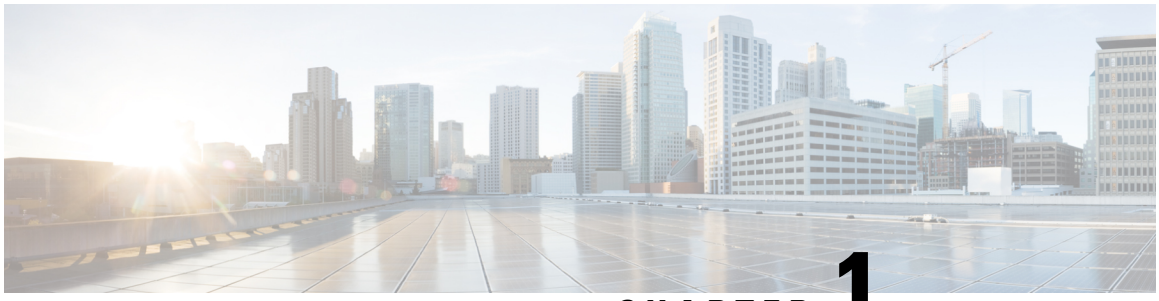
Cisco Wi-Fi Interface Module (WIM) Configuration Guide

First Published: 2023-12-22

Last Modified: 2024-12-11

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

Cisco Wi-Fi Interface Module Overview

This chapter contains the following sections:

Cisco Wi-Fi Interface Module (WIM) Overview

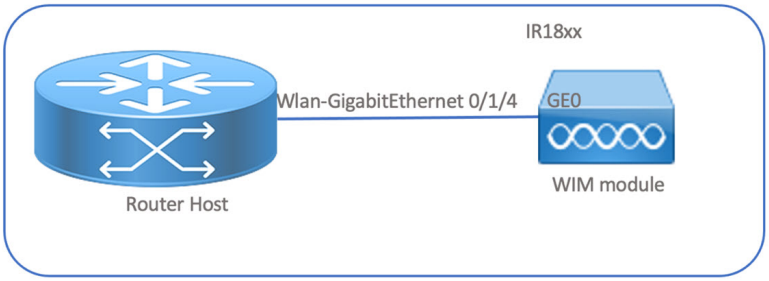
This section provides an overview of the Cisco Wi-Fi Interface Module (WIM). The PID is WP-WIFI6-*x* where x signifies the regulatory domain.

Highlights of the WIM are:

- Pluggable 802.11ax module for Cisco Catalyst IR1800 series
- WiFi-6 (802.11ax), 2x2 MIMO with 2 spatial streams
- Extended Temperature Range
- Field Replaceable Unit (FRU), however does not support OIR (Online Insertion and Removal)
- Versatile RF coverage with external RP-SMA antenna connectors
- Flexible Antenna Port feature support
- Based on the Cisco AP 9105AXI

Hardware Overview

The following diagram shows the control and data path of the WIM. The wired interface is connected to the IR1800 series Switch port (named wlan-GigabitEthernet 0/1/4).



The following graphic shows the front panel of the WIM.

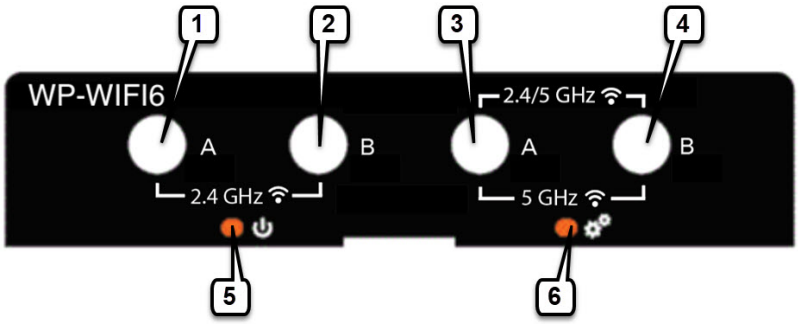


Table 1: WIM Front Panel

Item	Description
1	Disabled when the flexible antenna ports are set to dual-band mode (Default). 2.4 GHz when the flexible antenna ports are set to single-band mode.
2	Disabled when the flexible antenna ports are set to dual-band mode (Default). 2.4 GHz when the flexible antenna ports are set to single-band mode.
3	2.4/5 GHz when the flexible antenna ports are set to dual-band mode (Default). 5 GHz only when the flexible antenna ports are set to single-band mode.
4	2.4/5 GHz when the flexible antenna ports are set to dual-band mode (Default). 5 GHz only when the flexible antenna ports are set to single-band mode.
5	Enable LED
6	Wi-Fi LED

Note Refer to Flexible Antenna Port, on page 69 for additional details.

The following table describes the Enable LED:

LED Status	Description
Off	No Power
Yellow	Power is on, module is not yet functional
Green	Module is fully functional

The following table describes the Wi-Fi LED:

Note LED status information is not applicable to concurrent radio mode. Concurrent radio Root AP + wireless client displays the default LED behavior — Alternate blinking red/green.

LED Status	Status Type	Description
Solid Green	Association Status	Normal operating condition, but no wireless client associated.
Solid Blue	Association Status	• WP-WIFI6 (CAPWAP mode): Infra AP registered with WLC, Client connected to the AP • WP-WIFI6 (UIW WGB): 1 — WGB registered with Infra AP 2 — Both Radio Root AP(second radio) + wireless client connected: NA
Solid Green	Boot Loader Status	Executing Boot Loader
Flashing Green	Boot Loader Status	Boot Loader Error, signing verification error.
Flashing Blue	Operating Status	Software upgrade in progress.
Alternate between Green and Red	Operating Status	Discovery/Join process is in progress.
Cycle through Red-Off-Green-Off-Blue-Off	Access Point operating system error	General warning; insufficient inline power.

Software Overview

The WIM is supported on all four models of the IR1800 series.

Feature support has changed through different versions that run on the WIM software. The IR1800 router software must be running IOS-XE version 17.7.1 or greater. Features available on the WIM depend on what is available on the IOS XE software version of the router, and what mode the WIM is running in. The following table provides details:

Table 2: Feature Matrix

Router IOS XE Release	WIM IOS XE Release	Feature	WIM Software Image Type
17.7.1 and Greater		Three Modes Supported:	
	17.6.1 to 17.10.x	Control And Provisioning of Wireless Access Points (CAPWAP)	ap1g8-k9w8
	17.6.1 to 17.10.x	Cisco Embedded Wireless Controller (EWC)	C9800-AP-iosxe-wlc.bin
	17.6.1 to 17.10.x	Workgroup Bridge (WGB)	ap1g8-k9w8
17.7.1 and Greater	17.11.1 and Greater	Unified Industrial Wireless (UIW) software image type is introduced to support the following: • UIW: WGB mode support move from ap1g8-k9w8 to ap1g8t-k9c1 • UIW: Concurrent Radio support with WGB uplink and Root AP mode • UIW: Concurrent Radio support with dual Root AP mode See more about the UIW image Upgrading 17.9 to 17.11.1 and Greater UIW Image. **Note** WGB mode in ap1g8-k9w8 discontinued starting with 17.11.1.	ap1g8t-k9c1

Feature set is aligned on AP 9105AXI. See the Feature Matrix for Cisco Wireless Access Points.

See the Software Download page for the different WIM software.

Ordering Information

In Cisco Commerce Configuration, Wi-Fi software offers three types of configurations, bundled with different image types. WIM module is shipped with pre-installed image bundle accordingly:

- SW-WPWIFI6-EWC — Default EWC Access Point with C9800-AP-iosxe-wlc.bin + ap1g8-k9w8 image bundle (EWC + CAPWAP)
- SW-WPWIFI6-CW — Default CAPWAP Access Point with ap1g8-k9w8 + ap1g8t-k9c1 image bundle (CAPWAP + UIW WGB)
- SW-WPWIFI6-WGB — Default WGB Access Point with ap1g8-k9w8 + ap1g8t-k9c1 image bundle (CAPWAP + UIW WGB)

The WIM is capable of booting up different images and converting the AP type to support different mode of operation, within the programmed image bundle capability. See the conversion section for details. EWC and WGB are exclusive.

Tip Cisco recommends you map the typical deployment use cases and order Wi-Fi software with pre-installed image bundle.

Related Documentation

There are many different options that can be configured on the Access Point depending on your installation scenario. Other sources of documentation are available here:

Cisco Catalyst 9100 Family of Access Points

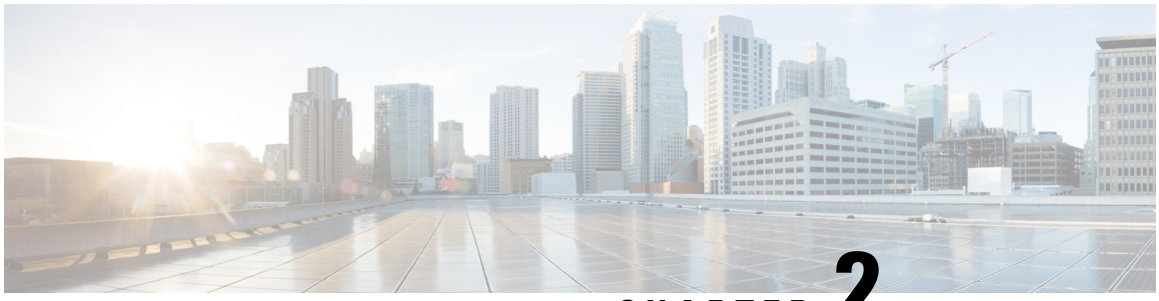
Cisco Wireless Controller Configuration Guide

Cisco Embedded Wireless Controller on Catalyst Access Points FAQ

Cisco Catalyst 9800 Series Configuration Best Practices

Cisco Wave 2 Access Points as Workgroup Bridges

Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide



CHAPTER 2

Wireless Connectivity for IR1800 Router

This chapter describes how to configure the Wi-Fi card to the internal switch interface and module management on the Cisco Catalyst IR1800 Rugged Series router.

This chapter contains the following sections:

IR1800 Configuration Overview

The following are some of the product configuration details:

- The module is fixed to subslot 0/3
- The Wi-Fi interface to communicate with the AP is known as Wl0/1/4
- By default, Wl0/1/4 is in VLAN 1
    - If a DHCP pool is set-up on VLAN1, AP (and associated clients) will get an IP address.
- The module cannot be hot-swapped but is field replaceable.
- The host router must be manually reloaded after the module is inserted.

WIM Module Management Commands

Commands used to view the status of the module from the IOS XE router console are:

- show platform

- show inventory
- show hw-module subslot 0/3 attribute
- show logging

Commands used to configure the module from the IOS XE router console are:

- hw-module subslot 0/3 maintenance enable | disable
- hw-module subslot 0/3 stop | start | reload [force]
- hw-module subslot 0/3 error-recovery password_reset
- hw-module session 0/3

Normal Router Bootup

The Wi-Fi module is powered on as soon as the host router reloads. The Wi-Fi module state turns from 'booting' to 'ok' when the host receives the 'ready' signal from Wi-Fi module. For example:

```
#show platform
Chassis type: IR1835-K9
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         IR1835-K9           ok                    15:25:47
 0/0      IR1835-1x1GE        ok                    15:23:37
 0/1      IR1835-ES-4         ok                    15:23:36
 0/3      WP-WIFI6-B          ok                    00:00:07
R0        IR1835-K9           ok, active            15:25:47
F0        IR1835-K9           ok, active            15:25:47
P0        PWR-12V             ok                    15:23:59
GE-POE    Unknown             ok                    15:23:59

# show logging
Apr  6 18:05:41.992 CST: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/3
Apr  6 18:05:54.886 CST: new extended attributes received from iomd(slot 0 bay 3 board 0)
Apr  6 18:05:55.226 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
```

Deactivating and Reactivating the WIM Module

The WIM module can be removed from the router without being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) before removing it. Use the following commands in EXEC mode:

1. **hw-module subslot 0/3 stop**

Note After deactivating a module using the **hw-module subslot 0/3 stop** command you want to reactivate it, use one of the following commands (in privileged EXEC mode).

2. **hw-module subslot 0/3 start**

3. **hw-module subslot 0/3 reload [force]**

Table 3: hw-module subslot Command Options

Command	Description
reload	Stops and restarts the specified module.
stop	Removes all interfaces from the module and the module is powered off.
start	Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots, and the entire module initialization sequence is executed.

Factory Reset

The user can execute the following command from the host router to factory reset the WIM:

```
Router# hw-module subslot 0/3 error-recovery password_reset
```

The above command sets the WIM to maintenance mode.

Note When you run the **hw-module subslot 0/3 error-recovery password_reset** command, the AP module automatically reloads to restore the configuration settings and enters the maintenance mode. In the maintenance mode, the AP module is on power on mode. Confirm the module configuration reset through the console or web UI. The user will need to issue the **hw-module subslot 0/3 reload force** command to reload the AP and take it out of maintenance mode.

The following sequence shows the factory reset:

```
Router# hw-module subslot 0/3 error-recovery password_reset
```

1. The WIM reloads.
2. The WIM is set to maintenance mode and shows out of service.

```
Router# show platform
Chassis type; IR1835-K9
Slot    Type           State          Insert time (ago)
0       IR1835-K9      ok             00:54:57
0/0     IR1835-1K1GE   ok             00:52:49
0/1     IR1835-ES-4    ok             00:52:46
0/3     WP-WIFI6-B     out of service 00:34:24
R0      IR1835-K9      ok, active     00:54:57
F0      IR1835-K9      ok, active     00:54:57
P0      P-R-12V        ok             00:53:09
GE-P06  Unknown        ok             00:53:09
```

The user should wait approximately 30 seconds, then use the following command:

```
Router# hw-module subslot 0/3 reload force
```

1. The WIM reloads.

2. The WIM quits maintenance mode. Wait for the WIM to turn to the ok state.

```
Router#show platform
Chassis type: IR1835-K9
Slot     Type           State    Insert time (ago)
0        IR1835-K9      ok       00:56:50
0/0      IR1835-1X1GE   ok       00:54:42
0/1      IR1835-ES-4    ok       00:54:39
0/3      WP-WIFI6-B     ok       00:01:36
```

WIM Power Down

The host router will power down the WIM if the WIM reloads 5 times within 20 minutes (for example, a continuous software crash):

```
*Apr  7 10:34:57.412 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr  7 10:36:19.021 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr  7 10:37:59.128 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr  7 10:39:18.942 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr  7 10:41:00.072 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr  7 10:42:15.864 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr  7 10:43:57.507 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr  7 10:45:06.049 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr  7 10:46:46.167 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr  7 10:48:12.425 CST: %SPA_OIR-3-SPA_POWERED_OFF: subslot 0/3: SPA WP-WIFI6 powered off
 after 5 failures within 1200 seconds
*Apr  7 10:48:12.425 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
```

```
Router# show platform
Chassis type: IR1835-K9
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         IR1835-K9           ok                    16:45:16
 0/0      IR1835-1x1GE        ok                    16:43:06
 0/1      IR1835-ES-4         ok                    16:43:05
 0/3      WP-WIFI6-B          out of service        00:00:39
R0        IR1835-K9           ok, active            16:45:16
F0        IR1835-K9           ok, active            16:45:16
P0        PWR-12V             ok                    16:43:28
GE-POE    Unknown             ok                    16:43:28
```

Connect to the WIM through the Router Console

To connect to the WIM, first establish a connection to the host router through the console, ssh protocol, or telnet protocol.

Then re-direct to the Access Point from the host router. See the following example:

```
Router# hw-module session 0/3
Establishing session connect to subslot 0/3
To exit, type ^a^q   <-This sequence to disconnect is Ctrl-a Ctrl-q
picocom v3.1
port is: /dev/ttyWIFI
flowcontrol: none
baudrate is: 9600
parity: none
```

```
databits are: 8
stopbits are: 1
escape is: C-a
local echo is: no
noinit is: no
noreset is: no
hangup is: no
nolock is: yes
send_cmd is: sz -vv
receive_cmd is: rz -vv -E
imap is:
omap is:
emap is: crcrlf,delbs,
logfile is: none
initstring: none
exit_after is: not set
exit is: no
Type [C-a] [C-h] to see available commands
Terminal ready
Username:
```

Disconnect from the Access Point by performing the following:

```
issue ^a^q <-This sequence to disconnect is Ctrl-a Ctrl-q
Username:
Terminating...
Skipping tty reset...
Thanks for using picocom
Router#
```

Default WIM Passwords

The default passwords of the WIM are different depending on the mode and software release.

WIM CAPWAP AP Password

The default login credentials for CAPWAP AP are:

- Username: **Cisco**
- Password: **Cisco**
- Enable Password: **Cisco**

WIM EWC Password

The default credentials for Embedded Wireless Controller are:

- Username: **webui**
- Password: **Cisco**

Note These credentials can be used for over-the-air setup wizard UI access, or SSH/CLI-based day-0 provisioning.

WIM WGB Passwords

The default passwords of WGB mode on the WIM are different depending on the router and WIM software release. More details can be found in the following table:

Table 4:

IOS XE Release for the IR1800	WIM IOS XE Version	Default Passwords
17.9.x and earlier	ALL	Username: **Cisco** Password: **Cisco** Enable Password: **Cisco**
17.10.1 and later	17.7.1 and earlier	Username: **Cisco** Password: **Cisco** Enable Password: **Cisco**
	17.8.1 and later	Username: **Cisco1** Password: **GigabitEth01!** Enable Password: **AppleTree01@**

Determine WIM Image Type

Prior to the IOS XE 17.11.1 AP image, the Wi-Fi module WGB, CAPWAP image (ap1g8) was used for AP type conversions (either switch to CAPWAP mode or WGB mode).

IOS XE 17.11.1 and greater has a new image type, called a Unified Industrial Wireless (UIW) image. This image is called ap1g8t-k9c1. Concurrent radio with WGB and root AP functions will be supported under this new software image.

Determine the Image Type

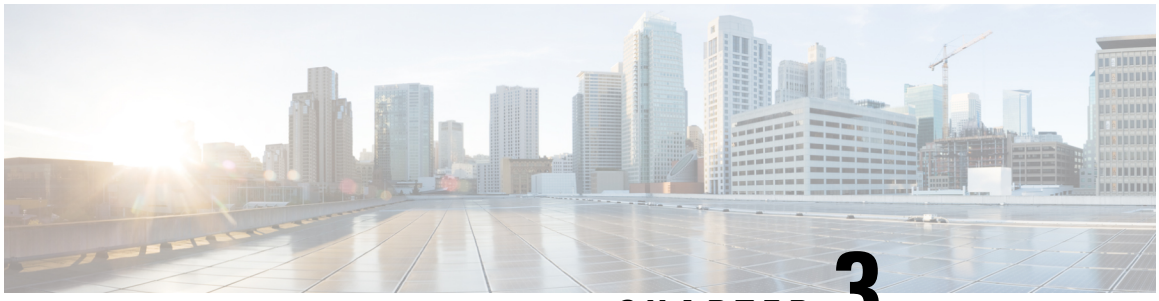
Use the following commands:

Command	Image Type
`AccessPoint#sh version | inc AP` `Cisco AP Software, (ap1g8)`	CAPWAP Image
`AccessPoint#sh version | inc AP` `Cisco AP Software, (ap1g8t), C6, RELEASE SOFTWARE.`	UIW Image
`AccessPoint# show version | include AP` `AP Image type:  EWC-AP IMAGE` `AP Configuration:  NOT ME OR EWC-AP CAPABLE`	EWC Image

To Identify if UIW Image is Installed or Not When Running CAPWAP Image

Use the following commands:

Command	Image Type
AccessPoint#**configure boot mode wgb** Image swapping will restore the device to factory settings. Are you sure to proceed? (y/n) **n** Process Canceled!	UIW Image Installed
AccessPoint#**configure boot mode wgb** Error: Unified client image missed.	No UIW Image Installed



CHAPTER 3

Upgrading the Firmware on the WIM

This chapter contains the following sections:

Prerequisites To Upgrading Firmware

Important Cisco recommends updating your router to IOS XE release 17.11.1 or greater before attempting to upgrade the module firmware.

Check that the following prerequisites exist:

- There must be a network connection between the IR1800 and the AP.
- The IR1800 will need a tftp server enabled for the AP to obtain the images.

IR1800 Configuration

See the following example:

```
Router#sh run int vlan1
Building configuration...

Current configuration : 60 bytes
!
interface Vlan1
ip address 10.10.10.1 255.255.255.0

interface Wl0/1/4
switchport mode access
```

```
switchport access vlan <id>
(In the example above vlan 1 is used)
end
```

Note The vlan id can be any in the range <1-4094>

Configuring the Wi-Fi Module with an IP Address for EWC AP and CAPWAP

Prior to upgrading or converting the Wi-Fi module, it must have an IP address. There are two methods:

1. Configuring the DHCP server on the IR1800 to provide an IP Address for the Wi-Fi Module.

```
IR1800 Router:
Router#sh run | sec vlan1
ip dhcp pool vlan1
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
Router#

WP-WIFI6: Gets ip from IR1800 DHCP server
APBCE7.120C.D748#sh ip in br
Interface          IP-Address    Method   Status   Protocol   Speed    Duplex
wired0             10.10.10.2    DHCP     up       up         1000     full
auxiliary-client   unassigned    unset    up       up         n/a      n/a
apr0v0             n/a           n/a      up       up         n/a      n/a
apr1v0             n/a           n/a      up       up         n/a      n/a
APBCE7.120C.D748#
```

2. Configuring the Wi-Fi Module with a Static IP Address.

   Use the **capwap ap ip** <*ip address*> <*netmask*> <*gateway*> command

```
APBCE7.120C.D748#capwap ap ip 10.10.10.4 255.255.255.0 10.10.10.1
[*12/07/2023 14:01:39.3510] ethernet_port wired0, ip 10.10.10.4, netmask 255.255.255.0,
 gw 10.10.10.1, mtu 1500, bcast 10.10.10.255, dns1 0.0.0.0, is_static true, vid 0,
static_ip_failover false, dhcp_vlan_failover false

APBCE7.120C.D748#ping 10.10.10.1
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds

PING 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.997/1.100/1.221 ms
APBCE7.120C.D748#
```

Configuring the Wi-Fi Module with an IP Address for UIW WGB Mode Running IOS XE 17.13.1 and Greater

Use the **configure ap address ipv4 static** <*ip address*> <*netmask*> <*gateway*> command. For example:

```
APBCE7.120C.D748#configure ap address ipv4 static 10.10.10.2 255.255.255.0 10.10.10.1
```

Note Gateway IP Address is the IR1800 Router SVI IP Address.

Configuring the Wi-Fi Module with an IP Address for UIW WGB Mode Running IOS XE 17.11.x and 17.12.x

With the router running IOS XE 17.11.x and 17.12.x, the single **configure ap address** command mentioned above will appear to work, but does not put a full IP presence on the Wi-Fi module. Additional commands are needed to put a "dummy" ssid configuration on the unit. The following commands are a prerequisite:

```
configure ssid-profile dummy ssid dummy authentication open
configure dot11 1 mode wgb ssid dummy
configure dot11 1 enable
configure dot11 1 disable
```

Note If WGB radio is already configured and enabled, then the static ip address can be added directly and does not require the above prerequisite steps.

Confirm the sub-if is “wbridge.x” as shown in the following example:

```
WGB#sh datapath command /click/br_router/dump_root_subifs
Root_port BG-ID   Hop-Address       Sub-If     VID VAP Trunk  Sec_Trunk Vlan-Trans Learn
Uni-Flood Flood-Age
 57       1       BC:E7:12:0C:E4:0F wbridge.0  0   0   true   true      false      false
true      0
```

Use the **configure ap address ipv4 static** *<ip address> <netmask> <gateway>* command. For example:

```
APBCE7.120C.D748#configure ap address ipv4 static 10.10.10.2 255.255.255.0 10.10.10.1
```

Upgrading the EWC AP Firmware

The firmware can be upgraded from the access point command line interface or the WebUI while in EWC mode.

This section describes the prerequisites for the upgrade, as well as steps to perform the upgrade.

Firmware Upgrade Using The AP Command Line Interface (CLI)

There are two methods to get the image files to the IR1800 bootflash. Secure Copy and TFTP transfer.

Prior to upgrading the image, ensure that vlan1 and the Wi-Fi module have IP addresses set. Check the Prerequisites To Upgrading Firmware, on page 15 section.

Using Secure Copy

1. Copy the image files to the IR1800 bootflash:

Note In order to use secure copy (scp), you must first set up an SSH configuration. See Configuring Secure Shell.

```
Router# copy scp: bootflash:
Address or name of remote host []? 192.168.1.2
Source username [xxxxx]?Enter
Source filename []? /auto/users/<your-image>
Destination filename [<your-image>]?
```

```
This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.

Password: <your-password>
Sending file modes: C0644 208904396 <your-image>
...........
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
```

2. Configure the IR1800 to act as SFTP server.

```
ip scp source-interface Vlan1   ! VLAN interface to be modified based on the configuration
sftp-server bootflash:<your-image>
```

3. Upgrade the AP firmware from AP CLI.

```
#ap-type ewc-ap sftp://10.10.10.1/ap1g8 sftp://10.10.10.1/<your-image>
```

Using TFTP Transfer

1. Copy the image files to the IR1800 bootflash:

```
Router# copy tftp: bootflash:
Address or name of remote host []? 192.168.1.2
Source filename []? /auto/users/<your-image>
Destination filename [<your-image>]?
...........
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
```

2. Configure the IR1800 to act as TFTP server.

```
ip tftp source-interface Vlan1   ! VLAN interface to be modified based on the
configuration
tftp-server bootflash:<your-image>
```

3. Upgrade the AP firmware from AP CLI.

```
#ap-type ewc-ap tftp://10.10.10.1/ap1g8 tftp://10.10.10.1/<your-image>
```

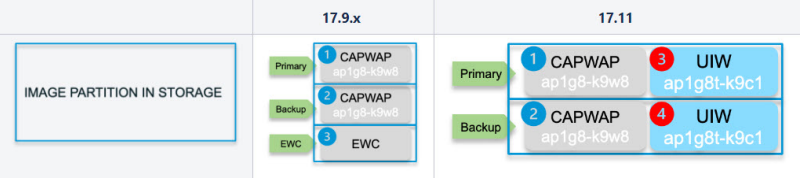
Upgrading 17.9 to 17.11.1 and Greater UIW Image

Starting with IOS XE 17.11.1, the image architecture changed to a new image type. The Unified Industrial Wireless (UIW) image for the WP-WIFI6 module was introduced. The image name is ap1g8t-k9c1. The UIW image will serve the WGB functionality instead of the traditional CAPWAP (ap1g8-k9w8) image.

If the UIW image has never been programed, this chapter will describe the progress to program the new image into the Wi-Fi module's flash partition.

If the UIW image is already installed, skip this chapter.

The two types of image will coexist on the device, and each image will own its independent primary and backup partitions. The following table shows the image partition differences between IOS XE 17.9 and 17.11:



Because the UIW image is supported from IOS XE 17.11 and greater, the device running on an older image that never installed UIW image should follow these steps to start the upgrade:

- Download 17.11 UIW and CAPWAP Image to Host Router
- Upgrade to CAPWAP 17.11 from 17.9
- Install the UIW 17.11 Images

Download 17.11 UIW and CAPWAP Image to Host Router

Download the required images onto your IR1800 prior to beginning the upgrade. You will need the following images:

- 17.11 CAPWAP CCO image
- 17.11 UIW CCO image

Procedure

Step 1 Prior to upgrading the image, ensure that vlan1 and the Wi-Fi module have IP addresses set. Check the Prerequisites To Upgrading Firmware, on page 15 section.

Step 2 Place the images into the *flash:* directory on the IR1800.

a) Configure the tftp blocksize

```
IR1800(config)#ip tftp blocksize 8192
```

b) Download the version 17.11 UIW CCO image

```
IR1800#copy tftp://<TFTP IP>/ap1g8t-k9c1-tar.17.11.0.155.tar flash:
```

c) Download the version 17.11 CAPWAP CCO image

```
Download 17.11 CAPWAP CCO image:
IR1800#copy tftp://<TFTP IP>/ap1g8-k9w8-tar.153-3.JPP.tar flash:
```

Step 3 Configure the IR1800 as TFTP server.

```
IR1800(config)#tftp-server bootflash:ap1g8t-k9c1-tar.17.11.0.155.tar
IR1800(config)#tftp-server bootflash:ap1g8-k9w8-tar.153-3.JPP.tar
```

Upgrade to CAPWAP 17.11 from 17.9

Tip When typing in longer command strings, it is easy to lose your place while lots of console messages are appearing. You can stop the messages from appearing by using the **logging console disable** command.

Procedure

Step 1 Enter the AP_WIFI6 shell. After login to the IR1800 via console/ssh, you can execute the **hw-module session 0/3** command to redirect to the AP_WIFI6 console. Then issue **Ctrl-a Ctrl-q** to return to IR1800.

```
IR1800#hw-module session 0/3
```

Step 2 Make sure the running image is always in CAPWAP mode before starting the upgrade. If running in WorkGroupBridge mode or EWC mode, convert to CAPWAP mode using the **ap-type capwap** command. The ap-type change will cause the Wi-Fi module to reboot. See the following examples:

a) WorkGroupBridge Mode

```
AP_WIFI6#sh running-config | inc Mode
AP Mode       : WorkGroupBridge

AP_WIFI6#ap-type capwap

Note: After rebooting, check the running image is CAPWAP:

APE8EB.349C.14F8#sh running-config | inc Mode
AP Mode       : Local
```

b) EWC Mode

```
WLC#wireless ewc-ap ap shell username <username>

AP_WIFI6#ap-type capwap
AP is the Master AP, system will need a reboot when ap type is changed to CAPWAP
. Do you want to proceed? (y/N)y

Note: After rebooting, check the running image is CAPWAP:
APE8EB.349C.14F8#sh running-config | inc Mode
AP Mode         : Local (or FlexConnect)
```

Step 3 Upgrade the CAPWAP 17.11 image into **primary partition for ap1g8-k9w8** (partition 1). Verify the network is reachable via the PING command, and then upgrade to 17.11 CAPWAP CCO image.

Note
The download and reboot time will take about 6 minutes.

```
AP_WIFI6#ping <IP of IR1800 TFTP> For example:192.168.145.77
AP_WIFI6#logging console disable
AP_WIFI6#archive download-sw /reload tftp://<IP of IR1800>/ap1g8-k9w8-tar.153-3.JPP.tar
Starting download AP image tftp://<IP of IR1800 TFTP>/ap1g8-k9w8-tar.153-3.JPP.tar ...
!This may take a few minutes.
!If longer, please abort command, check network and try again.
      -=O=-    #     #    #   #
```

Step 4 Continue to upgrade the CAPWAP **backup partition for ap1g8-k9w8** (partition 2).

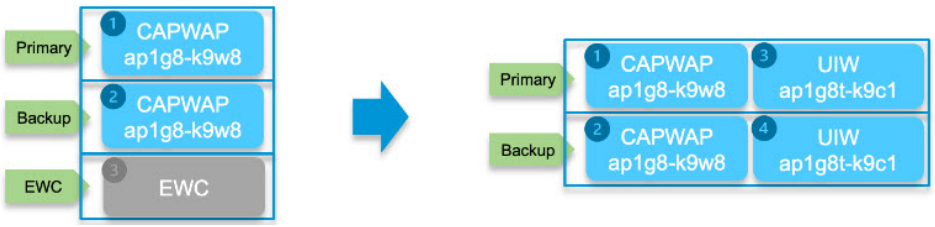
Verify the network is reachable via PING message and then upgrade 17.11 CAPWAP CCO image with the CLI **option no-reload**. For example:

```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP, for example: 192.168.145.77>

AP_WIFI6#logging console disable
AP_WIFI6#archive download-sw /no-reload tftp://<IP of IR1800 TFTP>/ap1g8-k9w8-tar.153-3.JPP.tar
```

Install the UIW 17.11 Images

The following steps describe the procedure to install the primary and backup UIW partition 3 and 4. Both the primary and backup partitions will be updated together, therefore, step 2 only needs to be executed once. Refer to the following image:



Important The EWC image will be permanently removed due to limited storage, and cannot return to EWC mode!

Tip When typing in longer command strings, it is easy to lose your place while lots of console messages are appearing. You can stop the messages from appearing by using the **logging console disable** command.

Procedure

Step 1 Determine whether the UIW image is already programed by using the **config boot mode wgb** command.

a) If the command fails, the UIW image had never programed. Proceed to Step 2.

The following example shows the UIW image is missing:

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8),

AP_WIFI6# config boot mode wgb
Error: Unified client image missed.
```

b) If the command succeeds, the UIW image is already programed. Proceed to Step 4.

The following example shows the UIW image exists:

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8),

AP_WIFI6#config boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

Step 2 Install the UIW 17.11 image with the **no-reload** option in CAPWAP 17.11. Both the primary and backup partitions (3 and 4) will be updated together.

```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP>
AP_WIFI6#logging console disable
AP_WIFI6#archive download-sw /no-reload tftp://<IP of IR1800 TFTP>/ap1g8t-k9c1-tar.17.11.0.155.tar
**************************************************************
Detected field upgrading unified client image by CAPWAP image...
New image will be added into flash, but EWC will be removed.
Are you sure to proceed?(y/n) y
After the upgrade, please remember to switch the mode manually.
Press any key to continue
**************************************************************
```

Note
If the procedure fails with the status **upgrade.sh: INFO: unified client image exists, please try command: config boot mode**, the upgrade failed because the device already has a programed UIW image. Go back to Step 1.

Step 3 Once the UIW is installed on the device, the image type can be changed to WGB by using the **configure boot mode wgb** CLI. This will reboot the Wi-Fi module, load the UIW software, and perform a factory reset.

```
AP_WIFI6#configure boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
Full Factory Reset triggered: clear all files from storage..
```

Step 4 Log in with the default credentials as described in Default WIM Passwords, on page 11.

Step 5 Verify the UIW image type is ap1g8t:

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8t), C6, RELEASE SOFTWARE
AP Running Image     : 17.11.0.155
```

What to do next

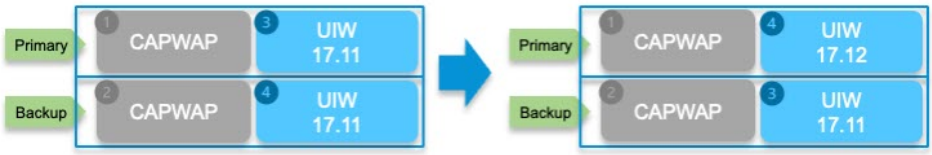
Manually configure the WGB with basic functionality. Refer to Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.11.x for additional information.

Upgrading the UIW Image From IOS XE 17.11 to IOS XE 17.12 and Greater

Before upgrading the UIW image, please make sure the running image type is also UIW (ap1g8t-k9c1). If the device has never installed the UIW image and running the IOS XE 17.11 CAPWAP image, start the upgrade from Step 3 under Install the UIW 17.11 Images, on page 21.

Note The image program only permits upgrading under the same image type, for example, CAPWAP to CAPWAP image and UIW to UIW image. If this is not your current type, change the image type before upgrading.

The primary UIW images will be upgraded to the new version, refer to the following example of 17.12:



Procedure

Step 1 Make sure your device is running the IOS XE release 17.11 UIW image.

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8t), C6, RELEASE SOFTWARE
AP Running Image     : 17.11.0.155
```

Step 2 Set up the TFTP server locally on the IR1800. Refer to Download 17.11 UIW and CAPWAP Image to Host Router, on page 19. Then set a static IP address in the AP_WIFI6.

```
AP_WIFI6#config ssid default ssid default auth open
AP_WIFI6#config dot11 1 mode wgb ssid default
AP_WIFI6#configure ap address ipv4 static <ip> <netmask> <gateway>
AP_WIFI6#reload
```

Step 3 The new UIW image can upgrade the old UIW image directly through the **archive** command, which will replace the image in partition 4 and make it primary.

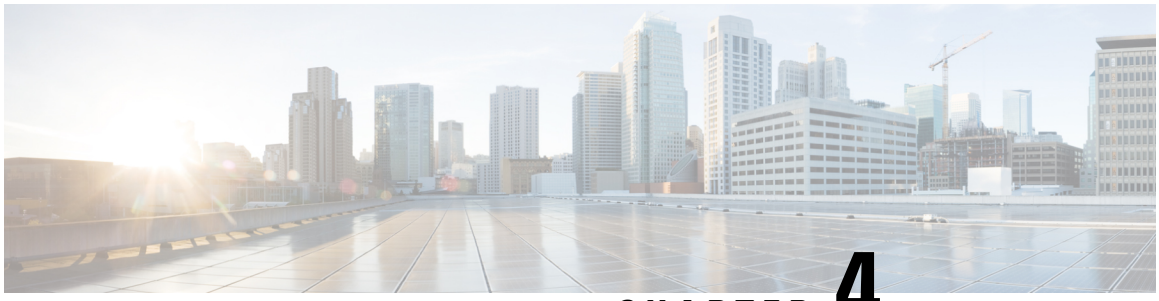
```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP> For example 192.168.145.77
AP_WIFI6#archive download-sw /no-reload tftp://<IP of TFTP>/ap1g8t-k9c1-tar.17.12.1.5.tar
```

Important
The **archive** command can be used to upgrade from any UIW image to another UIW image. There is no version checking.

Downgrading the Image

The WIM WGB mode and new WGB features migrate from CAPWAP image (ap1g8-k9w8) to UIW image (ap1g8t-k9c1) and are supported after.

Important Downgrading to 17.10 and below is **NOT** supported.



CHAPTER 4

Converting Between Modes

This chapter contains the following sections:

Wi-Fi Mode Conversion

When ordering the Wi-Fi pluggable module from Cisco, CAPWAP, EWC and WGB Mode are currently available from Cisco Commerce Workspace (CCW). The best way is considering target deploy mode and order the module with desired software type installed.

The steps described in this section can help you to convert it to another mode wanted, but be aware some mode conversions may not be supported.

Upgrading the firmware on the module and converting the Wi-Fi mode is different depending on whether you are running IOS XE 17.11.1 and greater, or running an IOS XE version earlier than 17.11.1. This section describes both scenarios.

Before you begin a conversion process, it is important to know your WIM image type, Version, and Mode you are running. Refer to the following table:

Image	Supported Mode
EWC image (C9800-AP-iosxe-wlc.bin):	Supports EWC mode
UIW image (ap1g8t-k9c1-tar)	Supports WGB mode from 17.11
CAPWAP image (ap1g8-k9w8-tar)	Supports only CAPWAP mode from 17.11
CAPWAP image (ap1g8-k8w8-tar)	Supports CAPWAP Supports WGB mode (until 17.10)

Before You Begin Conversion

For proper operation of the conversion, please follow these steps to check the current WIM image type, version, and mode before performing any conversion. Refer to the table in Wi-Fi Mode Conversion, on page 25.

Procedure

Step 1 Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured username/password or default password.

Note
For EWC internal access point, to get into the primary AP CLI, type **wireless ewc-ap ap shell username** *[AP-username]* at the controller prompt and login to the internal Access Point shell.

Step 2 Get the current image type on the WIM, using the commands described in Determine WIM Image Type, on page 12. The image type should be one of CAPWAP, UIW, and EWC-AP.

Step 3 Check the current version on the WIM using different a CLI depending on image type as below:

a) For image type CAPWAP and UIW, use the command **show version | inc Running** on WIM to get version.

```
AP#show version | inc Running
AP Running Image     : 17.11.0.100   <-version number 17.11
```

b) For Image type EWC-AP, use the command **show version | inc Cisco IOS XE Software** on WIM to get version.

```
AP#show version | inc Cisco IOS XE Software
Cisco IOS XE Software, Version BLD_V179_xxxx.  <-version number:17.9
```

Step 4 Use the **show running-config | inc AP** command on the WIM to check the mode.

a) For WGB mode, **AP Mode : WorkGroupBridge** should be in the output.

```
APE8EB.349C.1510#show running config | inc AP
AP Name              : APBCE7.120C.D850
AP Mode              : WorkGroupBridge
```

b) For CAPWAP AP mode, **Local** or **FlexConnect** should be in output.

```
APBCE7.120C.D658#show running-config | inc AP
AP Name                     : APBCE7.120C.D658
AP Mode                     : FlexConnect
```

Note After confirming the software version and mode using the above steps, you can proceed to the corresponding conversion section that follows.

Converting Wi-Fi Mode Prior to IOS XE 17.11.1

This section contains the following:

Converting From CAPWAP to EWC Mode

This conversion is required when you have a WIM with a CAPWAP image, and you want to use the WIM to deploy a embedded wireless controller based network. To do this, you must convert the CAPWAP AP to an embedded wireless controller.

To convert a WIM with a CAPWAP image to an embedded wireless controller capable image, follow the conversion steps below to download the controller image. Additional information can be found in the Conversion section of EWC White Paper.

CAPWAP to EWC Mode Procedure

Procedure

Step 1 Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.

Step 2 Check if the EWC image already programed on the WIM using the **show version | include AP** command.

If the EWC image is programed, you see the following output:

```
APE8EB.349C.1510#show version | include AP
Cisco AP Software, (ap1g8),
APE8EB.349C.1510 uptime is 1 days, 13 hours, 07 minutes
AP Running Image     : 17.13.0.98
AP Image type    : EWC-AP IMAGE
```

If the EWC image is not present, you see the following output:

```
APBCE7.120C.DAD8# show version | include AP
AP Image type    : EWC-AP IMAGE
AP Configuration : NOT ME OR EWC-AP CAPABLE
APBCE7.120C.DAD8#
```

Note
If the images are not there, copy them onto the IR1800 bootflash: or on a remote TFTP server using the sub-steps that follow:

a) Download and unzip EWC image file.
b) Copy the required image: **C9800-AP-iosxe-wlc.bin** and respective AP images (**ap1g8**) onto remote TFTP server.
c) Alternatively, to use the IR1800 as a local TFTP server, perform the additional commands below on the IR1800.

Copy the EWC and AP image files onto the IR1800 bootflash: using the following example:

```
IR1800#copy tftp://<TFTP IP>/C9800-AP-iosxe-wlc.bin flash:
IR1800#copy tftp://<TFTP IP>/ap1g8 flash:
```

Configure a TFTP server on the IR1800. For example, AP attached on VLAN100 interface.

```
IR1800# config term
ip tftp source-interface Vlan100
tftp-server bootflash:C9800-AP-iosxe-wlc.bin tftp-server bootflash:ap1g8
```

Step 3 Start the conversion process.

a) If the AP images are available on the WIM, perform the following:

```
AP# ap-type ewc-ap tftp://<image>
```

b) If the AP image is not available by checking the show version output, it means the AP is running a CAPWAP image. To do the conversion, execute the command **ap-type EWC tftp://**<*TFTP Server IP*>**/ap1g8 tftp://**<*TFTP Server IP*>**/C9800-AP-iosxe-wlc.bin**. For example:

```
AP-console#ap-type ewc-ap tftp://192.168.72.11/ap1g8 tftp://192.168.72.11/C9800-AP-iosxe-wlc.bin
Starting download eWLC image tftp://192.168.72.11/C9800-AP-iosxe-wlc.bin
It may take a few minutes. If longer, please abort command, check network and try again.

######################################################################## 100.0%
```

The AP will restart and now the configuration for the new mode must be performed. Refer to the Cisco Embedded Wireless Controller (EWC) section.

Converting From CAPWAP to WGB Mode

Conversion to workgroup bridge (WGB) mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port.

CAPWAP to WGB Mode Procedure

Perform the following steps:

1. Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.
2. Convert the CAPWAP AP to WGB mode on the WIM using the following commands:

```
APBCE7.120C.DAA8#ap-type workgroup-bridge
WGB is a wireless client that serve as nonroot ap for wired clients.
AP is the Master/CAPWAP AP, system will need a reboot when ap type is changed to
 WGB. Do you want to proceed? (y/N): y
```

3. The AP will restart and now the configuration for the new mode must be performed. Refer to the Workgroup Bridge (WGB).

Converting from WGB to CAPWAP Mode

This conversion is required if you want to migrate the WIM from workgroup bridge mode to non-embedded wireless controller network; or if you do not want the APs to participate in the primary AP election process.

WGB to CAPWAP Mode Procedure

1. Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.
2. Convert the CAPWAP AP to WGB mode on the WIM using the **ap-type capwap** command. See the following example:

```
APBCE7.120C.DAA8#ap-type capwap
AP serving in WGB mode, system will reboot when ap type is changed to CAPWAP. Do you
want to proceed? (y/N): y
```

3. WGB will restart and now the configuration of WGB will be cleared. The AP will bootup and start the CAPWAP join process.

Converting From EWC to CAPWAP Mode

If you want to migrate Access Points with Embedded Wireless Controller (EWC) to an appliance or vWLC based deployment. Follow the below steps to perform conversion on WIM by CLI.

For other conversion work-flow and detailed steps, please refer to Conversion section of EWC White Paper.

EWC to CAPWAP Mode Procedure

Procedure

Step 1 Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.

Step 2 To get into the internal AP CLI, type **wireless ewc-ap ap shell username** *[AP-username]* at the controller prompt and login to the internal Access Point shell.

Step 3 Execute the **ap-type capwap** command. This will reload the AP and perform a complete factory reset of both the AP and EWC partition. the Access Point will no longer participate in the primary election process. See the following example:

```
WLC#wireless ewc-ap ap shell username Cisco
The authenticity of host '192.168.129.1 (192.168.129.1)' can't be established.
ECDSA key fingerprint is SHA256:xxxxxx
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.129.1' (ECDSA) to the list of known hosts.
Cisco@192.168.129.1's password:

AP#ap-type capwap
APBCE7.120C.D760#ap-type capwap
AP is the Master AP, system will need a reboot when ap type is changed to CAPWAP.
Do you want to proceed? (y/N) Y
```

Converting Wi-Fi Mode On IOS XE 17.11.1 and Greater

Starting with IOS XE 17.11.1, the WGB mode support for the WP-WIFI6 module was enhanced with the introduction of the UIW image, and corresponding mode conversion now utilizes a new CLI.

The module supports two unique conversion scenarios based on the current image bundle:

- Convert between EWC and CAPWAP AP modes without a programmed UIW image
- Convert between CAPWAP AP and WGB modes with a programmed UIW image

If the WP-WIFI6 module has been programed a UIW image, it will no longer be able to convert to EWC mode.

Converting Between AP and EWC Mode

Refer to the Determine WIM Image Type, on page 12 section to determine whether the WP-WIFI6 module has been programmed with the UIW image.

Note The conversion between AP and EWC mode is only allowed with pre-installed EWC + CAPWAP image bundles.

Follow the same procedure to switch between EWC and AP mode if no UIW image was programed in the WIM before.

- Converting From CAPWAP to EWC Mode
- Converting From EWC to CAPWAP Mode

Converting From CAPWAP to WGB Mode

This conversion is required if you want to convert from CAPWAP AP mode to workgroup bridge mode from IOS XE 17.11 and greater. Please follow the procedure in Install the UIW 17.11 Images, on page 21 first.

Use the **config boot mode wgb** command in the WP-WIFI6 module console.

Conversion Procedure

1. Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.
2. Convert the CAPWAP AP to WGB mode on the WIM using the **config boot mode wgb**. See the following example:

```
AP_WIFI6# config boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

3. The AP will restart and now the configuration for the new mode must be performed. Refer to Workgroup Bridge (WGB) section.

Converting From WGB to CAPWAP Mode

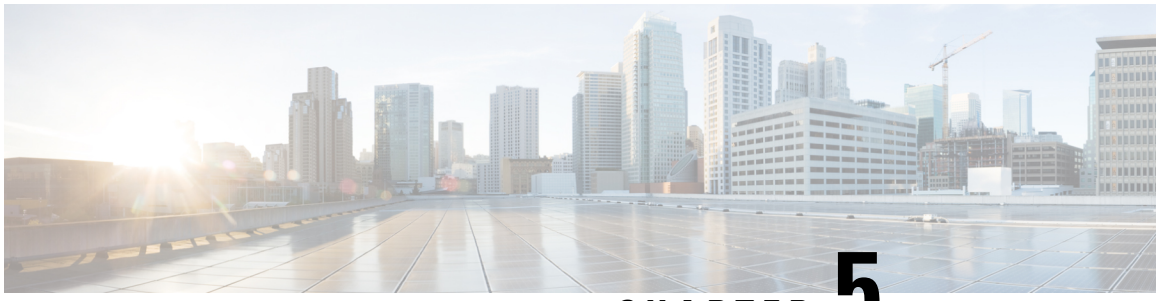
This conversion is required if you want to migrate the APs from a workgroup bridge mode to a wireless controller network.

Conversion Procedure

1. Connect to the WIM through the Router Console, on page 10, login and enter **Enable** to go to privileged execution mode by configured CAPWAP AP username/password or use the Default WIM Passwords, on page 11.
2. Convert the CAPWAP AP to WGB mode on the WIM using the **config boot mode capwap** command. See the following example:

```
AP_WIFI6# config boot mode capwap
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

3. WGB will restart and now the configuration of WGB will be cleared. The AP will bootup and start the CAPWAP join process.



CHAPTER 5

Typical Deployment Modes on the WIM

This chapter contains the following sections:

Typical Deployment Scenarios

Some of the typical scenarios that the WIM can be deployed in are described in this section.

The Wireless Interface Module closely resembles the Cisco Catalyst Series 9105AXI Access Point in functionality.

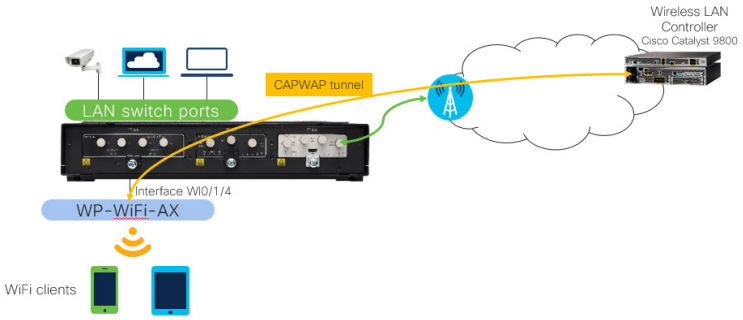
As a wireless insert module of the host router, it can support provision the WIM module work as a wireless access point (CAPWAP AP mode), then the router can serve the Wi-Fi wireless clients get the network access and at the same time the AP function can be managed by a central wireless controller. In case you do not want to deploy a central wireless controller to manage the AP functions, you can deploy the WIM with EWC mode. Then the host router can still serve the wireless clients network access and at the same time manage the AP function by the local EWC controller.

If you provision the WIM to work in WGB mode, then can configure the host router to use the Wi-Fi wireless connection as a candidate backhaul link. With the 17.11.1 UIW software enhancement, it will give the host router capability to use one radio to serve WGB backhaul, and another radio serve the wireless clients access.

Control And Provisioning of Wireless Access Points (CAPWAP)

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. While WP-WIFI6 module working as an access point, it connected directly to a wired LAN provides a connection point for wireless users.

The image used for CAPWAP mode is ap1g8-k9w8.



Prerequisites for Configuring CAPWAP Access Point Configuration on the IR1800

Access points must be discovered by a controller before they can become an active part of the network. CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.

The following section shows the basic configuration of DHCP server and SVI interface on the router for WIM CAPWAP AP to communicate with controller. For modifying additional NAT, DNS and other routing configuration please refer to the IR1800 configuration guide.

Note If the AP is already in CAPWAP mode, the AP does not reboot. If the AP is in EWC or WGB mode, the AP reboots after which the mode is changed to CAPWAP.

Configuring CAPWAP Access Point Configuration on the IR1800 Procedure

Use the following steps:

Step	Command or Action	Purpose
Step 1	**ip dhcp pool** *name* **network** *ip address subnet mask* **default-router** *ip address* **dns-server** *ip address* **option 43 hex** <*value*> **Example**: `Router(config)#ip dhcp pool wireless` `Router(dhcp-config)#network 10.10.10.0 255.255.255.0` `Router(dhcp-config)#default-router 10.10.10.1` `Router(dhcp-config)#dns-server 192.0.2.1` `Router(dhcp-config)#option 43 hex f108c0a80a05c0a80a14`	Create a DHCP server address pool which IP address will be used for Switched Virtual Interface (SVI) Refer Step 4. Assign default gateway and DNS server address for the pool.

Step	Command or Action	Purpose
Step 2	**interface GigabitEthernet** *slot/subslot/port* **ip address dhcp** **ip nat outside** **Example**: `Router(config)#interface GigabitEthernet 0/0/0` `Router(config-if)#ip address dhcp` `Router(config-if)#ip nat outside`	Configure router Uplink WAN port IP address and use NAT command to connect the interface with the outside network.
Step 3	**interface Wlan-GigabitEthernet** *slot/subslot/port* **switchport mode trunk** **switchport trunk native vlan** *number* **Example**: `Router(config)#interface Wlan-GigabitEthernet 0/1/4` `Router(config-if)#switchport mode trunk` `Router(config-if)#switchport trunk native vlan 10`	Configure switchport mode and native VLAN of WIM internal switch interface. Native VLAN should be AP management VLAN.
Step 4	**interface vlan** *number* **description** <*name*> **ip address** *ip-address subnet_mask* **ip nat inside** **Example**: `Router(config)#interface vlan 10` `Router(config-if)#description Wireless` `Router(config-if)#ip address 10.10.10.1 255.255.255.0` `Router(config)#ip nat inside`	Create a Switched Virtual Interface (SVI), assigned IP address from DHCP pool and connect the interface to the inside network.
Step 5	**ip route 10.10.10.10 10.10.10.10** *default gateway ip-address* **Example**: `Router(config)#ip route 10.10.10.10 10.10.10.10 192.0.2.1`	Direct all the traffic to the default gateway of the router
Step 6	**ip nat inside source list** *number* **interface GigabitEthernet** *slot/subslot/port* **overload** **ip access-list standard** *number* *number* **permit** *ip address wildcard mask* **Example**: `Router(config)#ip nat inside source list 10 interface GigabitEthernet 0/0/0 overload` `Router(config)#ip access-list standard 10` `Router(config)#10 permit 10.10.10.0 0.0.0.255`	Establish dynamic source translation, specifying the access list. Create ACL to permit or deny traffic.

Configuring and Deploying the Access Point

When the Wireless Interface Module is running in CAPWAP mode, once an IP address is set on the module, it communicates and is managed through its WLC, such as a Cisco 9800 series. The configuration process takes place on the controller.

Further information on CAPWAP and Cisco Wireless LAN can be found in the following sources:

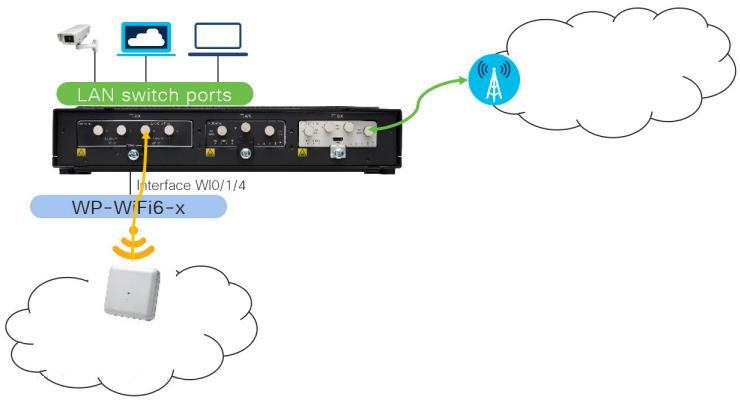
- Configure DHCP OPTION 43 for Lightweight Access Points Guide
- Cisco Catalyst 9800 Series Configuration Best Practices
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x

Workgroup Bridge (WGB)

The Workgroup Bridge (WGB) scenario offers:

- Low Cost High-Speed Wi-Fi Uplink
- Only one radio is allowed to operate in uWGB or WGB mode
- WGB supports up to 20 wired clients
- uWGB supports a single client MAC address, for example, VLAN10 interface in a configuration where Wl0/1/4 is a routed interface for Wi-Fi as backhaul link

Important WGB mode on the IR1800 is only recommended for stationary deployments.



Workgroup Bridge mode is a special mode used for Data Offloading Over Infrastructure Wi-Fi. The WIM running in this mode works like a wireless station. It is normally used to bridge wired clients (connected to it via its Gigabit port) to a wireless infrastructure.

An example usage scenario is to provide Wi-Fi backhaul for cameras and other devices which may be connected to a wired Ethernet port on the IR1800. Note that WGB mode assumes that the wireless infrastructure is from Cisco.

From Cisco IOS-XE Release 17.8.1, the Universal WGB mode is supported for WIM.

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.

For more information on WGB and uWGB configuration, see the following:

Cisco Wave 2 Access Points as Workgroup Bridges

Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide

Prerequisites for WGB configuration on the IR1800

The following section shows the basic configuration of the IR1800 to bridge wired client with Infrastructure Wi-Fi traffic. For NAT, ACL and other specific configuration, please refer to the IR1800 configuration guide.

Step	Command or Action	Purpose
Step 1	**vlan** *number-number* **Example**: `Router(config)#vlan 2001-2002`	Create specific VLAN for different wired client traffic VLAN. VLAN 2001 for wired client Printer. VLAN 2002 for video camera.
Step 2	**interface Wlan-GigabitEthernet** *slot/subslot/port* **switchport mode trunk** **switchport trunk allowed vlan** *number* **Example**: `Router(config)#interface Wlan-GigabitEthernet 0/1/4` `Router(config-if)#switchport mode trunk` `Router(config-if)#switchport trunk allowed vlan 2001-2002`	Use the **Wlan-GigabitEthernet** command to connect the Wi-Fi card of the internal switch interface. Configure switchport mode and allowed wired client traffic VLAN passthrough.

Step	Command or Action	Purpose
Step 3	**interface GigabitEthernet** *slot/subslot/port* **description** *name* **switchport mode trunk** **switchport trunk native vlan** *number* **interface GigabitEthernet** *slot/subslot/port* **description** *name* **switchport mode access** **switchport access vlan** *number* **Example**: `Router(config)#interface GigabitEthernet 0/1/0` `Router(config-if)#description Printer` `Router(config-if)#switchport mode trunk` `Router(config-if)#switchport trunk native vlan 2001` `Router(config)#interface GigabitEthernet 0/1/1` `Router(config-if)#description Camera` `Router(config-if)#switchport mode access` `Router(config-if)#switchport access vlan 2002`	Configure switchport mode and VLAN for each wired client connected port.

Configuring and Deploying WGB

The following section shows the minimum WGB CLI configuration needed on the WP-WIFI6 module. Please follow the guidance in Converting Between Modes, on page 25 to bootup WP-WIFI6 module as WGB first. For further WGB configuration please refer to Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide.

Procedure

Step 1 Configure an SSID profile.

Example:

```
WIM-WGB# configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

Step 2 Configure radio interface to WGB mode and map the SSID profile. Select authentication as dictated by the wireless infrastructure.

Example:

```
WIM-WGB# configure dot11Radio 1 mode wgb ssid-profile Test
WIM-WGB# configure dot11Radio 1 encryption mode ciphers aes-ccm
WIM-WGB# configure dot11Radio 1 enable
```

Step 3 Configure unused radio as root-AP and off. At the time of this writing, single radio is used by WGB.

Example:

```
WIM-WGB# configure dot11Radio 0 mode root-ap
WIM-WGB# configure dot11Radio 0 disable
WIM-WGB# configure wgb antenna band mode single
```

Step 4 Check WGB basic configuration by using the **show configuration** on the WIM.

Example:

```
WIM-WGB# show configuration
AP Name : WIM-WGB
AP Mode : WorkGroupBridge
SSH State : Enabled
AP Username : Cisco1
Syslog Host : 0.0.0.0

Radio and WLAN-Profile mapping:-
===================================
Radio ID Radio Mode SSID-Profile SSID Authentication
-------------------------------------------------------------------------------------------------------------
1 WGB Test Free PSK

Radio configurations:-
==============================
Radio Id : 0
Admin state : DISABLED
Mode : RootAP
Radio Id : 1
Admin state : ENABLED
Mode : WGB

WGB specific configuration:-
==================================
WGB Radio Id : 1
Mode State : Enable
SSID Profile : Test

Antenna Band Mode : Single
```

Step 5 Check WGB association **Uplink State** and **RSSI** using the **show wgb dot11 associations** command on the WIM.

Example:

```
WIM-WGB# show wgb dot11 associations

Uplink Radio ID : 1
Uplink Radio MAC : BC:E7:12:0C:FF:6F
SSID Name : Free
Connected Duration : 0 hours, 0 minutes, 5 seconds
Parent AP Name : AP60E6.F0D4.4E34
Parent AP MAC : 60:E6:F0:D4:4A:6A
Uplink State : CONNECTED
Auth Type : PSK
Key management Type : WPA2
Dot11 type : 11ax
Channel : 124
Bandwidth : 40 MHz
Current Datarate : 6 Mbps
Max Datarate : 573 Mbps
RSSI : 40
IP : 192.168.56.107/24
Default Gateway : 192.168.56.1
DNS Server1 : 192.168.71.2
Domain : iottest.local
IPV6 : ::/128
Assoc timeout : 5000 Msec
```

```
Auth timeout : 5000 Msec
Dhcp timeout : 60 Sec
Country-code : US
```

Step 6 Check WGB **wired client mac**, **IP**, and **vlan id** in the bridge table by using the **show wgb bridge** command on the WIM.

Example:

```
WIM-WGB# show wgb bridge
***Client ip table entries***
mac vap port vlan_id seen_ip confirm_ago fast_brg
60:E6:F0:D4:4A:6A 0 wbridge1 0 0.0.0.0 24.082000 true
E4:62:C4:49:96:F4 0 wired0 2256 192.168.56.108 6.668000 true
```

Configuring and Deploying uWGB

The following section shows the minimum uWGB configuration needed on the WP-WIFI6 module. Please follow the procedure listed in Converting Between Modes, on page 25 to bootup WP-WIFI6 module as WGB first. For further uWGB configuration please refer to Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide.

Check the **show configuration** once opening session to 0/3. Review the following:

- 2.4GHz radio (dot11 radio 0) is turned off
- The 5GHz radio (dot11 radio 1) is set-up to attach to a 3rd party AP

Note Either 2.4 GHz or 5 GHz can be configured to uWGB mode.

The following are the high level steps to configure uWGB to connect to a 3rd party app.

Procedure

Step 1 Configure an SSID profile.

Example:

```
configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

Step 2 Configure the radio interface to uWGB mode and map the SSID profile. Select authentication as dictated by the wireless infrastructure. In the following example, c44d.849b.0a8c is the uWGB wired client device mac address which gets its address from the infra.

Example:

```
configure dot11radio 1 mode uwgb c44d.849b.0a8c ssid-profile Test
configure dot11radio 1 encryption mode ciphers aes-ccm
configure dot11radio 1 enable
```

Step 3 Configure the unused radio as root-AP and off. At the time of this writing, single radio is used by uWGB.

Example:

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

uWGB Configuration Examples

The following are examples of a uWGB configuration.

```
APBCE7.120C.DAA8#show config
AP Name             : APBCE7.120C.DAA8
AP Mode             : WorkGroupBridge
CDP State           : Enabled
Watchdog monitoring : Enabled
SSH State           : Disabled
AP Username         : Cisco
Session Timeout     : 300

Radio and WLAN-Profile mapping:
===================================
Radio ID   Radio Mode   SSID-Profile   SSID   Authentication
1          UWGB         Test           Free   PSK

Radio Configuration:
Radio Id           : 0
  Admin state      : DISABLED
  Mode             : RootAP
  Beacon Period    : 100 mSec
Radio Id           : 1
  Admin state      : ENABLED
  Mode             : UWGB
  Uclient mac      : C44D.849B.0A8C
  Current state    : WGB
  UClient timeout  : 0 Sec
  Dot11 type       : 11ax
  Encryption mode  : AES128

WGB specific configuration:
===================================
WGB Radio Id         : NA
  Mode State         : NA
  SSID Profile       : NA
UWGB Radio Id        : 1
  Mode Enable        : Enable
  SSID Profile       : Test
  Uclient MAC Address: C44D.849B.0A8C
```

Check attached wired device on the IR1800:

```
#show wgb bridge
***Client ip table entries***
mac vap                 port  vlan_id   seen_ip       confirm_ago  fast_brg
10:DD:B1:CE:B2:E6       0     wired0    192.168.10.25 0.016000      true
```

Check the association. In the following example, the Client must be attached to see uWGB status. If there is no traffic from wired client or vice-versa, it falls back to WGB.

```
#show wgb dot11 associations
Uplink Radio ID       : 1
Uplink Radio MAC      : BC:E7:12:0C:F1:CF
SSID Name             : Free
Parent AP MAC         : 08:02:8E:8D:52:9A
Uplink State          : CONNECTED
Auth Type             : PSK
```

```
Key management Type    : WPA2
Uclient mac            : C4:4D:84:9B:0A:8C
Current state          : UWGB
Uclient timeout        : 60 Sec
Dot11 type             : 11ac
Channel                : 36
Bandwidth              : 80 MHz
Current Datarate       : 433 Mbps
Max Datarate           : 1200 Mbps
RSSI                   : 53
IP                     : 0.0.0.0
IPV6                   : ::/128
Assoc timeout          : 5000 Msec
Auth timeout           : 5000 Msec
Dhcp timeout           : 60 Sec
```

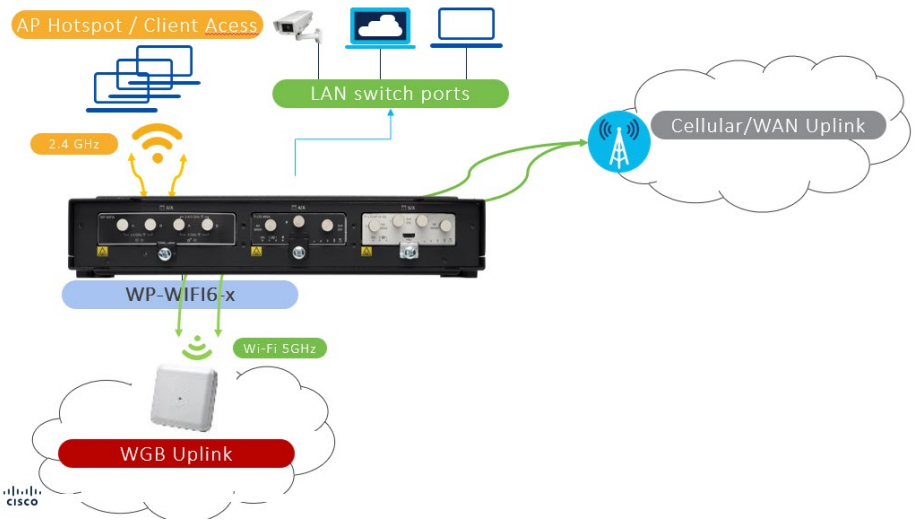
Concurrent Radio Support with uWGB or WGB Uplink and Root AP Modes

Cisco IOS XE 17.11.1 introduced concurrent radio support with WGB uplink and Root AP mode feature in the new Unified Industrial Wireless image(ap1g8t-k9c1). It allows configuring one radio as WGB uplink (2.4G or 5G) and the second radio as WGB Root AP mode for local wireless client serving (also known as hotspot Wi-Fi) independently, or both radios could be configured as Root AP mode.

From 17.14.1 onwards, the WiFi module supports concurrent radio operation, with one radio functioning as an uplink backhaul in uWGB mode and the other as a Root AP radio.

This feature enables to bridge the wireless client traffic with different WLAN-VLAN mapping to internal ethernet port. IR1800 router will route and forward these wireless client traffic to different uplink depends on the use case and configuration.

See the following figure for a typical use case:



Traffic flow for the wireless clients connected to root ap radio (second radio):

- Client serving radio traffic is not bridged directly to wireless backhaul

- Wireless client traffic is bridged to the integrated router via internal gig0
- Wireless clients get their ip address through DHCP from Router's internal DHCP server
- Router can then be configured with NAT/ip route to route the packets from wireless clients to infrastructure network and then forward the traffic accordingly (based on the use-case)

Concurrent radio supported scenarios and maximum wireless client limit:

The wireless clients associated and authenticated at the Wi-Fi module client serving radio shall not be updated to infra-Root AP as these are locally serving clients.

1. First Scenario
   - Radio 0 — WGB mode configured; Status: Disabled (uplink radio Disabled).
   - Radio 1 — Root AP mode; Max 100 wireless clients could be connected.
2. Second Scenario
   - Radio 0 — WGB mode configured; Status: Enabled (uplink enabled).
   - Radio 1 — Root AP mode; 100 wireless clients supported.
3. Third Scenario
   - Radio 0 — Root AP mode; 100 wireless clients supported.
   - Radio 1 — Root AP mode; 100 wireless clients supported.

Note In the above scenarios, the root ap radio and wgb uplink radio can be configured as either Radio 0 or Radio 1 based on the requirement.

Prerequisite Router Configurations for Concurrent Radio Support

This section provides command examples to show the necessary configuration.

Uplink VLAN Configuration on the IR1800:

Unique mac config on Uplink VLAN is a mandatory configuration on the IR1800 for the efficient packet traversing to WP-WIFI6 and vice-versa. The following is an example:

```
interface Vlan119             ->This is the interface that can carry the data from local
network to the infrastructure n/w.
 mac-address c014.fe60.ef8d   ->unique mac address configuration
 ip address dhcp              ->Uplink VLAN gets ip from infra via DHCP
 ip nat outside               ->This config should be done to NAT the downlink/wireless
client traffic from vlan 4094 to vlan 119
```

Note The unique mac-address derived from Gig0/0/0 mac address + 4

In case of uWGB as uplink, the unique mac address needs to be provided as wired client mac while executing the uWGB configuration CLI.

configure dot11radio <0/1> mode uwgb *<c014.fe60.ef8d> ssid-profile <ssid profile name>*

In order to obtain the mac address, use the **show int GigabitEthernet0/0/0** command:

```
Router#show int GigabitEthernet0/0/0
GigabitEthernet0/0/0 is administratively down, line protocol is down
  Hardware is IR1821-1x1GE, address is c014.fe60.ef80 (bia c014.fe60.ef80)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is Auto Select
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

The following is sample wgb bridge table output:

```
AP84EB.EF55.1438#sh wgb bridge
    ***Client ip table entries***
mac vap            port  vlan_id     seen_ip              confirm_ago     fast_brg
A0:E7:0B:D5:99:95  12    apr0v12     4094  192.168.94.13   158.708000      true
76:68:82:01:86:C9  13    apr0v13     4094  192.168.94.2    0.000000        true
C0:14:FE:60:EF:8D  0     wired0      0     10.119.119.229  1.814000        true
```

Note In the bridge table entry only the SVI/ Wired client based on Uplink VLAN(119) and the wireless client based on downlink VLAN will be learnt. The SVI address based on downlink VLAN(4094), will not be learnt here. The uplink VLAN(VLAN 119) configured on IR1800 will be learnt by vlan id '0' since it is the native VLAN.

Downlink VLAN Configuration on the IR1800:

See the following example:

```
interface Vlan4094           ->Downlink VLAN for wireless client traffic
  ip address 192.168.94.1 255.255.255.0
  ip nat inside              ->Should be provided in the local network VLAN to communicate
 with infrastructure VLAN
```

DHCP Pool Configuration for the Downlink VLAN Interfaces:

See the following example:

```
ip dhcp pool vlan4094  -> Downlink VLAN's are the used for wireless client(Root ap: WLAN-VLAN
 mapping)
  network 192.168.94.0 255.255.255.0
  default-router 192.168.94.1
  dns-server 8.8.8.8
```

Wl0/1/4 Port Configuration:

The following is an example of the Wl0/1/4 port configuration. The internal-Gig0 port to which the AP is connected to the router.

```
interface Wlan-GigabitEthernet0/1/4
  switchport trunk native vlan 119
  switchport trunk allowed vlan 119,4094
  switchport mode trunk
```

Note The vlan 119 is the wgb uplink vlan and vlan 4094 is the Downlink VLAN used for the traffic of wireless clients.

NAT ACL Configuration:

The following example shows a configuration to create NAT ACL rules.

```
ip access-list extended NAT_ACL
  10 permit ip 192.168.94.0 0.0.0.255 any
//subnet of Downlink VLAN 4094 interface
   route-map RM_WGB_ACL permit 10   ->Used for Routing table mapping
   match ip address NAT_ACL         ->NAT list used for translation
   match interface Vlan119          ->NAT interface (infrastructure VLAN)
```

Route Map to Communicate with the Outside Network:

```
ip nat inside source route-map RM_WGB_ACL interface Vlan119 overload
```

Note For additional router topology scenarios, refer to the Cisco Connected Mass Transit System Implementation Guide (Cisco Validated Design).

Configuring Radio Interface as WGB/uWGB and Root AP Mode

The wireless client support requires administrative configurations for various items. To support this feature, the following CLIs are used.

Configure the Unified WGB Mode from CAPWAP Mode

Use the following command:

```
configure boot mode wgb
```

Configure the SSID on WGB Uplink or Root AP in Radio Interface

Use the following command:

```
configure ssid-profile <profile-name> ssid <ssid-name>
authentication <auth-type> key-management <key-mgmt>
```

Configure the Radio as WGB Mode

Use the following commands:

```
configure dot11Radio <0|1> mode wgb ssid-profile <ssid profile name>
configure dot11Radio <0|1> enable
```

Configure the Radio as uWGB Mode

Use the following commands:

```
configure dot11Radio<0|1>mode uwgb <client mac> ssid-profile<ssid profile name>
```

Note <client mac> - In case of uWGB as uplink, the unique mac address of Router SVI or PC wired client mac can be provided as <wired client mac> while executing the uWGB configuration CLI.

For concurrent root ap radio mode to work if the uplink backhaul is in uWGB mode, provide the unique MAC address of the Router Switched Virtual Interface (SVI) as the 'wired client mac' in the CLI. This step allows the Router SVI to obtain an IP address while the Wi-Fi module is configured in uWGB mode. The Router SVI will be the uplink VLAN, enabling it to forward packets from the downlink VLAN,such as wireless clients, once IP routing or NAT configurations are applied.

For more information, see Prerequisite Router Configurations for Concurrent Radio Support

Configure the Radio as Root-AP Mode

Use the following command:

```
configure dot11Radio <0|1> mode root-ap
```

Map the SSID to Root-AP Mode Radio Interface along with VLAN-ID

Use the following commands:

```
configure dot11Radio <0|1> wlan add <profile-name> <wlan id> vlan <vlan-id>
```

Note In the above command, the VLAN creation in client serving radio will be bridged to wired0, so that the traffic from the wireless client will be forwarded directly to the Router. The Wlan id Range is from 2 -16 (Max support 15 wlans).

The root ap related configurations will be saved/taken effect only after toggling the root ap radio.

If Broadcast tagging in wgb is enabled, then the Root AP cannot support wireless client connection. Broadcast tagging configuration will be disabled by default.

```
configure dot11Radio <0|1> wlan delete <profile-name>
```

Configure the Radio Channel to Broadcast the SSID for Root-AP Radio Interface

Use the following command:

```
configure dot11Radio <0|1> channel <channel number> <width>
```

Note If radar is detected on a configured channel, then the channel will be changed automatically and will not return to the configured channel.

Configure the Antenna for Radio Interface

Use the following command:

```
configure dot11Radio <0|1> antenna <dot11 antenna a/ab>
```

Configure QoS Profile and Attach it to SSID Profile (Optional)

Use the following command:

```
configure qos profile <qos-prof-name> <bronze|gold|platinum|silver> configure ssid-profile
<profile-name> ssid <ssid> qos profile <qos-prof-name>
```

Enable or Disable Types of 802.11

Use the following commands:

```
configure dot11radio <slot-id> 802.11ax <enable/disable>
configure dot11radio <slot-id> 802.11n <enable/disable>
configure dot11radio <slot-id> 802.11ac <enable/disable>
```

Configure Power Constraint and Channel sw-count

Use the following command:

```
configure dot11radio <slot-id> 802.11h power-constraint <value> channel-switch-count <value>
```

Configure tx-power in the Radio Interface

Use the following command:

```
configure dot11Radio <0|1> tx-power <1-8>
```

Root AP Radio Configuration Examples When uWGB as Uplink Backhaul

The following are examples of Root AP radio configuration when uWGB as uplink backhaul.

```
WIFI module uWGB configuration:
==============================
AP6879.0974.F728#sh running-config
AP Name : AP6879.0974.F728
AP Mode : WorkGroupBridge
CDP State : Enabled
Watchdog monitoring : Enabled
SSH State : Enabled
AP Username : admin
Session Timeout : 0
WGB Trace : Disabled
Syslog Host : 0.0.0.0


Radio and WLAN-Profile mapping:-
==================================
Radio ID Radio Mode SSID-Profile SSID
Authentication
0 RootAP root_wlan root_wlan
OPEN
1 UWGB Test Test
OPEN


Radio configurations:-
==============================
Radio Id : 0
Admin state : ENABLED
Mode : RootAP
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Channel(Band) : 1 (20)
Beacon Period : 100 mSec
Tx Power : 1
802.11ac : Disabled
802.11ax : Enabled
802.11n : Enabled
Encryption mode : AES128
Radio Id : 1
Admin state : ENABLED
Mode : UWGB
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Uclient mac : C014.FE60.EF8D
Current state : UWGB
UClient timeout : 0 Sec
Dot11 type : 11ax
11v BSS-Neighbor : Disabled
A-MPDU priority : 0x3f
A-MPDU subframe number : 255
RTS Protection : 2347(default)
Rx-SOP Threshold : AUTO
Radio profile : NA
Encryption mode : AES128


List of Root-AP SSID-Profiles:
=======================================
Radio id : 0, SSID-Profile_8 : root_wlan
```

```
WGB specific configuration:-
====================================
WGB Radio Id : NA
Mode State : NA
SSID Profile : NA
UWGB Radio Id : 1
Mode Enable : Enable
SSID Profile : Test
Uclient MAC Address: C014.FE60.EF8D

Password Policy configured:-
====================================
password policy : Enable
password minimum length : 8
password lifetime : Disable
Upper Case Required : 1
Lower Case Required : 1
Digit Required : 1
Special Character Required : 1

Rx Beacon Missing Action : Enable
Rx Beacon Missing Count : 100
Packet retries Action : Reconnect
Packet retries Value : 64
RSSI Threshold Value : 70 dBm
Threshold timeout : 5 Sec
HSR-Scan status : Disable
Auth response timeout : 5000 Msec
Assoc response timeout : 5000 Msec
11v neighbor query timeout : 10 sec
WGB channel scan timeout : 20 Msec
Dhcp response timeout : 60 Sec
EAP timeout : 3 sec
Bridge table aging-time : 300 Sec
Probe pak data rate type : NA
Probe pak data rate : 0
Antenna Band Mode : Dual
Broadcast tagging : Disable
Wired Client 802.1x Auth : Disable
IGMP querier IP address : ::
Offchan scan status : Disable

Total configurations size on different structure:-
=================================================
Total channels : 0
Total SSID-Profiles : 3
Total Root-AP SSID-Profile : 1
Total EAP Profiles : 0
Total QOS Profiles : 0
Total dot1x credentials : 0
Total PKI truspoints : 0
Total bridge groups : 0

Total SSID profiles configured are:
=========================================
SSID-Profile : Test
SSID Name : Test
SSID Profile path : /data/platform/wbridge/Test
Auth type : OPEN
DTIM Period : 1
QOS profile :
```

```
SSID-Profile : root_wlan
SSID Name : root_wlan
SSID Profile path : /data/platform/wbridge/root_wlan
Auth type : OPEN
DTIM Period : 1
QOS profile :

L2NAT Configuration are:
====================================
Status: disabled
Default Vlan: 0
The Number of L2nat Rules: 0
Dir Inside Outside Vlan

Ethernet Port Native VLAN Configuration are:
====================================
Ethernet Port: 0
Status: disabled
Native VLAN ID: 0
Ethernet Port: 1
Status: disabled
Native VLAN ID: 0

Total QoS Mapping profiles configured are:
==========================================
Number of QoS Mapping Profiles: 0

Configuration command list:
===========================
### WGB Running config - Hostname: AP6879.0974.F728 ###
configure ap management add username admin password $1$$khxfBj0qAAV4gFMFboJcg. s
ecret $1$$khxfBj0qAAV4gFMFboJcg.
configure ssid-profile Test ssid Test authentication open
configure ssid-profile root_wlan ssid root_wlan authentication open
configure dot11Radio 1 mode uwgb C014.FE60.EF8D ssid-profile Test
configure dot11Radio 1 enable
configure wgb mobile period 5 70
configure dot11Radio 0 mode root-ap
configure dot11Radio 0 wlan add root_wlan 8 vlan 10
configure dot11Radio 0 encryption mode ciphers aes-ccm
configure dot11Radio 0 antenna ab-antenna
configure dot11Radio 0 channel 7 20
configure dot11Radio 0 802.11ac disable
configure dot11Radio 0 tx-power 1
configure dot11Radio 0 enable
configure dot11Radio 1 encryption mode ciphers aes-ccm
configure dot11Radio 1 tx-power 1
```

Web Authentication on WGB Root AP

Web Authentication Overview

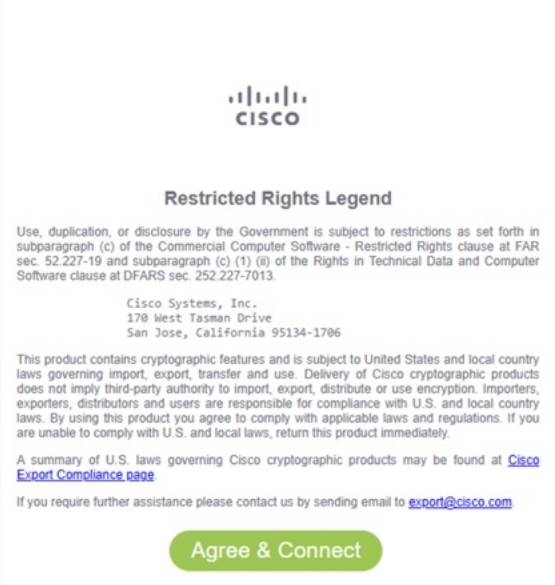
Web authentication serves as a Layer 3 security feature for setting up guest-access networks. It authenticates through a web browser on a wireless client and allows you to connect to an open SSID without creating a user profile.

From Cisco IOS XE Release 17.15.1, you can configure and customize web authentication on the WGB Root AP. Configuring web authentication activates a captive portal on the WGB Root AP for WP-WIFI6. Agree the terms and conditions on the web portal to gain internet access.

You can configure web authentication to use either a default or a customized web page.

The following figure represents the default captive portal page.

Figure 1: Default Captive Portal Page



Also, you can customize the web authentication to:

- Redirect the URL of your choice after accepting the captive portal web page.
- Copy the customized consent web page to WIM and use it for web authentication of WGB Root AP.
- Allocate a custom virtual interface IP address for the captive portal web page.
- Add preauthentication Access Control List (ACL) rules to access specific internet destinations before they accept the terms and conditions in a captive portal web page.

  For instance, displaying advertisements from an external website on the current captive portal web page.

Note Web authentication supports Android, iOS, macOS, and Windows wireless clients.

Web Authentication Process

1. **Connect to Wi-Fi**: Select the hotspot SSID and connect to the public Wi-Fi network to establish the connection on your device.
2. **Detect Captive Portal**: The device automatically detects the associated captive portal after connecting to the SSID.

3. **Activate Web Authentication**: The device activates a web browser, displaying a specific consent web page.
4. **Complete the Authentication**: Read and understand the instructions on the web authentication page, then click the **Agree & Connect** button on the consent web page to accept the terms of service.
5. **Access the Internet**: After completing the steps required by the Captive Portal Assistant, you gain internet access through the network.

Note **Client Cache**: The device bypasses the consent page upon reconnection within a 5 minutes window after completing web authentication.

Prerequisites of Web Authentication Configuration

Perform the following steps to configure the WiFi module and router.

Procedure

Step 1 Configure radio interface to WGB and root AP mode, see Configuring Radio Interface as WGB/uWGB and Root AP Mode, on page 45.

Step 2 Configure the router for concurrent radio support, see Prerequisite Router Configurations for Concurrent Radio Support, on page 43.

Step 3 Configure the router IP Service Level Agreements (SLA) to ping WGB static IP address.

```
Device(config)#ip sla number
```

Example:

```
Router(config)#ip sla 10
Router(config-ip-sla)#icmp-echo 192.0.2.1 source-interface Vlan4094
Router(config-ip-sl-echoa)#frequency 5
Router(config)#ip sla schedule 10 start-time now
```

Note

- 192.0.2.1 is the WGB's static IP address and Vlan4094 is the downlink VLAN to communicate between router and WGB.
- The router's IP SLA pings the WGB's static IP address.
- If the WGB root AP has a static IP address, you need to activate the WGB's static IP address after a reload by pinging it or initiating a ping from the WGB. Otherwise, the web authentication page will not pop out successfully.
- The router's IP SLA configuration activates the WGB's static IP address and allows the web authentication page to pop up without manual ping.

Limitations of Web Authentication

Web authentication is designed to support only IPv4 addresses and IP addresses for preauthentication Access Control Lists (ACLs). It does not support Fully Qualified Domain Name (FQDN) ACLs.

Configure a redirect URL is mandatory for Android clients.

Configure Web Authentication Settings

Enable Web Authentication

In the AP, perform these steps to configure the web authentication.

Procedure

Step 1 Run the command to enable the HTTPd service.

Device#**configure ap http enable**

Note
By default, HTTPd service is enabled. Run the **configure ap http disable** command to disable the HTTPd service.

Step 2 Run the command to enable web authentication.

Device#**configure webauth enable**

Note
Run the **configure webauth disable** command to disable web authentication.

Step 3 Run the command to configure web authentication in Root-AP WLAN.

Device#**configure dot11Radio** {**0** | **1**} **wlan add** <**profile-name**> <**wlan id**> **vlan** <**vlan id**> **webauth** {**default_webpage**/**customized_webpage**}

Note
The default web page is webauthpassthrough.html. If required, you can use a custom web page.

If a custom web page is not uploaded to WGB, the AP prints a warning and uses the default web page.

Example:

The following are the examples of default and custom web page configuration:

- Default web page:

```
Device#configure dot11Radio 1 wlan add WebAuth 4 vlan 4094 webauth default_webpage
```

- Custom web page:

```
Device#configure dot11Radio 1 wlan add WebAuth-customize 5 vlan 4094 webauth customized_webpage
```

Customize Web Authentication Settings

In the AP, perform these steps to customize the web authentication settings:

Procedure

Step 1 Copy the customize web page from the server to WIM storage.

Device#**copy webpage {tftp|sftp}://<server-ip>[/dir][/filename]**

Device#**copy webpage scp://username@<server-ip>[:port]:/dir[/filename]**

Note
You can copy a .tar file or an HTML file. The .tar file size should not exceed 10 MB.

Example:

```
Device#copy webpage scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar
copy "scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar" to
"/storage/webauth/customized_webpage" (Y/N)Y
root@100.10.10.3's password:
wp_wifi6_web.tar                              100%   30KB   6.4MB/s   00:00
[*04/24/2024 08:27:34.1830] wp_wifi6_web/
[*04/24/2024 08:27:34.1830] wp_wifi6_web/logo.jpg
[*04/24/2024 08:27:34.1830] wp_wifi6_web/webauth.css
[*04/24/2024 08:27:34.1830] wp_wifi6_web/reg_customized_webpage.html
[*04/24/2024 08:27:34.1840] % Customized webpage will use wp_wifi6_web/reg_customized_webpage.html
as index.html
```

Save the files to the storage path: /storage/webauth/customized_webpage/. Extract the tar package into this directory and rename the HTML page to index.html.

Step 2 Configure a redirect URL.

Device#**configure webauth redirect-url** {**customized|default**}**RedirectURL**

Example:

```
Device#configure webauth redirect-url customized https://www.example.com/
```

Note
To remove the custom redirect URL, use the **configure webauth redirect-url default** command.

Step 3 Configure a virtual interface in web authentication interface.

Device#**configure interface webauth address ipv4 static**<**interface_ip**> <**netmask**>

Example:

```
Device#configure interface webauth address ipv4 static 10.10.10.10 255.255.255.255
```

Note
By default, the web authentication interface uses the IP address 1.1.1.1, which is a virtual interface IP (consent page website IP address).

Step 4 Configure preauthentication ACL.

Device#**configure webauthpreauth-acl add** <**aclrules**>

Example:

```
Device#configure webauth preauth-acl add "allow true and dst 192.168.93.1 mask 255.255.255.0 and ip
 proto 6″
```

Sample ACL rules formats are.

- {allow/deny} {icmp/tcp/udp}
- {allow/deny} {icmp/tcp/udp} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <> {and/or} {ip proto <>}
- {allow/deny} true
- {allow/deny} all
- {allow/deny} true {and/or} {tcp/udp} {src/dst} port <>

Note

- The preauthentication ACL is activated when the client enters the WEBAUTH_REQD state.
- The maximum length for an ACL rule is 255 characters. There is no limit on the number of ACL entries.
- To delete the preauthentication ACL, run the **configure webauth pre-authentication acl delete** command.
- Deleting a preauthentication ACL clears all preauthentication ACL entries.

Importing and Exporting WGB Configuration

When you want to create a configuration similar to an existing, 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:

```
Device#copy configuration upload {sftp:|tftp:|scp:}// ip-address [directory] [file-name]
```

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

```
Device#copy configuration download {sftp:|tftp:|scp:}// 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.

Verify Web Authentication

Web Authentication

To verify the web authentication configuration, use the **show webauth** as shown in the example here.

```
Device#show webauth

WEBAUTH Configuration are:
==================================
HTTP Status: enabled
Webauth Status: enabled
Webauth Redirect-URL: https://www.example.com/
Webauth Preauth-ACL: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6,
allow icmp dst 198.51.100.1 mask 255.255.255.0,  allow icmp src 198.51.100.1 mask
255.255.255.0
Customized Webpage Exists: Yes
Customized Webpage MD5 HASH: 05ff0f8944e5466e484c342cba6fc403
```

Web Authentication Current Status

To view the root AP WLAN status, use the **show controller dot11radio {0|1} wlan** as shown in the example here.

```
Device#show controllers dot11Radio 1 wlan

apr1v0    Link encap:Ethernet  HWaddr 68:79:09:B8:03:8F
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:60425858
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:38

radio vap id              mac              ssid state ml_enabled              mld webauth

    1      3 68:79:09:B8:03:8C            WebAuth    UP         No 00:00:00:00:00:00
Yes
    1      4 68:79:09:B8:03:8B  WebAuth-customize    UP         No 00:00:00:00:00:00
Yes

NON_ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr1v3   3051 2976    75 2376573    919      0   2902 2556   346  575037     0  4.196000
apr1v4    427  402    25  289034     31      0    460  344   116   70123     0  4.196000
ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr1v3      0    0     0       0      0      0      0    0     0       0     0  4.196000
apr1v4      0    0     0       0      0      0      0    0     0       0     0  4.196000

Vlan BSSID Pri/U/M EncryPolicy Key0 Key1 Key2 Key3 iGTK                SSIDs MFP
2290   38C   3 3 3       NONE                      DIS              WebAuth   0
2290   38B   3 3 3       NONE                      DIS     WebAuth-customize   0

VAP-ID                 SSID  Bridging Type
     3              WebAuth Local-Switched
     4     WebAuth-customize Local-Switched
```

Web Authentication Client Status

To verify the client web authentication status, use the **show controller dot11radio {0|1} client** as shown in the example here.

```
Device#show controllers dot11Radio 1 client

              mac radio vap aid        state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D     1   3   2 WEBAUTH_REQD OPEN MCS112SS    HE  HE        false
00:00:00:00:00:00         No        Yes             No
00:50:54:27:A2:9F     1   3   1          FWD OPEN MCS112SS    HE  HE        false
00:00:00:00:00:00         No        Yes             Yes

APAP6879.0974.FD08#show client summary

Radio Driver client Summary:
============================
apr1v3
-------
STA BC:6E:E2:67:CD:9D
  chanspec 153 (0xd099)
  state: AUTHENTICATED ASSOCIATED AUTHORIZED
  per antenna rssi of last rx data frame: -34 -34 0 0
  per antenna average rssi of rx data frames: -34 -33 0 0
```

```
  per antenna noise floor: -82 -84 0 0
smoothed rssi: -33
tx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 2xLTF GI 1.6us auto
rx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 4xLTF GI 3.2us auto

apr1v4
-------

WCP client Summary:
====================

              mac radio vap aid        state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D     1    3   2 WEBAUTH_REQD OPEN MCS112SS    HE  HE        false
00:00:00:00:00:00         No        Yes             No

Assoc time:
=============
              mac      assoc_time
BC:6E:E2:67:CD:9D 00d:00h:04m:08s
```

Note Before you accept the consent page, the client state is WEBAUTH_REQD, and after the web authentication is complete, the client state changes to FWD (forward).

Preauthentication ACL

To view the client's current preauthentication ACL, use the **show client access-lists pre-auth all client mac-address** as shown in the example here.

```
Device#show client access-lists pre-auth all BC:6E:E2:67:CD:9D
Pre-Auth URL ACLs for Client: BC:6E:E2:67:CD:9D
IPv4 ACL: PREAUTH
IPv6 ACL:
ACTION    URL-LIST
Resolved IPs for Client: BC:6E:E2:67:CD:9D
HIT-COUNT      URL        ACTION    IP-LIST
PREAUTH
    rule 0: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6
    rule 1: allow icmp dst 198.51.100.1 mask 255.255.255.0
    rule 2: allow icmp src 198.51.100.1 mask 255.255.255.0

No IPv6 ACL found
Redirect URL for client: BC:6E:E2:67:CD:9D

Acl name Quota Bytes left In bytes Out bytes In pkts Out pkts Drops-in Drops-out
 PREAUTH     0          0        0       148       0        2       21       201
CLIENT STATE: WEBAUTH_REQD
WEBAUTH_REQUIRED: TRUE
DNS POST AUTH:  FALSE
PREAUTH ENABLED: TRUE
POSTAUTH ENABLED: FALSE
```

802.1x authentication on Wi-Fi Interface Module

Information about 802.1x authentication

The IEEE 802.1x is a standard for network access control and it uses enterprise networks to secure both wired and wireless access.

Note The WIM supports only WPA2-Enterprise for 802.1x authentication.

Key components of 802.1x authentication

- Extensible Authentication Protocol (EAP): EAP packets are used to exchange authentication messages.
- Identity Services Engine (ISE): Works with RADIUS servers to authenticate and authorize devices that intend to connect to the AP.
- Remote Authentication Dial-In User Service (RADIUS): Provides centralized Authentication, Authorization, and Accounting (AAA) management for network services.

802.1x authentication support

From release 17.16.1, the concurrent Root radio in the Wireless Interface Module supports 802.1x authentication for wireless clients.

802.1x authentication allows the configuration of primary and secondary RADIUS servers.

Service-VLAN and router

During the 802.1x authentication process for wireless clients connected to the Root radio mode:

1. Configure the router with a VLAN using static IP address to handle RADIUS packets from WIM for RADIUS authentication.
2. Configure the Service-VLAN on the WIM.

Note Ensure that the gateway IP address of the router and the Service-VLAN on the WIM are within the same IP network and are able to communicate with each other.

This setup forwards RADIUS packets between the router and the WIM through the VLAN.

The router identifies the active link on the infrastructure side and routes the traffic to either the WGB uplink, the cellular backhaul, or the Ethernet link, depending on which connection is active and configured.

When the WGB uplink is enabled, the router uses it as the active backhaul and when it is disabled, the router switches to the cellular backhaul.

The NAT configurations are applied between the service VLAN and uplink VLAN to ensure the RADIUS server is reachable.

802.1x Authentication Methods

The concurrent Root radio with 802.1x supports two types of authentication.

- Certificate-based authentication methods:
  - TLS, and
  - Tunneled Transport Layer Security (TTLS).

Note For certificate-based authentication, RADIUS server generates the certificates and shares them with the wireless client. The certificate include the username, password, and the client's MAC address.

- Non-certificate-based authentication methods:
  - Protected Extensible Authentication Protocol (PEAP): Encapsulates EAP within an encrypted and authenticated TLS tunnel.
  - Flexible Authentication via Secure Tunneling (FAST): Establishes a secured TLS tunnel with RADIUS using a strong shared key.
  - Lightweight Extensible Authentication Protocol (LEAP): Supports strong mutual authentication using a logon password as the shared secret, and provides dynamic per-user, per-session encryption keys.

Note For non-certificate-based authentication methods, RADIUS server creates the username and password.

Configures RADIUS server credentials in the wireless client which allows the client to associate with the PEAP protocol.

After the RADIUS server completes authentication, the wireless client is assigned an IP address and can transmit traffic.

For more information Cisco ISE configuration, see the Cisco Identity Services Engine Administrator Guide.

Benefits of 802.1x authentication support

The benefits of 802.1x authentication for network security and reliability:

- Authorized devices can access the network by authenticating devices using RADIUS servers.
- Maintains authentication capabilities even if the primary uplink is lost, by using a dedicated Service-VLAN interface.
- Supports configuration of both primary and secondary RADIUS servers for redundancy.

Configure 802.1x authentication on Wi-Fi Interface Module

Use this task to configure the 802.1x authentication on the WIM.

Before you begin

To configure the 802.1x authentication on the WIM, ensure the given prerequisites are met:

- Configure the router for concurrent radio support. Prerequisite Router Configurations for Concurrent Radio Support, on page 43
- Configure the service VLAN interface with a static IP address.
- Configure the service VLAN, Root AP VLAN, and Bridge Virtual Interface (BVI) on different VLANs.
- Enable EAP support on the RADIUS server.

Procedure

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

```
Device#configure eap-profile test-eap method fast
```

This command sets up the EAP profile with a specified authentication method. In this example, the EAP method is set to FAST.

Step 2 Use the **configure dot1x credential** *credential-name* **username** *name* **password** *password* command to configure 802.1x credential profile on the WIM.

Note
The WIM receives the username and password from the RADIUS server.

```
Device#configure dot1x credential test1 username XYZ password *****
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *credential-name* command to map the previously configured 802.1x credential to the EAP profile on the WIM.

```
Device#Device# configure eap-profile test-eap dot1x-credential test1
```

Step 4 Use the **configure radius authentication** {**primary** | **secondary**} **add ipv4** *radius-server-ip-address* **port** *radius-server-port-number* **secret** *radius-secret* command to configure a primary or secondary, or both RADIUS server with an IPv4 address, port, and secret. on the WIM.

```
Device#configure radius authentication primary add ipv4 192.168.1.2 port 1812 secret Cisco123
```

This sets up the RADIUS server details for authentication.

Step 5 Use the **configure interface service-vlan address ipv4 static** *ap-servicevlan-ipaddress netmask router-servicevlan-ipaddress* **vlan** *vlan-id* command to configure the interface service-VLAN on the WIM.

```
Device#configure interface service-vlan address ipv4 static 192.168.94.15 255.255.255.0 192.168.94.1
 vlan 96
```

router-servicevlan-ipaddress is the router's interface IP address to forward RADIUS packets between the AP and the router.

Note
The Service-VLAN configuration functions only if one of the radios is in Root radio mode.

Step 6 Use the **configure ssid-profile** *profile-name* **ssid** *ssid-name* **authentication eap profile** *eap-pofile* **key-management** {**wpa2** | **dot11r**} command to configure downlink 802.1x wlan in concurrent radio Root AP.

```
Device#configure ssid-profile Test ssid Free authentication eap profile test-eap key-management wpa2
```

Step 7 Use the **configure dot11Radio 0 wlan add** *ssid-name wlan-id* **vlan** *vlan-id* command to map the downlink wlan to concurrent radio Root AP.

```
Device#configure dot11Radio 0 wlan add root_wlan 8 vlan 10
```

Note
Ensure that the Service-VLAN and the VLAN configured for the Root radio are in different VLANs.

Step 8 Use the **configure dot11Radio 0** {*enable* | *disable*} command to enable or disable concurrent radio Root AP.

```
Device#configure dot11Radio 0 enable
```

Step 9 (Optional) Verify the configuration using the show commands as required.

- Use the **show ip route** command to print the gateway IP for the service VLAN interface.

```
Device#sh ip route
IPv4:
  gateway-ip  :
  gateway-mac :
IPv6:
  gateway-ip  :
  gateway-mac :
SERVICE-VLAN:
  gateway-ip  : 192.168.94.1
```

- Use the **show controllers dot11Radio** {*0* | *1*} **wlan** command to verify the WLAN mapped to radio interface 0.

```
Device#sh controllers dot11Radio 0 wlan
apr0v0    Link encap:Ethernet  HWaddr 68:79:09:B7:EC:00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:1004957
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:42

radio vap id               mac ssid state ml_enabled               mld webauth
    0      7 68:79:09:B7:EC:07  zxc    UP         No 00:00:00:00:00:00      No

NON_ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr0v7   5387  771  4616  108305   2492      0   4493 1576  2917  500790     0  2.606000
ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
apr0v7      0    0     0       0      0      0      0    0     0       0     0  2.606000

Vlan BSSID Pri/U/M EncryPolicy Key0 Key1 Key2 Key3 iGTK SSIDs MFP
  10   EC7   3 3 3       NONE                      DIS   zxc   0
```

- Use the **show wgb bridge** command to verify the client connected to the WIM and their IP addresses.

```
Device#sh wgb bridge
    ***Client ip table entries***
             mac vap   port vlan_id        seen_ip confirm_ago fast_brg
E4:62:C4:49:B9:74   0 wired0      20 192.168.69.106    21.696000     true
E4:62:C4:49:B9:78   0 wired0       0 192.168.69.103    4.354000     true
00:50:56:85:15:B7   0 wired0       0 192.168.69.118    4.100000     true
00:13:EF:F1:0D:78   7 apr0v7      10 192.168.69.200    2.616000     true
```

- Use the **show client summary** command to verify additional details about the clients connected to the WIM.

```
Device#show client summary

Radio Driver client Summary:
============================
apr0v7
-------
STA 00:13:EF:F1:0D:78:
         chanspec 7 (0x1007)
         state: AUTHENTICATED ASSOCIATED AUTHORIZED
         per antenna rssi of last rx data frame: -49 -55 0 0
         per antenna average rssi of rx data frames: -49 -51 0 0
         per antenna noise floor: -80 -76 0 0
smoothed rssi: -49
tx nrate
mcs index 12 stf mode 3 auto
rx nrate
legacy rate 1 Mbps stf mode 0 auto
```

Delete 802.1x configuration on Wi-Fi Interface Module

Use this task to delete the 802.1x configurations on the WIM.

Procedure

Delete the configuration using the given commands as required.

- Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

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

- Use the **configure dot1x credential** *profile-name* **delete** command to delete a dot1x credential profile.

  ```
  Device#configure dot1x credential test1 delete
  ```

- Use the **configure radius authentication** {**primary** | **secondary**} **delete** command to delete a primary and (or) secondary radius server.

  ```
  Device#configure radius authentication primary delete
  ```

- Use the **configure interface service-vlan delete** *ipaddress* command to delete the service-VLAN.

  ```
  Device#configure interface service-vlan delete 192.168.1.15
  ```

Configure 802.1x authentication on router

This section provides command examples to show the configuration and verification on the IR1800.

Configure Service VLAN on the IR1800

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface vlan96
Router(config-if)#ip address 192.168.94.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#end
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#vlan 96
Router(config-vlan)#end
```

VLAN 96 is the Service-VLAN configuration on the router side for the RADIUS server.

Use the **show ip interface brief** command to verify the VLAN configuration on the IR1800.

```
Interface    IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1/0   unassigned      YES unset  administratively down down
GigabitEthernet0/1/1   unassigned      YES unset  down                  down
GigabitEthernet0/1/2   unassigned      YES unset  up                    up
GigabitEthernet0/1/3   unassigned      YES unset  administratively down down
Wl0/1/4                unassigned      YES unset  up                    up
Cellular0/4/0          unassigned      YES NVRAM  down                  down
Cellular0/4/1          unassigned      YES NVRAM  administratively down down
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 192.168.69.103  YES NVRAM  up                    up
Vlan20                 192.168.69.118  YES NVRAM  up                    up
Vlan50                 192.168.69.106  YES NVRAM  up                    up
Vlan96                 192.168.94.1    YES NVRAM  up                    up
Vlan2309               192.168.69.103  YES DHCP   up                    up
```

Use the **show run interface vlan96** command to verify the Service VLAN configuration on the IR1800.

```
Router#sh run int vlan96
Building configuration...

Current configuration : 63 bytes
!
interface Vlan96
 ip address 192.168.94.1 255.255.255.0
 ip nat inside
end
```

Configure uplink VLAN on the IR1800

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface vlan2309
Router(config-if)#ip address dhcp
Router(config-if)#mac-address e462.c449.b978
Router(config-if)#ip nat outside
Router(config-if)#end
```

Use the **show run interface vlan2309** command to verify the uplink VLAN configuration on the IR1800.

```
Router#sh run int vlan2309
Building configuration...

Current configuration : 87 bytes
!
interface Vlan2309
 mac-address e462.c449.b978
 ip address dhcp
 ip nat outside
end
```

Configure NAT between uplink VLAN and Service VLAN

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended NAT_ACL
Router(config-ext-nacl)#10 permit ip 192.168.94.1 255.255.255.0 any
```

```
Router(config-ext-nacl)#exit
Router(config)#route-map RM_WGB_ACL permit 10
Router(config-route-map)#match ip address NAT_ACL
Router(config-route-map)#match interface Vlan2309
Router(config-route-map)#ip nat inside source route-map RM_WGB_ACL interface Vlan2309
overload
```

Use the **sh run | i NAT** command to verify the NAT Configuration on the IR1800.

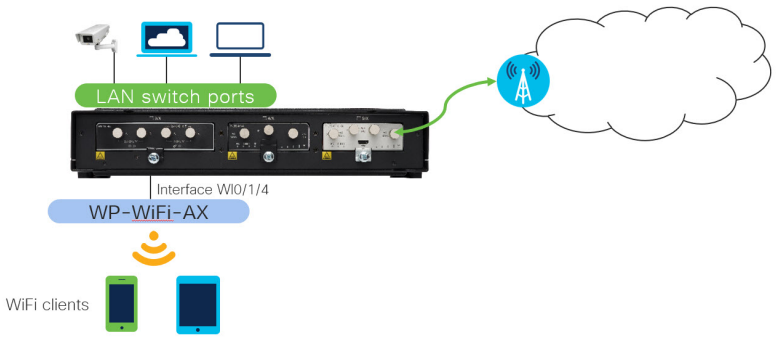
```
Router#sh run | i NAT
ip access-list extended NAT_ACL
 match ip address NAT_ACL
 match ip address NAT_ACL
Router#sh run | i ACL
ip nat inside source route-map RM_WGB_ACL interface Vlan2309 overload
ip access-list extended NAT_ACL
route-map RM_WGB_ACL permit 10
 match ip address NAT_ACL
route-map RM_WGB_ACL permit 20
 match ip address NAT_ACL
```

Cisco Embedded Wireless Controller (EWC)

The Embedded Wireless Controller (EWC) scenario offers:

- Self-Management
- Traffic Local-Switching
- May manage cascaded AP, aligned on C9105 + IR1800 performances
- WebUI management
- Cisco Catalyst Wireless Mobile Application (iPhone/Android)

EWC mode is typically used for Mass Transit/Transportation Remote & Mobile Assets.



When the Wireless Interface Module is running in EWC mode, it acts as a wireless controller and an Access Point (usually called internal AP). EWC manages other APs in a similar way as dedicated wireless controller (like C9800 series).

In a Cisco EWC network, an Access Point (AP) running the wireless controller function is designated as the active AP. The other access points, which are managed by this active AP, are referred to as subordinate APs.

The image used for EWC mode is C9800-AP-iosxe-wlc.bin.

The active EWC has two roles:

- Functions and operates as a Wireless LAN Controller (WLC) to manage and control the subordinate APs. The subordinate APs operate as lightweight access points to serve clients.
- Operates as an access point to serve clients.

For Wi-Fi landing page feature (Web-based authentication) support, see the Web-Based Authentication chapter in the Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide.

Further information on the Cisco Embedded Wireless Controller can be found in the following:

Cisco Embedded Wireless Controller on Catalyst Access Points FAQ

Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) White Paper

Prerequisites for Configuring EWC Access Point on the IR1800

Before configuring the EWC Access Point on the router, ensure the following prerequisites are met:

- It is recommended not to have any other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Embedded Wireless Controller (EWC) network.
- A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address.
- To configure the EWC and AP integrated into IR1800 series router, you must configure a DHCP server, SVI interface, and NAT on the router. For more information on configuring the AP, see the Prerequisites for Configuring CAPWAP Access Point Configuration on the IR1800, on page 34 section.
- On an Embedded Wireless Controller (EWC), management traffic is untagged and should be configured as native VLAN on the switch port. If the WIM and WLANs are all on different VLANs, the WIM connected port on the router need to be configured as trunk and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a router configuration with WIM and WLANs on different VLANs:

Command	Purpose
interface Wlan-GigabitEthernet *slot/subslot/port* **switchport mode trunk** **switchport trunk native vlan** *number* **switchport trunk allowed vlan** *numbers*	Configure switchport mode and native VLAN of WIM internal switch interface. Native VLAN 10 should be AP management VLAN. VLAN 20 and 30 used for WLAN traffic.

See the following example:

```
Router(config)#interface Wlan-GigabitEthernet 0/1/4
Router(config-if)#switchport mode trunk
Router(config-if)#switchport trunk native vlan 10
Router(config-if)#switchport trunk native vlan 10,20,30
```

Configuring EWC Using Day 0 Provisioning

There are three ways to configure the AP using day 0 provisioning:

1. To connect the SSID to CiscoAirProvision-XXXX, follow the steps in Deploying the EWC.
2. You can also scan the QR Code by using the Catalyst Wireless Application on a mobile phone. Follow the steps in the User Guide for Cisco Catalyst Wireless Mobile Application.
3. You can manually configure the AP using CLI by following the steps in Configuring the Controller Using Day 0 Wizard (CLI), or performing the basic configuration manually by following the steps in Option 1. Initial CLI Configuration in the Convert Catalyst 9100 Access Points to Embedded Wireless Controller.

Other items to consider are:

- For day 0 configuration done through the WebUI or Cisco Wireless Mobility application, it is recommended to reload the Wi-Fi module making sure it obtains an IP address from configured VLAN pool, for example, VLAN10.
- For WebUI day 0, it may not work if using an IP address different from the default IP address:192.168.0.1, which also collides with day0 IP address of the IR1800 IOS-XE.

Connecting Cisco Embedded Wireless Controller (EWC) Capable Access Point to the Network

Depending on the deployment, Embedded Wireless Controller (EWC) Capable Access Point connected to the router port can be configured as an Access port or a Trunk port.

If Access Points and WLANs are all on the same network, Embedded Wireless Controller (EWC) capable Access Points can connect to router by access mode as shown in the following example.

```
interface Wlan-GigabitEthernet 0/1/4
switchport access vlan 10
switchport mode access
```

On an Embedded Wireless Controller (EWC), management traffic is untagged. If Access Points and WLANs are all on different VLANs, the Embedded Wireless Controller (EWC) capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown in the example below is a deployment with Access Points and WLANs on different VLANs.

```
interface Wlan-GigabitEthernet 0/1/4
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30
switchport mode trunk
```

EWC Mode WebUI Management

This section provides steps for configuring the WIM in EWC mode through the WebUI.

Day 0 Provisioning Using the Over-The-Air WebUI Setup Wizard

When the AP has rebooted in the Embedded Wireless Controller (EWC) mode, it broadcasts a provisioning SSID ending with the last digits of the MAC address. You can connect to provisioning SSID using the PSK password.

You can then open a browser and be redirected to mywifi.cisco.com, which takes you to the AP web UI. Enter the username as **webui** and password as **cisco**. Seeing further day0 configuration steps in following link: https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/white-paper-c11-743398.html#DeployingtheEWC

Note The web redirection to the Embedded Wireless Controller (EWC) configuration portal only works if you are connected to the provisioning SSID. It does not work if your laptop is connected to another Wi-Fi network or on the wired network. You cannot configure the AP from the wired network even if you enter the EWC IP address when it is in day0 wizard provisioning mode.

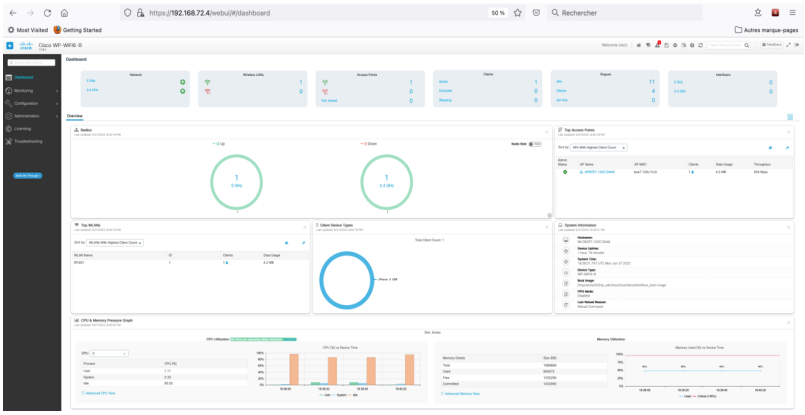
Logging in to the EWC WebUI

To log in to the EWC, perform the following steps:

Procedure

Step 1 Open the WebUI from a browser. Use the IP address allocated from DHCP.

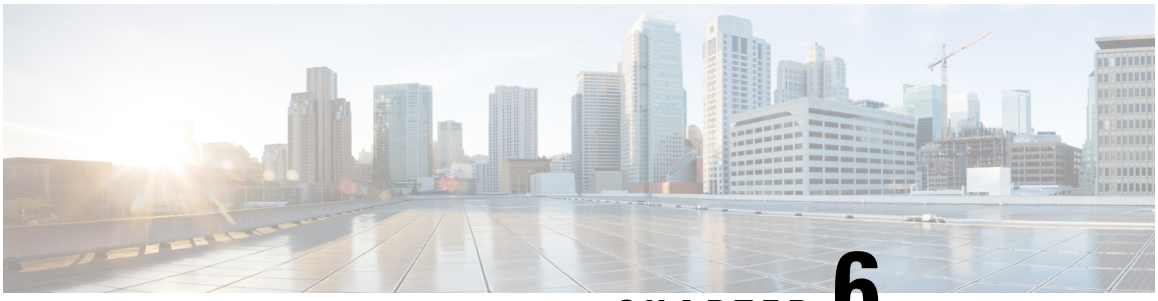
Step 2 The WebUI dashboard appears.



Step 3 Once connected to the Wireless LAN Controller (WLC), configuration is performed as any other access point. Refer to the following resources for additional information:

Overview of Cisco Embedded Wireless Controller on Catalyst Access Points

Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE



CHAPTER 6

Flexible Antenna Port

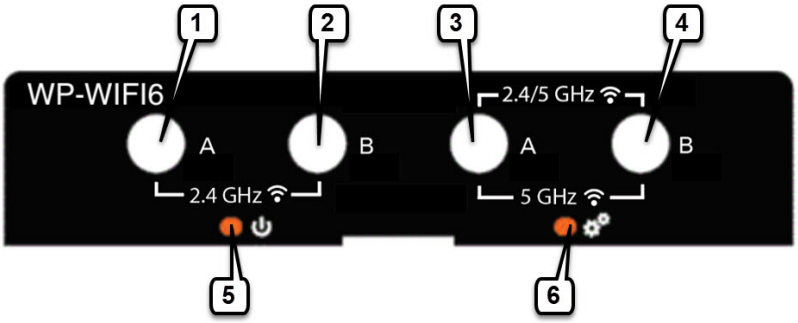
This chapter contains the following sections:

Flexible Antenna Port

The flexible antenna port feature allows customers to customize their radio coverage. The user can configure the feature as dual band mode or single band mode via CLI commands or the WebUI. The default is dual band mode.

For the antenna port labeling, the WIM uses A&B to label both the 2.4G and the 5G posts.

Looking at the front panel of the WIM the four antennae ports have been called out as 1 through 4. The 5 and 6 call-outs are status LEDs covered in the Hardware Overview, on page 1:



In Dual Band mode, install dual-band antennae to Antenna Port 3 & 4 on the right side.

In Single Band mode, install 2.4G band antennae to Antenna Port 1 & 2 on the left side, and install 5G band antennae to Antenna Port 3 & 4 on the right side.

Configuring Flexible Antenna Port for CAPWAP AP

These two procedures are used:

Configure CAPWAP AP Antenna Band Mode on Controller Using CLI

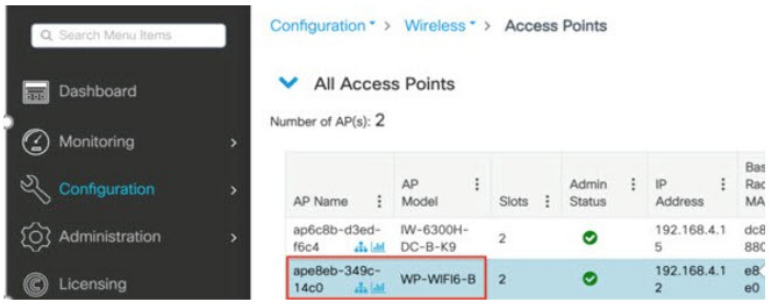
ap name <*Cisco AP*> **antenna band-mode** *[single]|[dual]*

For example:

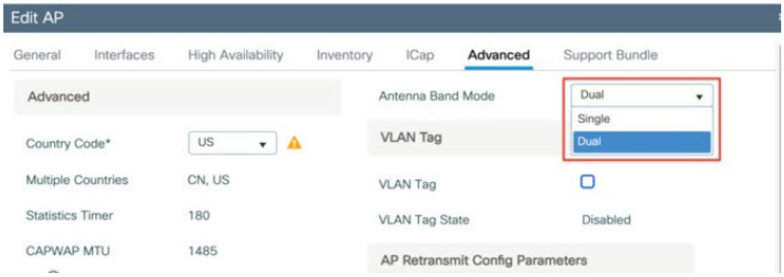
```
ap name ape8eb-349c-14c0 antenna-band-mode ?
  dual    Dual band mode
  single  Single band mode
```

Configure CAPWAP AP Antenna Band Mode on Controller Using WebUI

1. Navigate to **Configuration > Wireless > Access Points** Select the Access Point.



2. Navigate to **Edit AP > Advanced**. Choose the Antenna Band Mode, then click **Update & Apply to Device** to save the configuration in the AP.



Checking the Antenna Band Mode

Check CAPWAP AP Antenna Band Mode on controller using the following CLI:

```
WLC#show ap name <Cisco AP> config general | inc Antenna Band
For example:
WLC#show ap name ape8eb-349c-14c0 config general | inc Antenna Band
Antenna Band Mode: Single
```

Check AP Antenna Band Mode on WIM by using the following CLI. The band mode is shown by the GPIO value:

```
AP#show capwap client config | inc GPIO
For example:
AP84EB.EF55.1498#show capwap client config | inc GPIO
GPIO_34: 0
GPIO_35: 1
```

Note GPIO_34:1 & GPIO_35:0 is dual band mode. GPIO_34:0 & GPIO_35:1 is single band mode.

Configuring Flexible Antenna Port For WGB

To configure WGB Antenna Band Mode on WIM by CLI, use one of the options in the example below:

```
WGB#configure wgb antenna band mode
  dual    Configure WGB antenna dual band
  single  Configure WGB antenna single band
```

For example:

```
AP84EB.EF55.1498#configure wgb antenna band mode single
[*10/24/2023 22:55:04.7280] Antenna band mode configuration has been saved successfully

AP84EB.EF55.4E53#configure wgb antenna band mode dual
[*10/24/2023 22:57:14.3470] Antenna band mode configuration has been saved successfully
```

To check WGB Antenna Band Mode on WIM by CLI, use the **show running-config | inc Antenna** CLI:

```
AP84EB.EF55.1498#show running-config | inc Antenna
Antenna Band Mode          : Single

AP84EB.EF55.4E53#show running-config | inc Antenna
Antenna Band Mode          : Dual
```