profile to all the RAP.

c) Configure one AP as Super Root which should be the first hop to the wireless controller.

See Configuring Super Root, on page 17.

d) Configure primary Ethernet port on the Super Root AP if you use SFP port as uplink.

See Configuring Primary Ethernet Port, on page 18.

Step 5 Enable Ethernet Bridging and Configure Ethernet port.

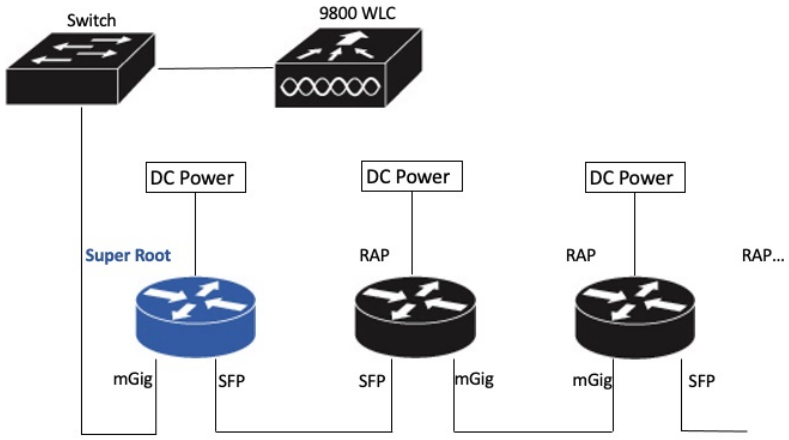
See Configuring Ethernet Bridging and Ethernet Port, on page 18.

a) Enable Ethernet Bridging.

b) Ethernet port configuration on both Port 0 and Port 1, including port mode and vlan. It is recommended to configure port to trunk mode.

Step 6 Verify the behavior in daisy chain topology.

a) Connecting the RAP via wired port one by one.



Note
The RAP which is the first hop from wireless controller should be configured as Super Root, as shown in the above figure.

b) Make sure that RAP of each hop can join the controller.

Note
In field deployment, just repeat Step 6 of this procedure. Make sure you configure the first hop as Super Root.

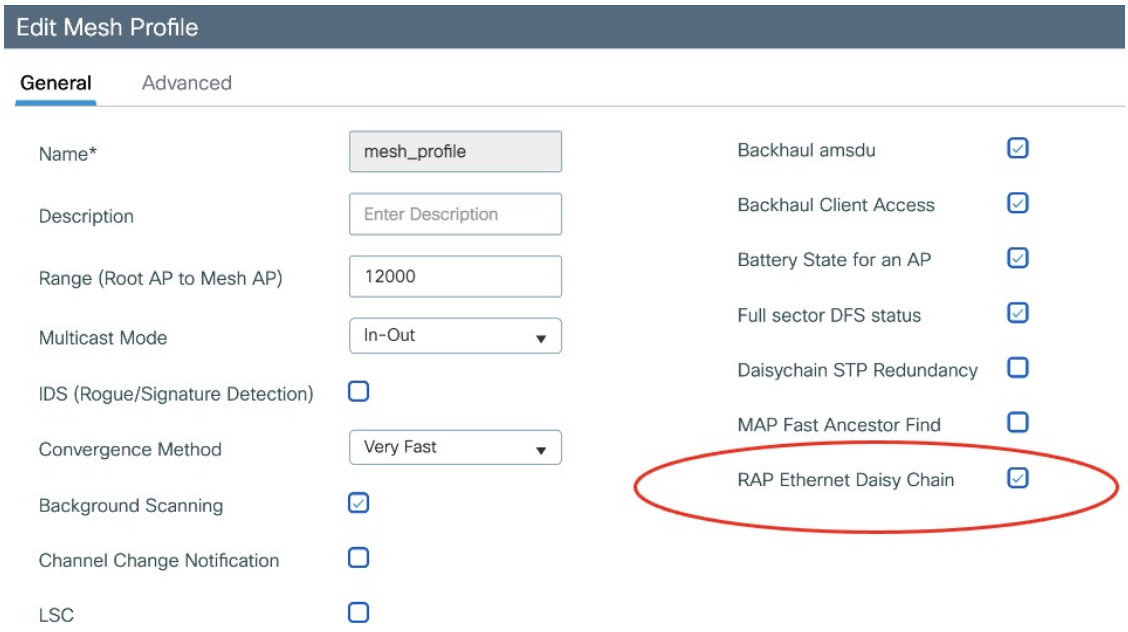
Enabling RAP Ethernet Daisy Chain

To enable RAP Ethernet Daisy Chain feature, use the **rap-eth-daisychain** command, or configure from GUI.

The following example shows enabling the feature from CLI:

```
#configure terminal
(config)#wireless profile mesh default-mesh-profile
(config-wireless-mesh-profile)#ethernet-bridging
(config-wireless-mesh-profile)#rap-ethernet-daisychain
```

The following figure shows enabling the feature from GUI:



To verify the configuration, use the **show wireless profile mesh detailed** command or **show wireless mesh ethernet daisy-chain summary** command from wireless controller, as shown in the following examples:

```
#show wireless profile mesh detailed <profile name>
…
RAP ethernet daisychain       : ENABLED

#show wireless mesh ethernet daisy-chain summary
AP Name      BVI MAC        BGN        Backhaul          Ethernet      STP Red        Super
 Root
-------------------------------------------------------------------------------------------------
APxxxxxx     xxxxxxx       xxxxx       Ethernet0          Up Up          NA
Enabled
```

Or use the **show mesh config** command on AP, as shown in the following example:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Disabled
```

Configuring Super Root

The first RAP which connects to the upstream switch should be configured as super root, which means it's the source of all WSTP hello. Other RAPs only start hello after receiving a hello.

You can configure the super root from wireless controller or from AP.

- From wireless controller, use the **ap name <name> [no] mesh rap-eth-daisychain super-root** command to configure a super root.

  To verify the configuration, use the following command:

  ```
  #show ap name <name> config general
  …
  RAP ethernet daisychain                 : Enabled
  Super Root                              : Enabled
  ```

- On AP, use the **capwap ap mesh wstp super-root** command to configure a super root.

  To verify the configuration, use the following command:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
```

Configuring Primary Ethernet Port

Super root must use its primary Ethernet port to connect to upstream switch. For IW9167EH, the default primary Ethernet port is Ethernet port 0. To manually configure the primary Ethernet port, use the **ap name <name> mesh backhaul ethernet <0/1>** command from wireless controller.

To verify the configuration, use the following command from wireless controller:

```
#show ap name <name> config general
…
AP Primary Ethernet port                        : 1
RAP ethernet daisychain                         : Enabled
Super Root                                      : Disabled
```

Or use the following commands on AP:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
AP Primary ethernet backhaul interface: 1

#show mesh adjacency parent
AdjInfo: Wired Backhaul: 1 [xx:xx:xx:xx:xx:xx]
```

Configuring Ethernet Bridging and Ethernet Port

Configuring Ethernet Bridging (CLI)

The Ethernet port on the MAPs are disabled by default. It can be enabled only by configuring Ethernet bridging on the Root AP and the other respective MAPs. Follow these steps to enable Ethernet bridging on the AP.

Procedure

Step 1 Enters global configuration mode.

```
Device#configure terminal
```

Step 2 Creates a mesh profile.

wireless profile mesh *profile-name*

Example:

```
(config)#wireless profile mesh rap-eth-daisy
```

Step 3 **ethernet-bridging**

Example:

```
(config-wireless-mesh-profile)#ethernet-bridging
```

Connects remote wired networks to each other.

Step 4 Disables VLAN transparency to ensure that the bridge is VLAN aware.

no ethernet-vlan-transparent

Example:

```
(config-wireless-mesh-profile)#no ethernet-vlan-transparent
```

Step 5 Exit global configuration mode.

end

Example:

```
(config-wireless-mesh-profile)#end
```

Example

Use the following command to verify the configuration:

```
#show wireless profile mesh detailed rap-eth-daisy

Mesh Profile Name           : rap-eth-daisy
-------------------------------------
Description                 :
Bridge Group Name           : unconfigured
Strict match BGN            : DISABLED
Amsdu                       : ENABLED
Background Scan             : DISABLED
Channel Change Notification : DISABLED
Backhaul client access      : DISABLED
Ethernet Bridging           : ENABLED
Ethernet Vlan Transparent   : DISABLED
Daisy Chain SP Redundancy   : DISABLED
Full Sector DFS             : ENABLED
```

Configuring Ethernet Bridging (GUI)

Follow these steps to configure Ethernet Bridging from wireless controller GUI:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

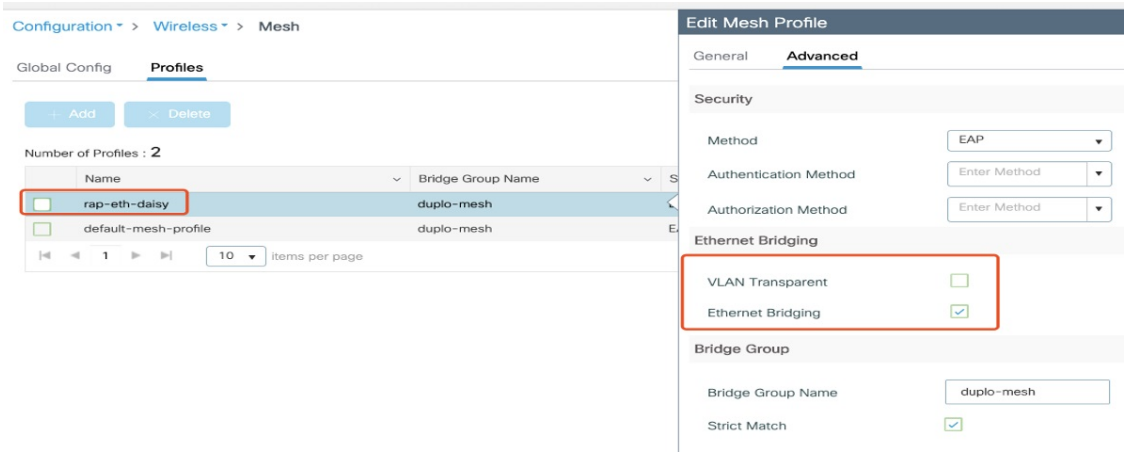
Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, uncheck the **VLAN Transparent** check box to disable VLAN transparency.

Step 5 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 6 Click **Apply to Device**.



Configuring Ethernet Port (CLI)

RAP Ethernet secondary port supports Access mode and Trunk mode. Follow these steps to configure Ethernet port mode.

- Use the following command to configure access mode.

  #**ap name** *ap-name* **mesh ethernet 1 mode access** *Vlan-ID*

- Use the following commands to configure trunk mode. VLAN support must be enabled in advance, and VLAN transparent should be disabled in your mesh profile.
  - Configure a trunk VLAN on the corresponding RAP.

    #**ap name** *ap-name* **mesh vlan-trunking native** *Vlan-ID*

  - Configure the native VLAN for the trunk port.

    #**ap name** *ap-name* **mesh ethernet 1 mode trunk vlan native** *Vlan-ID*

  - Configure the allowed VLANs for the trunk port. Permits VLAN filtering on an ethernet port of any Mesh or Root Access Point. Active only when VLAN transparency is disabled in the mesh profile.

    #**ap name** *ap-name* **mesh ethernet 1 mode trunk allowed** *Vlan-ID*

Configuring Ethernet Port (GUI)

Follow these steps to configure Ethernet port from wireless controller GUI:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

The **All Access Points** section, which lists all the configured APs in the network, is displayed with their corresponding details.

Step 2 Click the configured mesh AP.

The **Edit AP** window is displayed.

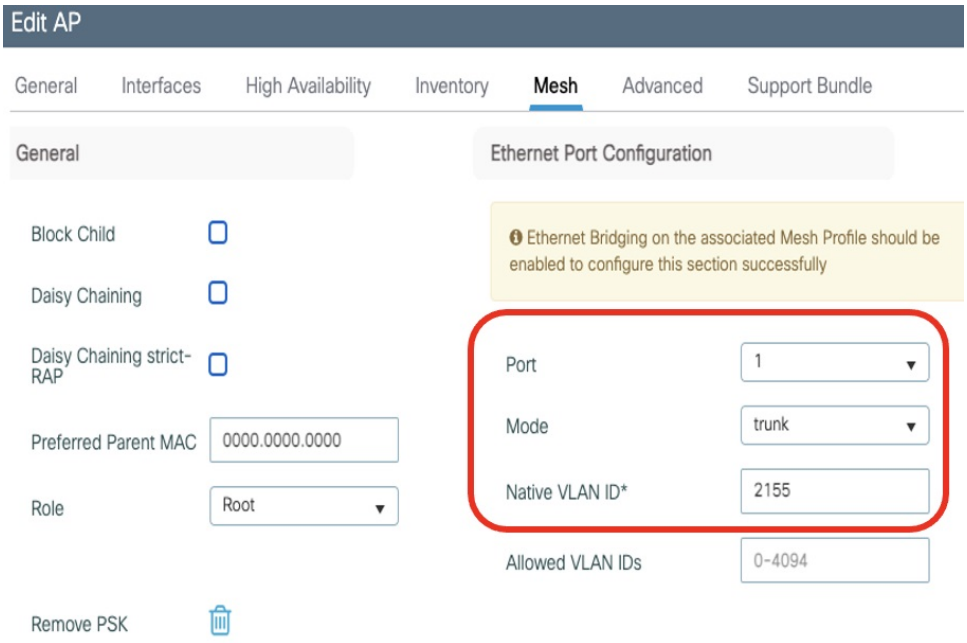
Step 3 Choose the **Mesh** tab.

Step 4 In the **Ethernet Port Configuration** section, from the **Port** drop-down list, choose the port to configure.

Step 5 From the **Mode** drop-down list, choose access mode or trunk mode.

Step 6 In the **Native VLAN ID** field, enter the native VLAN for the trunk port.

Step 7 Click **Update and Apply to Device**.



Show and Debug Command

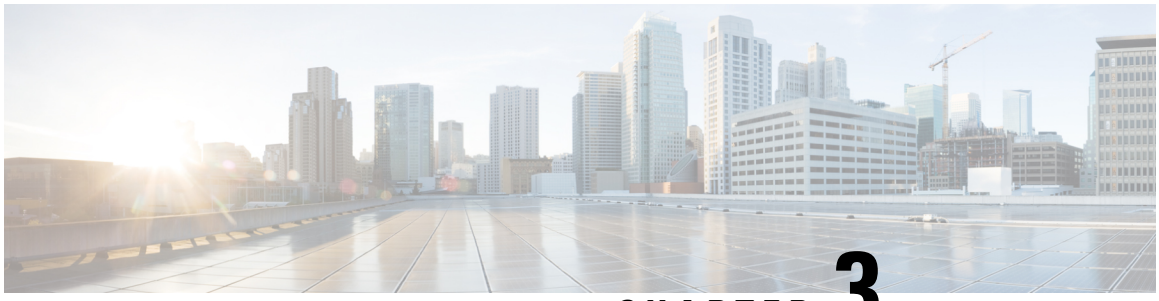
- Use the following command to debug WTP:

```
AP#debug mesh wstp
  error     Mesh wstp error debugs
  events    Mesh wstp events debugs
  packets   Mesh wstp packet debugs
```

```
03:05:24.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:24.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:24.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
03:05:26.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:26.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:26.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
```

- Use the following command to display the WSTP statistics:

```
AP#show mesh stats
WSTP stats:
Attach-Cnt Hello-TX Hello-Rx TCN-TX TCN-RX SR-Chg-Cnt ST-Roam-Cnt
         0       58       58      0      0          0           0
```



CHAPTER 3

Workgroup Bridges

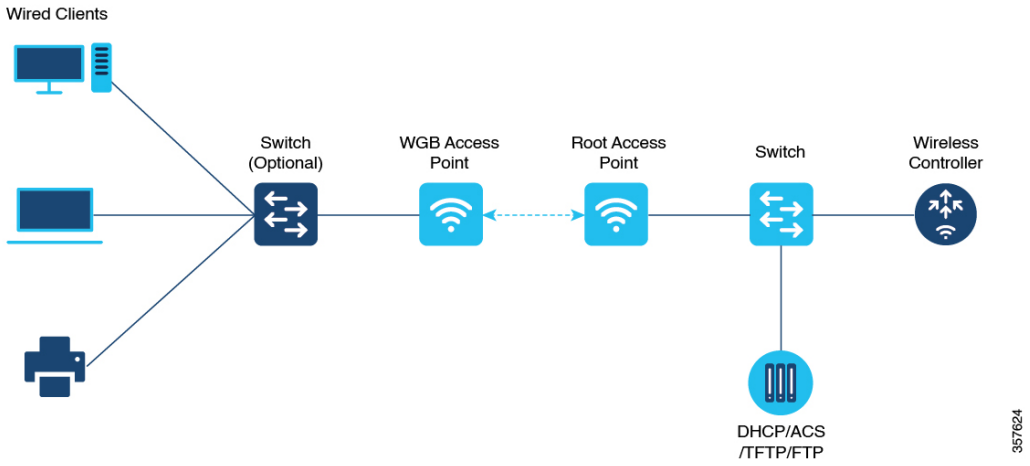
- Overview, on page 23
- Limitations and Restrictions, on page 24
- Configuring Strong Password in Day0, on page 25
- Controller Configuration for WGB, on page 26
- uWGB Image Upgrade, on page 27
- WGB Configuration, on page 28
- uWGB Configuration, on page 37
- Converting Between WGB and uWGB, on page 45
- Fast Roaming With Assistant Second 5G Radio, on page 45
- LED Pattern, on page 46
- Configuring WGB/uWGB Radio Parameters, on page 46
- Assign Country Code to WGB/uWGB With -ROW PID, on page 47
- Indoor Deployment for -E Domain and United Kingdom, on page 47
- Configuring WGB Roaming Parameters, on page 48
- Importing and Exporting WGB Configuration, on page 48
- Verifying the Configuration of WGB and uWGB, on page 49

Overview

A workgroup bridge (WGB) is an Access Point (AP) mode to provide wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the WLC through infrastructure AP using Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

Universal WGB (uWGB) is a complementary mode of WGB feature that acts as a wireless bridge between the wired client connected to uWGB and wireless infrastructure including Cisco and non-Cisco wireless network. One of the wireless interface is used to connect with the access point. The radio MAC is used to associate AP.

Figure 3: Example of a WGB



Starting from Cisco IOS XE Dublin 17.11.1, WGB is supported on the Cisco Catalyst IW9167E Heavy Duty Access Points.

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 universal WGB can associate to a third party access point.
- In a Meraki wireless infrastructure that uses WPA1 security, uWGB do not associate with any SSIDs.
- Speed and duplex are automatically negotiated based on the capabilities of the locally connected endpoint and cannot be manually configured on the AP's wired 0 and wired 1 interfaces.
- 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.
- uWGB mode does not support SSH connecting to itself.
- uWGB mode supports neither TFTP nor SFTP. For software upgrade, you should perform it from WGB mode. For more information, see uWGB Image Upgrade, on page 27.
- uWGB does not support host IP service. Some functions, such as image upgrade via radio uplink and remote management via SSH session, are not supported.
- For IW9167EH WGB/uWGB mode, the **packet retries [N] drop** command does not work in IOS XE Release 17.11.1.
- DFS channels are supported on IW9167EH WGB/uWGB from Release 17.13.1.
- Only Dot11Radio 0 and Dot11Radio 1 interfaces can be used as wireless uplink on IW9167EH WGB/uWGB.
- 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 <0|1> disable

Example:

```
#configure Dot11Radio 0 disable
#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)

Note Ensure that the below configuration order is followed when EAP-TLS security is desired on the WGB:

1. Configure the device username/password, NTP server, hostname, and valid IP address.
2. Create trustpoints and import the certificates using your preferred method.
3. (Optional) Configure the dot1x credentials.
4. Create the EAP profile and map the method, trustpoint name and dot1x credentials (optional).
5. Bind the EAP profile to the SSID profile.
6. Bind the SSID profile to the preferred radio.

Note If you make any modifications to the dot1x credential profile, trustpoint profile, or EAP profile, the changes do not take effect immediately. You must manually re-attach the EAP profile to the SSID profile for the changes to apply.

Use **configure ssid-profile <ssid_prof_name> ssid authentication eap profile <eap_prof_name> key-management <key_type>** command to re-attach the EAP profile to the SSID profile.

```
Device#configure ssid-profile <ssid_prof_name> ssid <ssid name> authentication eap profile
 <eap_prof_name> key-management <key_type>
```

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 0 mode wgb ssid-profile demo-FAST
configure dot11radio 0 enable
```

The following sections provide detailed information about WGB configuration.

Configure IP address

Configure IPv4 address

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

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

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

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

Verify current IP configuration

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

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

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. This configuration allows you to manage the AP through a wired interface without uplink connection.

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

Enable IPv6 auto configuration

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

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



Note

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

Configure IPv6 address using DHCP

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

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

Verify current IP configuration

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

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

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

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

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

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

Deauthenticate WGB wired client

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

```
Device#clear wgb client all
```

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

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

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

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

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

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

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

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

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

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

Configure trustpoint manual enrollment for terminal

Procedure

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

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

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

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

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

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

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

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

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

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

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

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

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

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

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

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

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

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

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

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

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

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

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

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

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

Configure trustpoint auto-enrollment for WGB

Procedure

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

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

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

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

This command fetches the CA certificate from CA server automatically.

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

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

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

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

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

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

Request the digitally signed certificate from the CA server.

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

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

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

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

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

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

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

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

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

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

show crypto pki timers

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

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 35
2. Configuring Radio Interface for Workgroup Bridges, on page 36

Create an SSID profile

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

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

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

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

Configure an SSID profile using PSK authentication

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

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

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

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

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

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

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

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

Configure an SSID profile using Dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**} } command to configure an SSID profile using Dot1x authentication.

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

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

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

Configuring Radio Interface for Workgroup Bridges

- From the available two radio interfaces, before configuring WGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  # **configure dot11radio** *radio-slot-id* **mode root-ap**

  Example

  ```
  # configure dot11radio 0 mode root-ap
  ```

  Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

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

  # **configure dot11radio** *radio-slot-id* **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** *radio-slot-id*{ **enable** | **disable** }

  Example

  ```
  # configure dot11radio 0 disable
  ```

Note Only one radio or slot is allowed to operate in WGB mode.

Configuring WGB/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 <**0**|**1**> **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 0 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 0 enable
```

The following sections provide detailed information about uWGB configuration.

Configure IP address

Configure IPv4 address

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

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

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

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

Verify current IP configuration

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

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

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. This configuration allows you to manage the AP through a wired interface without uplink connection.

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

Enable IPv6 auto configuration

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

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

Note

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

Configure IPv6 address using DHCP

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

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

Verify current IP configuration

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

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

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

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

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

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

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

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

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

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

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

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

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

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

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

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

Configure trustpoint manual enrollment for terminal

Procedure

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

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

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

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

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

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

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

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

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

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

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

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

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

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

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

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

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

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

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

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

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

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

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

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

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

Configure trustpoint auto-enrollment for WGB

Procedure

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

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

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

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

This command fetches the CA certificate from CA server automatically.

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

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

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

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

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

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

Request the digitally signed certificate from the CA server.

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

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

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

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

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

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

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

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

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

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

show crypto pki timers

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

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 35
2. Configuring Radio Interface for uWGB, on page 44

Create an SSID profile

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

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

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

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

Configure an SSID profile using PSK authentication

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

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

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

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

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

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

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

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

Configure an SSID profile using Dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}} command to configure an SSID profile using Dot1x authentication.

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

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

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

Configuring Radio Interface for uWGB

- From the available two radio interfaces, before configuring WGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  # **configure dot11radio** *radio-slot-id* **mode root-ap**

  Example

  ```
  # configure dot11radio 0 mode root-ap
  ```

Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

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

  # **configure dot11radio** *radio-slot-id* **mode uwgb** *uwgb-wired-client-mac-address* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  # **configure dot11radio** *radio-slot-id*{ **enable** | **disable** }

  Example

  ```
  # configure dot11radio 0 disable
  ```

Note After configuring the uplink to the SSID profile, we recommend you to disable and enable the radio for the changes to be active.

Note Only one radio or slot is allowed to operate in uWGB or WGB mode.

Converting Between WGB and uWGB

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

#**configure dot11radio** <**0**|**1**> **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]
```

Fast Roaming With Assistant Second 5G Radio

IW9167EH is equipped with dual 5G radios. Only the first 5G (radio 1) can be used as uplink. With proper configuration, the second 5G can accelarate scanning in roaming.

Note This feature is supported only on WGB mode, and is not supported on uWGB mode.

To enable this feature, use the following command:

```
#configure dot11radio 2 mode scan
```

When the assistant scanning feature is enabled, the second radio keeps scanning configured SSID based on the channel list. By defualt, the channel list contains all supported 5G channels (based on reg domain).

You can also configure the channel list explicitly, 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.

Note It is recommended to make the second 5G radio (antenna port 5-8) have the same antenna installation as the first 5G radio (antenna port 1-4).

Check the scanning table by using the following 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
```

LED Pattern

Two new LED patterns are added to IW9167EH WGB mode:

- When WGB is in disassociated state, the System LED is blinking RED.
- When WGB makes association to parent AP, System LED turns to solid GREEN.

Configuring WGB/uWGB Radio Parameters

Configuring WGB Radio Antenna

Use the following command to configure WGB radio antenna gain. The default antenna gain is 4 dBi.

configure dot11 <**0**|**1**|**2**> **antenna gain** *<1-30>*

Use the following command to configure WGB radio antenna. Default is abcd-antenna.

configure dot11 <**0**|**1**|**2**> **antenna** <**a-antenna**|**ab-antenna**|**abcd-antenna**>

802.11ax 1600ns and 3200ns Guard Interval

802.11ax supports multiple Guard Interval (GI) value: 800ns, 1600ns, and 3200ns. By default, GI is set to 800ns. But you can set it to a different value.

Longer GI is commonly used in outdoor deployment.

```
#configure dot11radio <0|1|2> guard-interval
  1600  Configure 1600 ns guard interval (only in HE mode)
  3200  Configure 3200 ns guard interval (only in HE mode)
  800   Configure 800 ns guard interval
```

Customized Transmit Power

By default, the transmit power of the radio is set to AUTO(0) level.

To manually set the transmit power of the radio use the following command:

```
# configure Dot11Radio <0|1|2> txpower-level <0-8>
```

Assign Country Code to WGB/uWGB With -ROW PID

On day 0, you should assign proper country code to the WGB/uWGB with -ROW reg domain. WGB will load corresponding power table after rebooting.

To assign country code, use the following command:

```
#configure countrycode
  Supported ROW country codes:
  GB VN

  WORD  Select one of above ROW country codes.
```



Note After the ROW country code is configured, if you want to change the configuration to another country, you need to perform a factory reset first, and then configure the new country code.

Indoor Deployment for -E Domain and United Kingdom

IW9167EH supports indoor deployment for -E domain and GB in -ROW domain .

For outdoor mode, the IW9167EH 5G radio supports channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140. When indoor deployment is enabled, 5G radio supports channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

To configure indoor mode, use the **configure wireless indoor-deployment enable** command.

To disable indoor mode, use the **configure wireless indoor-deployment disable** command.

```
#configure wireless indoor-deployment
  disable  Disable indoor deployment
  enable   Enable indoor deployment
```

You can check the indoor or outdoor mode by using the **show controllers Dot11Radio [1|2]** command. In the command output, "-Ei" means the indoor mode is enabled, and "-E" means indoor mode is disabled, as shown in the following examples. The CLI output also shows the supported channels.

```
#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-Ei)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140

#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-E)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
100 104 108 112 116 120 124 128 132 136 140
```

Configuring WGB Roaming Parameters

Use the following command to configure the threshold duration and signal strength to trigger reconnecting. Default value is: period 20s and threshold -70db.

```
# configure wgb mobile period <time> <rssi-threshold>
```

Use the following command to configure beacon miss count to trigger reconnecting. Default value is 10.

```
# config wgb beacon miss-count <count>
```

Use the following command to configure max packet retry to trigger reconnecting. Default value is 64.

```
# configure wgb packet retries <retry-count>
```

Use the following command to configure the static roaming channel:

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> add
```

Use the following command to delete the mobile channel:

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> delete
```

Use the following command to scan all channels:

```
# configure wgb mobile station interface Dot11Radio 1 scan all
```

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 NONINFRINGEMENT 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.

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)

© 2023 Cisco Systems, Inc. All rights reserved.