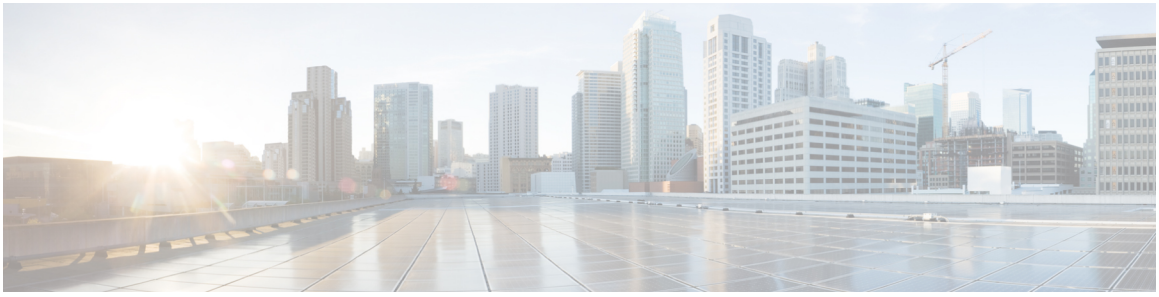
Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.12.1

First Published: 2023-07-31

Last Modified: 2025-07-31

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

Preface

This preface describes this guide and provides information about the configuration of URWB on Cisco Catalyst Industrial Wireless access points, and related documentation.

It includes the following sections:

About this Guide

This guide details the configuration of the URWB mode of operation for the Catalyst IW9167 and IW9165 access points. UWRB is supported as part of the Unified Industrial Wireless (UIW) software. UIW release 17.12.1 introduces new features for the Catalyst IW9167E as well as support for the Catalyst 9165 series access points. Support for URWB on the Catalyst IW9167E access point was previously introduced in UIW release 17.11.1.

Related Documentation

Documentation for the access point control and provisioning of wireless access points (CAPWAP) and workgroup bridge (WGB) modes of operation for Catalyst IW9167 are available in the following URL:

https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.

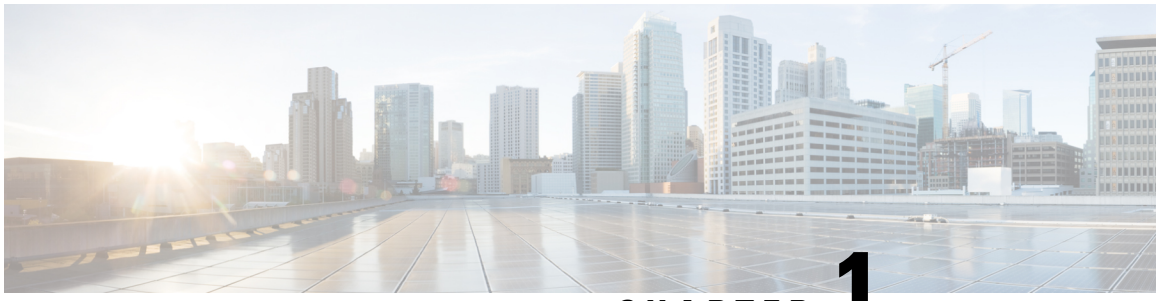
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

Overview of Cisco Catalyst IW9167E and IW9165 Access Points

Overview of Cisco Catalyst IW9167E and IW9165 Access Points

Overview of Cisco Catalyst IW9167E

The Catalyst IW9167E access point provides reliable wireless connectivity for mission-critical applications in a state-of-the art platform to deliver a network that is more reliable and secure, with higher throughput, more capacity, and less device interference. The Catalyst IW9167E is Cisco's first outdoor Wi-Fi 6E ready Access Point supporting tri-radio and tri-band (2.4/5/6 GHz bands). The Catalyst IW9167E can operate in Wi-Fi (control and provisioning of wireless access points (CAPWAP)) mode or Ultra-Reliable Wireless Backhaul (URWB) mode and URWB software on Catalyst IW9167E designed to support the Cisco style parser.

Overview of Cisco Catalyst IW9165

The Catalyst IW9165 supports up to a 3.6 Gbps PHY data rate with two 2x2 multiple input and multiple output (MIMO) and two ethernet ports (2.5 mGig and 1G). The Catalyst IW9165 uses Cisco Ultra-Reliable Wireless Backhaul (URWB), which offers seamless handoffs, low latency, and high availability. The Catalyst IW9165 is designed to take advantage of the 6 GHz band expansion to deliver a network that is more reliable and secure, with higher throughput, more capacity, and less device interference. The Catalyst IW9165 has the option to switch images by just updating the software to operate the Catalyst IW9165 in workgroup bridge (WGB) or URWB mode without changing the hardware.

The Catalyst IW9165 series is available in two models:

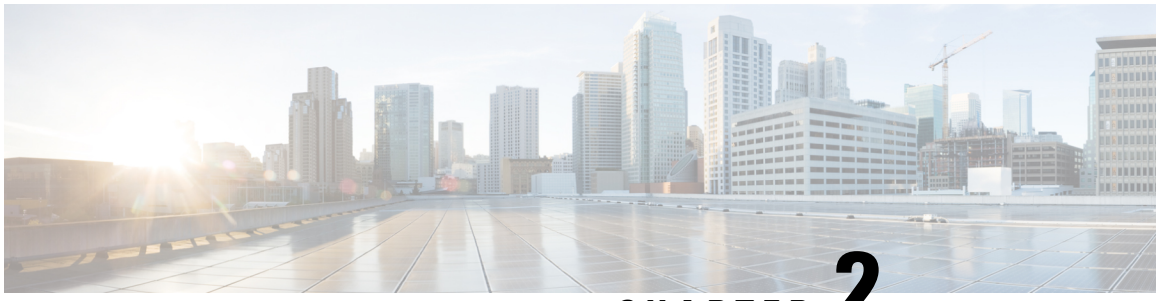
- Catalyst IW9165E Rugged Access Point and Wireless Client
- Catalyst IW9165D Access Point

Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

The Catalyst IW9165E supports a 2x2 Wi-Fi 6E design with external antennas, and it is designed to add ultra-reliable wireless connectivity to moving vehicles and machines. Low power consumption, rugged IP30 design and small form factor make the Catalyst IW9165E very simple to integrate into industrial assets.

Cisco Catalyst IW9165D Access Point

The Catalyst IW9165D supports a 2x2 Wi-Fi 6E design with internal and external antennas, and it is designed to simplify wireless backhaul deployment. The Catalyst IW9165D is designed with heavy-duty IP67 and a built-in directional antenna that enables long-range, high-throughput connectivity when fiber is not an option, so that you can create a fixed wireless infrastructure (point-to-point, point-to-multipoint, and mesh) as well as backhaul traffic from mobile devices along wayside or trackside deployments. The external antenna ports let you quickly extend your network to new places when needed and choose the right antenna based on the use cases and deployment architectures.



CHAPTER 2

Device Initial Configuration in Provisioning Mode

Provisioning mode

From UIW Release 17.16.1, IoT OD IW is changed and called as IW Service.Catalyst IW access point (AP) running in URWB mode supports configuration either from:

- Online Cloud-Managed: configure the device using Industrial Wireless (IW) Service, or
- Offline: configure the device using local management interfaces (GUI or CLI).

By default, an AP with no configuration starts in Provisioning mode. In this mode, the IW Service provides the initial configuration.

How Provisioning mode works

In Provisioning mode, an AP attempts to request the network configuration using DHCP and then connects to the IW Service.

- If network connectivity exists, AP connects to the IW Service.
  - Configure AP using the IW Service: If the AP obtains network connectivity, it attempts to connect to IW Service. IW Service uses DNS geo-location to direct APs to the appropriate cluster (US or EU). Ensure your IW Service organization is configured to the correct cluster.
- If there is no network connectivity, AP can be configured locally. Local management can be accessible using the console port or SSH.
  - Configure AP using the Local configuration: If network connectivity is unavailable, the AP can be configured locally via GUI or CLI, accessible through the console port or SSH.

Use these default credentials to log either into the GUI or CLI:

- Username: Cisco
- Password: Cisco

Handling DHCP and IP Address in Provisioning mode

When the device is in Provisioning mode, it tries to get an IP address from DHCP. If this process fails or DHCP is unavailable, these options apply:

- If the device fails to receive an IP address through DHCP, it switches to the fallback IP address:192.168.0.10/24.
- If DHCP is unavailable and configuration through IW Service is needed, then you can manually configure the IP address, subnet, default gateway, and DNS.

Note DHCP is used only during provisioning mode. For regular tasks, use a static IP address.

Configure fallback IP address using GUI

Perform this task to configure a fallback IP address that the device will use if it fails to obtain an IP address from the DHCP server. This ensures continued device operation in the absence of dynamic IP assignment.

Before you begin

The fallback IP address acts as a static IP address that the device defaults to when DHCP fails to assign one. This feature is critical for maintaining connectivity in scenarios where the DHCP server is unavailable.

Procedure

Step 1 Launch the computer's web browser and enter the URL to open the URWB configurator login page.

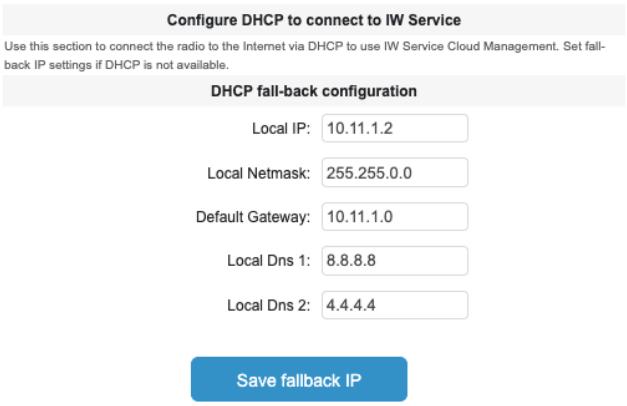
Step 2 Enter the username and password in the respective fields.

Step 3 Click **Login**.
After successfully logging into the GUI, the URWB configurator page is displayed.

Step 4 Click **IW Service** on the URWB configurator page and navigate to **Configure DHCP to connect to IW Service** section.

Step 5 Enter the appropriate IP addresses in the respective fields:

- Fallback Local
- Local Netmask
- Default Gateway
- Local Primary DNS
- Local Secondary DNS



Step 6 Click **Save fallback IP** to complete the configuration.

Configure fallback IP address using CLI

Before you begin

When an AP fails to obtain an IP address from a DHCP server, it reverts to a pre-configured fallback IP address.

Procedure

Perform this task to configure fallback IP address on the AP.

Use the `configure ap address ipv4 static` *`IP address`*`static netmask` *`IP address`* `of gatewaydns1 ip` *`IP address`*`dns2 ip` *`IP address`*command to configurefallback IP address on the device.

```
Device#configure ap address ipv4 [ static IP address [ static netmask [ IP address of default gateway
 [ dns1 ip [ dns2 ip ] ] ] ] ]
```

Example:

```
Device#configure ap address ipv4 static 192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200
192.168.10.201
```

Configure the AP using GUI (Offline)

Procedure

Step 1 Launch the computer's web browser and enter the URL to open the URWB configurator login page.

Step 2 Enter the username and password in their respective fields.

Step 3 Click **Login**.
After successfully logging into the GUI, the URWB configurator page is displayed.

Step 4 Click **IW Service**.
IW Service Configuration Mode page appears.

Step 5 Select **Offline**.
The device exits from Provisioning mode and switch to Fallback IP address.

Configure the AP using IW Service (Online Cloud-Managed)

This task explains how to configure the access point in online cloud-managed mode through the IW Service. This mode allows the device to be managed from the IW Service cloud server if connected to the internet.

Procedure

Step 1 Launch the computer's web browser and enter the URL to open the URWB configurator login page.

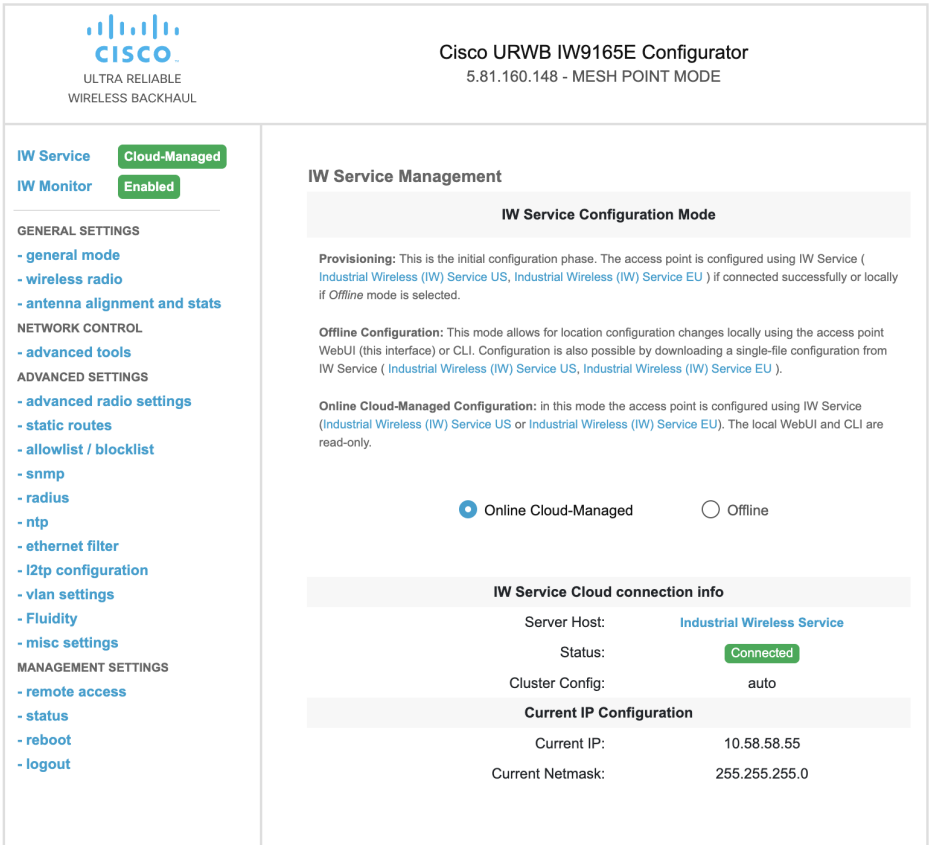
Step 2 Enter the username and password in their respective fields.

Step 3 Click **Login**.
After successfully logging into the GUI, the URWB configurator page is displayed.

Step 4 Click **IW Service**.
IW Service Configuration Mode page appears.

Step 5 By default, the device is shown as Online Cloud-Managed.

The device can be managed from IW Service cloud server (if it is connected to the internet). The device exits Provisioning mode only if the user pushes the configuration from IW service or switches to offline mode.



The device exits provisioning mode only when the configuration is pushed from IW Service or the mode is switched to offline.

Verify the AP status using GUI

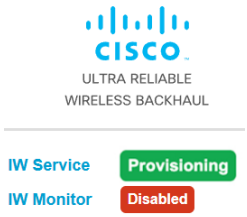
Procedure

Step 1 Launch the computer's web browser and enter the URL to open the URWB configurator login page.

Step 2 Enter the username and password in their respective fields.

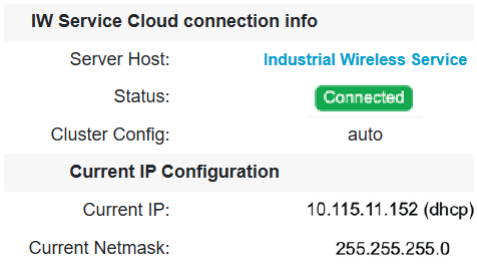
Step 3 Click **Login**.
After successfully logging into the GUI, the URWB configurator page is displayed.

- Provisioning mode



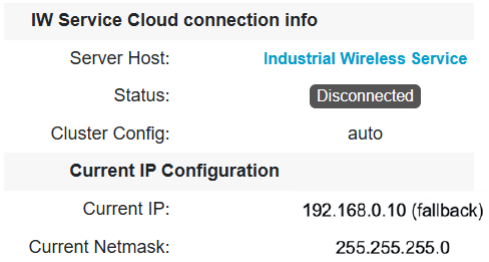
- Device configurator in connected status

  If the connection to IW Service is successful, status is shown as **Connected**.



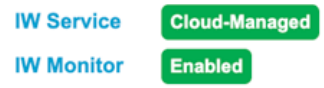
- Device configurator in disconnected status.

  If the connection to IW Service is failed, status is shown as **Disconnected**.



- **Offline mode**

- **Online cloud-managed**



Verify the AP status using CLI

Use this task to verify the current operational status of an AP within the URWB configurator.

Procedure

Use the `show iw-service status` command to verify the status of the device.

```
Device#show iw-service status
```

Example:

- Device in Provisioning mode

```
Device#show iw-service status

IW Service mode: Provisioning

Status: Connected
```

- Device in Offline mode

```
Device#show iw-service status

IW Service mode: Offline
```

- Device in Online Cloud-Managed

```
Device#show iw-service status

IW Service mode: Online Cloud-Managed

Status: Connected
```

Verify DHCP connection status using CLI

Procedure

Step 1 This CLI example shows that the device is in provisioning mode and retrieved the IP address from the DHCP server:

Use the `show ip` to view the status of DHCP.

- Example: DHCP Success

```
Device#show ip


IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers:
```

```
DHCP Address (PROVISIONING Mode):

IP: 10.0.0.2

Network: 255.255.255.0

Gateway: 10.0.0.1

Nameservers: 8.8.8.8

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

Step 2 This CLI example shows the device is in provisioning mode fails to retrieve the IP address from the DHCP server and then device uses the default fallback IP address 192.168.0.10:

Use the `show ip` to view the status of DHCP.

- Example: DHCP Failure (uses default Fallback IP)

```
Device#show ip

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers:

DHCP Address (PROVISIONING Mode):

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers: 127.0.0.1

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

LED behavior

The device's status LEDs blink continuously in a repeating cycle until the device enters a fallback condition, online cloud-managed mode, or offline mode. Refer to "LED Pattern for Catalyst IW9165" or "LED Pattern for Catalyst IW9167" for specific LED patterns.

Troubleshoot IW Service connectivity in Provisioning mode

If the device fails to connect to IW Service, try these steps:

Procedure

Step 1 Physical Connection: Verify the Ethernet cable is correctly connected.

Step 2 DNS Resolution: Ensures

- device.ciscoiot.com
- us.ciscoiot.com
- eu.ciscoiot.com

Step 3 Outbound HTTPS: Confirm the access point allows outbound HTTPS connections on tcp/443 for the domains listed in step2.

Step 4 Local Configuration: If IW Service remains offline, perform a local (offline) configuration using the device's configurator interface.

Reset the Device to Factory Default using GUI

You can reset the device to factory default either by pressing a reset button for 30 seconds when power is supplied to the access point or through configurator interface. For more information about reset button, see Using the Reset Button.

Note A hard reset reverts all device configuration settings, including the device IP address and administrator password to factory defaults. Instead if you want to reboot the device, see Reboot the Device using GUI, on page 13.

1. In the **MANAGEMENT SETTINGS**, click **reset factory default**.

2. Click **YES** in the confirmation pop-up window. To abort the factory reset, click **NO**.
3. If you have previously saved a configuration file for the device, you can restore the saved configuration settings to the device, see Save and restore the device settings, on page 13.

Note Do not perform a hard reset unless the device requires reconfiguration using its factory configuration as the starting point. Hard reset resets the device's IP address, administrator password, and it disconnects the device from the network.

Reset the Device to Factory Default using CLI

To reset of the device configuration, use the following CLI command:

```
device#configure factory reset config
WARNING: "configure factory reset config" will clear config and reboot.
Do you want to proceed? (y/n)
```

Enter `y` in the CLI command to start the device reset process or alternatively enter `n` to abort the process.

To reset the device configuration and data wipe, use the following CLI command:

```
Device#configure factory reset default
WARNING: "configure factory reset default" will take minutes to perform DATA WIPE.
```

The following files are cleared as part of this process:

```
1) Config, Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
```

```
5) Pktlogs
6) Manually created files
Do you want to proceed? (y/n)
```

Enter `y` in the CLI command to start the device reset of the configuration and data wipe or alternatively enter `n` to abort the process.

Reboot the Device using GUI

To reboot the device's operating system, follow these steps:

1. In the **MANAGEMENT SETTINGS**, click **reboot**.

2. In the confirmation pop-up window, click **Yes**. To abort the reboot, click **No**.

Reboot the Device using CLI

To perform reboot, use the following CLI command:

```
Device#reload
Proceed with reload command (cold)? [confirm]
```

Enter `confirm` in the CLI command to start the device reboot process.

Save and restore the device settings

The **LOAD OR RESTORE SETTINGS** window allows you to perform the following tasks:

- Save the device's existing software configuration as a configuration (*.conf) file.
- Upload and apply a saved configuration file to the current device.

Note Device software configuration (*.conf) files are not interchangeable with IoT OD configuration setup (*.iwconf) files.

Tip Saved configuration files are reused for all devices of the same type. These saved configuration files act as configuration backup files to speed up redeployment if you need to replace the damaged device with a new device of the same type.

To download the device's existing configuration settings to your computer, follow these steps:

1. In the **MANAGEMENT SETTINGS**, click **configuration settings**.

   The **LOAD OR RESTORE SETTINGS** window appears.

2. Click **Save** to download the device configuration (*.conf).

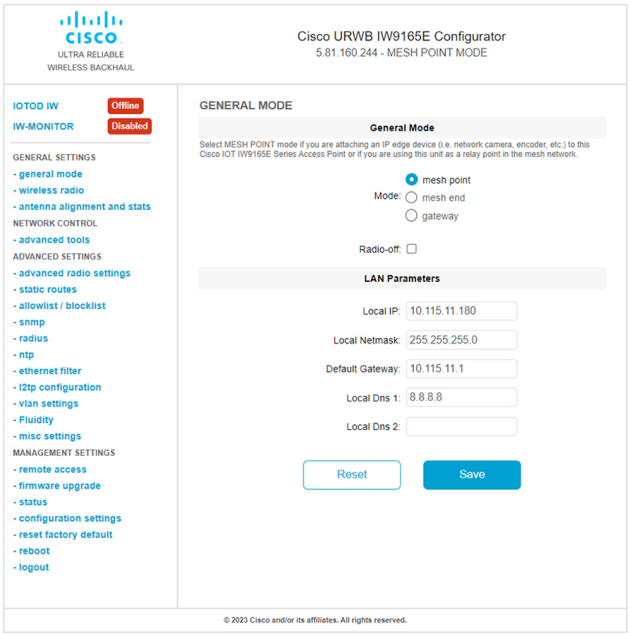
To upload a saved configuration file to the device, follow these steps:

1. Click **Browse** to upload the configuration (*.conf) file to the device.
2. Click **Restore** to apply the configuration settings to the device.

Configure general settings

To change the **General Mode** settings, follow these steps:

1. In the **GENERAL SETTINGS**, click **general mode**.



The **General Mode** has the operational mode controls. Devices capable of operating in a mesh radio network are shipped in **mesh point** mode.

Note When designing the required network layout, there must be at least one mesh end device. This device performs control and administrative functions, such as license management. This is necessary for correct network operation, even if the network consists of only two devices.

To change the device's operational mode, select any one of the following mode:

- **Gateway** - This mode is applicable for advanced Layer 3 mobility deployments, and it is not used in most networks.
- **Mesh Point** - This mode is applicable for the remaining access points in the network. These access points establish links to other access points with the same network passphrase configured as mesh end or mesh point using wireless links or wired links. In this scenario, the access point has Layer 2 visibility of other access points.
- **Mesh End** - This mode configures the access point to perform control and administrative network functions. There must be at least one mesh end in each network. This access point is typically installed in the most central point where the wireless and wired networks converge.

Configure general settings using CLI

To configure general settings, use the following CLI command:

```
Device#configure modeconfig mode
  gateway    layer 3 global gateway mode
  meshend    mesh end mode
  meshpoint  mesh point mode
```

```
Device#configure modeconfig mode meshend
  mpls       MPLS support
  radio-off  disable radio interfaces
```

Change the LAN parameters

The LAN parameters has entry controls for local address setting. Perform the following to change the LAN parameters:

1. Once the **General Mode** window is opened for the first time, the **Local IP** and **Local Netmask** LAN parameters are shown with factory-set default values.
2. If needed, enter the local primary DNS address in the **Dns 1** field, and enter the local secondary DNS address in the **Dns 2** field.
3. Click **Save** to save the LAN settings. To clear the settings, click **Reset**.

Configure LAN parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

```
device#configure ip address ipv4 static
192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200 192.168.10.201
```

Connect to the Access Point Console Port

To configure the access point locally (without connecting to a wired LAN), connect the computer to the access point's console port using a DB-9 to RJ-45 serial cable and to open the CLI by connecting to the access point's console port, follow these steps:

1. Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.
2. Set up a terminal emulator to communicate with the access point. In the terminal emulator, use the following settings:

Parameter	Value
Baud rate	115200 bps
Data	Eight bits
Parity	No
Stop	One stop bit
Flow Control	No

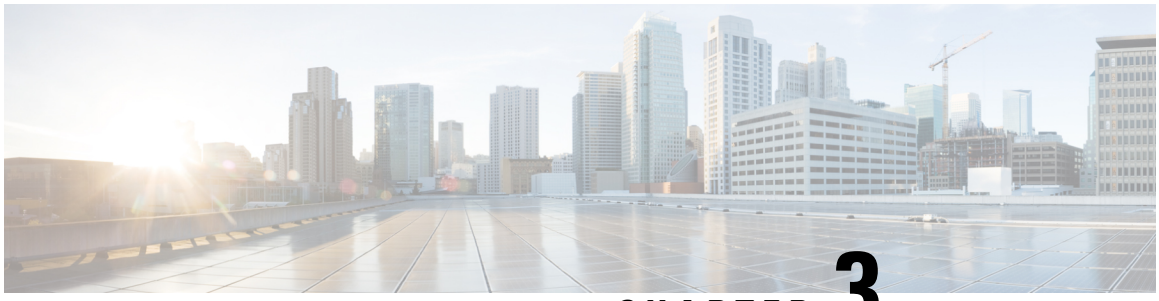
3. There are two available command-prompt modes: standard command prompt (>) and privileged command prompt (#). When logged in for the first time, it directs you to standard command prompt (>) mode to execute unprivileged commands.

   To access privileged command-prompt (#) mode, enter the enable command (abbreviated as en) and enter the enable password (the privilege mode login password is different from the standard login password).

Use these default credentials to log in:

- Username: Cisco
- Password: Cisco

Note Once the initial configuration completes, ensure to remove the serial cable from the access point.



CHAPTER 3

Upgrade the Device using GUI

Upgrade the device using GUI

Procedure

Step 1 Launch the computer's web browser and enter the URL to open the URWB configurator login page.

Step 2 Enter the username and password in their respective fields.

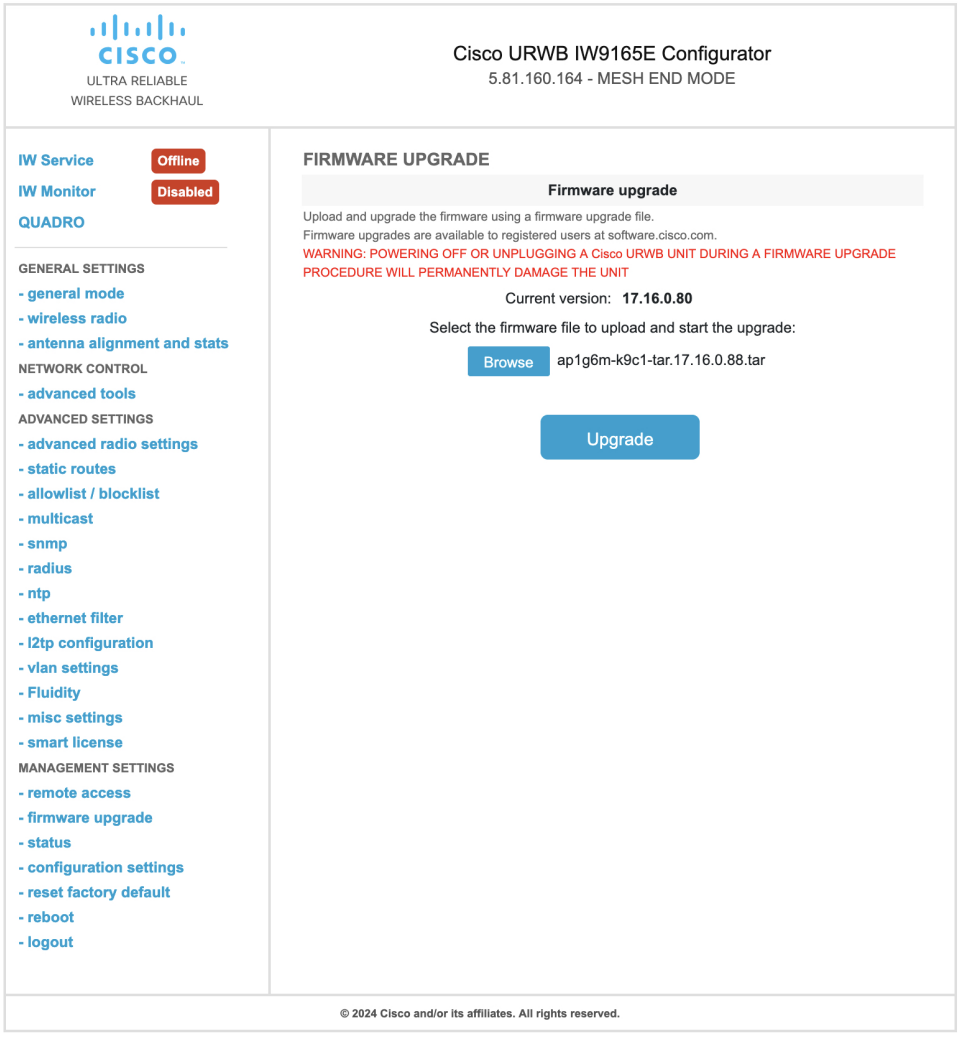
Step 3 Click **Login**.
After successfully logging into the GUI, the URWB configurator page is displayed.

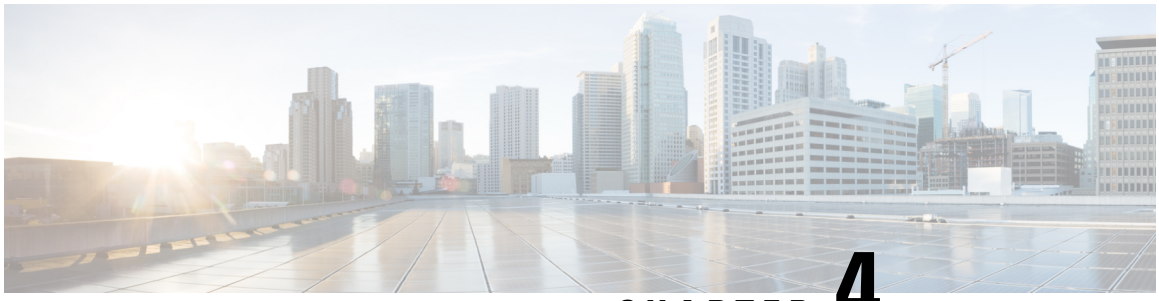
Step 4 In the **MANAGEMENT SETTINGS**, click the **firmware upgrade** link to open the **FIRMWARE UPGRADE** window.

Step 5 Click the **Browse** button to locate and select the firmware upgrade file.

Step 6 Click the **Upgrade** button to initiate the upgrade process.

Step 7 Click **OK** to confirm uploading the firmware file to the device.
Once the firmware is successfully uploaded to the device, the AP verifies the image and then reboots.


ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9165E Configurator
5.81.160.164 - MESH END MODE
IW Service
Offline
IW Monitor
Disabled
QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
FIRMWARE UPGRADE
Firmware upgrade
Upload and upgrade the firmware using a firmware upgrade file.
Firmware upgrades are available to registered users at software.cisco.com.
WARNING: POWERING OFF OR UNPLUGGING A Cisco URWB UNIT DURING A FIRMWARE UPGRADE PROCEDURE WILL PERMANENTLY DAMAGE THE UNIT
Current version: 17.16.0.80
Select the firmware file to upload and start the upgrade:
Browse
ap1g6m-k9c1-tar.17.16.0.88.tar
Upgrade
© 2024 Cisco and/or its affiliates. All rights reserved.



CHAPTER 4

Configuring URWB Operation Mode

Configuring URWB Operation Mode

Catalyst Industrial Wireless access points support multiple wireless technologies, such as Catalyst Wi-Fi (AP), Cisco Ultra-Reliable Wireless Backhaul (URWB), and Workgroup Bridge (WGB). The modes supported vary by specific access point.

The access point OS supports two different software images: Catalyst Wi-Fi (AP) and Unified Industrial Wireless (UIW). Both URWB and WGB are part of the UIW software. The access point mode is determined at boot time based on the mode the access point is configured to operate in.

Determining from CLI

The access point OS supports two different software images: Catalyst Wi-Fi (AP) and UIW. Use the following show command to determine which software is running and look for the indicated platform code:

```
Device# show version
Cisco AP Software, (ap1g6j), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu Aug 18 01:01:29 PDT 2022
ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100
APFC58. 9A16.E464 uptime is 1 days, 3 hours, 58 minutes
Last reload time : Wed Sep 7 11:17:00 UTC 2022
Last reload reason: reload command
```

If the show version displays `ap1g6a` or `ap1g6b`, it means that the access point OS is running. If the show version displays `ap1g6j` or `ap1g6m`, it means the UIW software is running.

To check if the access point is running in URWB mode, use the following CLI command:

```
Device#show iotod-iw status
```

If the command exists, then the access point is running in URWB mode, otherwise the access point is running in WGB mode.

Reset Button Settings

The following reset actions are performed in the URWB mode when the LED turns to blinking red (after the boot loader gets the reset signal). Ensure you to press the device's reset button before the device is powering on.

- If you press the reset button for < 20 seconds, it clears the existing configuration.
- If you press the reset button for > 20 seconds and < 60 seconds, it triggers the factory reset.
- If you press the reset button for > 60 seconds, it does not clear the configuration.

Configuring Image Conversion

To convert a Catalyst IW9167E access point either from Wi-Fi mode (CAPWAP AP) to URWB mode or from URWB mode to Wi-Fi mode (CAPWAP AP), follow these steps:

1. To convert from CAPWAP to URWB mode or from WGB/uWGB to URWB mode, use the following CLI command. The access point then reboots and starts up in URWB mode.

   ```
   configure boot mode urwb
   ```

2. To convert from URWB to CAPWAP mode or from WGB/uWGB to CAPWAP mode, use the following CLI command. The access point then reboots and starts up in CAPWAP mode.

   ```
   configure boot mode capwap
   ```

3. To convert from CAPWAP to WGB/uWGB mode or from URWB to WGB/uWGB mode, use the following CLI command:

   ```
   configure boot mode wgb
   ```

Note Image conversion performs a full factory reset which completely erases the configuration and data.

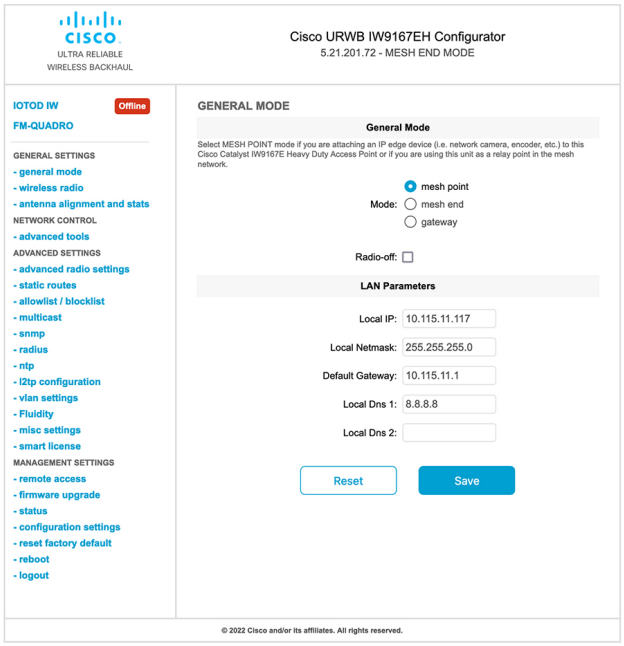
Instructions to Access the GUI

To access the Web UI (Web User Interface), use the following procedure:

1. To access a Web UI, open the web browser and enter the following URL: https://<IP address of unit>/

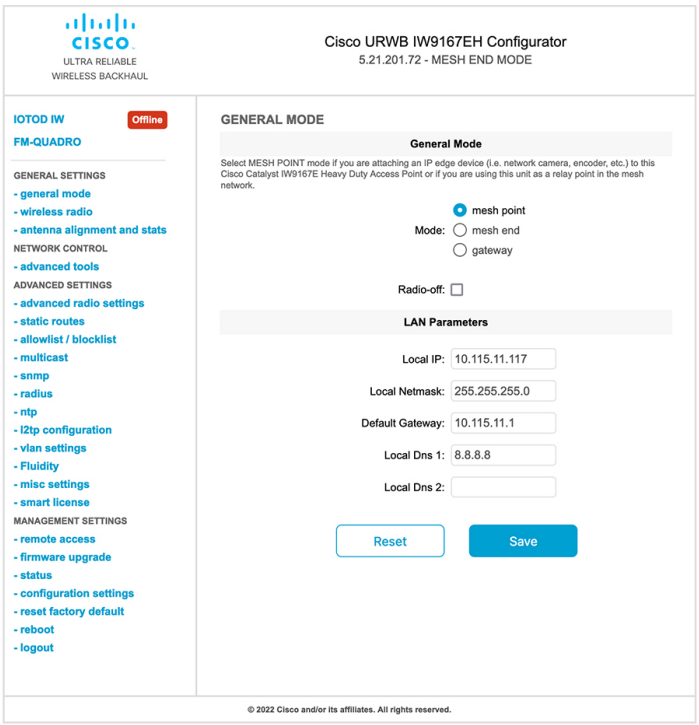
   The **IW9167E or IW9165 Configurator** window appears.

2. To access the configuration page, use the credentials as follows: **Username** and **Enable password**.
3. Once you successfully log into the GUI, the URWB configurator displays:



URWB Catalyst IW9167E Configuration using GUI

The following image shows the configuration of the Catalyst IW9167E configurator:



Committing CLI Configuration

To save the current or running configuration settings to local storage or memory, type `write` CLI command. The modified value is in the cache configuration file, once the `write` command is entered, re-boot the device to take effect of the current configuration. To make the configuration effective, use the following CLI commands:

```
Device# write
```

or

```
Device# wr
```

write or wr: commit the current configuration settings to memory.

```
Device# reload
```

reload: reload the device.

Example:

```
Device# write
!!! Please reboot to take effect
Device# reload
```

Proceed with reload? [confirm]

(enter to confirm)

Configure IoT OD IW Online and Offline Mode using CLI

IoT OD is the cloud management portal, and the device is connected to the online through the cloud network. In offline mode the device is configured in local mode using CLI and GUI, and it is not connected to the cloud.

When the device is configured in offline mode, choose following options:

- Configure the device manually using CLI and GUI.
- Configure the device on IoT OD cloud service and select the configuration file exported from IoT OD and upload the configuration file using upload configuration button at the end of IoT OD management page.

To activate or deactivate IoT OD configuration capability, use the following CLI command:

```
Device#configure iotod-iw {offline | online}
```

Online - To set up IoT OD mode to online . The device can be managed from IoT OD cloud server (if it is connected to the network).

Offline - To set up IoT OD mode to offline. The device is disconnected from IoT OD and must be manually configured using the CLI, or offline configurator interface.

Configuring Password (after first login) using CLI

Once the device switches to offline mode (after the initial login), you need to set up new login credential. To configure login credentials using GUI or CLI, the login credentials should follow these criteria:

- The username length must be between 3 to 32 characters long.
- The password length must be between 8 to 32 characters long.
- The password must include the following:
  - At least one uppercase letter
  - At least one lowercase character,
  - At least one digit
  - At least one special character
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not allowed:

  " [double quote]

  ' [single quote]

  ? [question mark]
- The password must not contain:
  - Three sequential characters or digits (ABC/ CBA)
  - The same three characters or digits consecutively (AAA) or (666)

- Same as the current or existing password
- Same as or the reverse of the username

Example:

Default credentials:

```
username: Cisco
password: Cisco
enable password: Cisco
```

To reset the credentials, use the following sample credentials:

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

Example of configuring password using CLI:

```
Device#configure iotod-iw {offline}
Switching to IOTOD IW Offline mode...
Will switch from Provisioning Mode to IOTOD IW offline Mode, device need to reboot:Y/N?
Y
User access verification.
[Device rebooting...]

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

After first login, reset the credentials:

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

Once the credentials are changed, re-login:

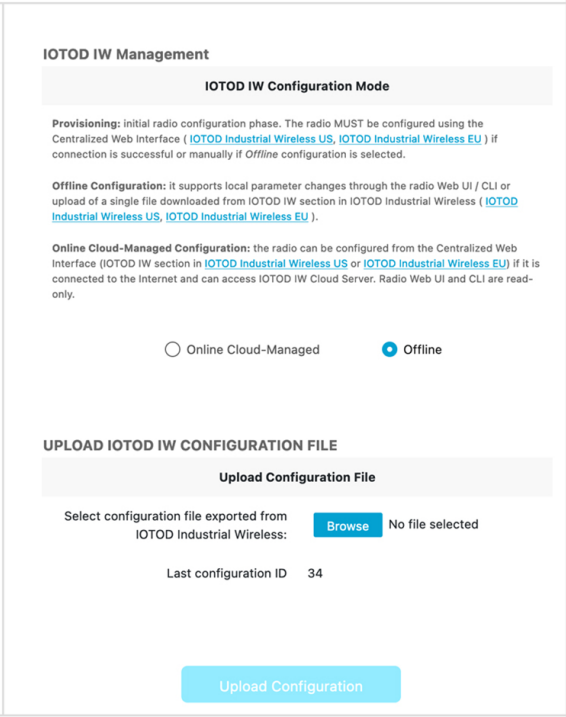
```
User access verification
Username: demouser
Password: DemoP@ssw0rd
Device> enable
Password:DemoE^aP@ssw0rd
```

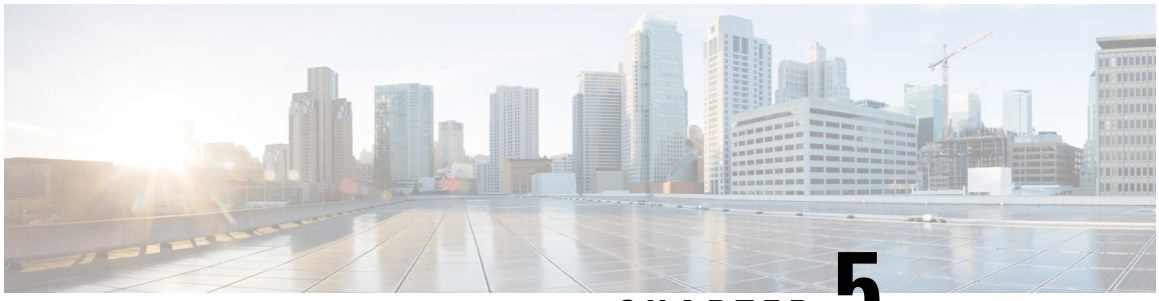
```
Device#
```

Note In the above example, all passwords are in plain text. This is for demo purposes (sample credential). In the real scenario, they are hidden behind asterisks (*).

Configure IoT OD IW using GUI

This image shows the configuration of IoT OD:





CHAPTER 5

Configuring URWB Radio Mode

Configuring URWB Radio Mode

The wireless interfaces are configured to operate in a specific mode, or you can disable it. Once you configure the Radio mode, the device starts working as a Fluidity or Fixed infrastructure.

The following table shows the configuration of Radio mode on the device:

Table 1: Radio Mode Configuration

Radio Role	Radio Mode	Description
Fixed Infrastructure	Fixed Fluidmax primary Fluidmax secondary	P2P mode (point to point) P2MP (point to multipoint) mode (Fluidmax) and P2MP P2MP mode (Fluidmax) and P2MP
Mobility AP	Fluidity	Mobility mode
Mobility Client	Fluidity	Mobility mode

Following table shows the Fluidity status and it is derived from operating mode of enabled radio interfaces:

Table 2: Operating Mode of Radio Interface

Radio 1 / Radio 2	Fixed Infrastructure	Fluidity
Fixed Infrastructure	Fluidity disabled	Fluidity enabled
Fluidity	Fluidity enabled	Fluidity enabled

Multiple and dual radio interfaces are possible based on the following table:

Table 3: Configuration of Multiple Radio interfaces

Radio 1 / Radio 2	Fixed Infrastructure / Mesh	Mobility AP	Mobility client
Fixed Infrastructure / Mesh	ME/MP relay, P2MP (mesh)	Yes, trailer use case (Mining trailer)	Supported but no specific use case
Mobility AP	Yes, trailer use case (Mining trailer)	Standard Fluidity (multiple clients on each radio)	Not supported, use V2V or Fixed + AP
Mobility client	Supported but no specific use case	Not supported, use V2V or Fixed + AP	Standard Fluidity (multiple clients on each radio)

Configuring Radio-off Mode from CLI

To configure Radio-off mode when both radios (Fluidity and fixed) are disabled, use the following CLI commands and procedure:

Note If you specify radio-off, the device disables all the wireless interfaces.

1. Set the device's current operating mode. Mode could be mesh end, mesh point or global gateway (L3).

   ```
   Device# configure modeconfig mode {meshpoint | meshend | gateway}
   ```

2. Set the device's selected Multi-Protocol Label Switching (MPLS) OSI layer and the possible value of layer is 2 (OSI Layer-2) or 3 (OSI Layer-3).

   ```
   Device# configure modeconfig mode {meshpoint | meshend | gateway}[layer {2|3}]
   ```

3. To set the radio-off mode.

   ```
   Device# configure modeconfig mode { meshpoint | meshend | gateway } [layer {2|3}] [
   radio-off {fluidity | fixed}]
   ```

4. To end the current configuration, use the following CLI command:

   ```
   Device# (configure modeconfig mode { meshpoint | meshend | gateway } [layer {2|3}] [
   radio-off {fluidity | fixed}])# end
   ```

```
Device# wr
```

Example:

```
Configure modeconfig mode meshend radio-off fluidity
Configure modeconfig mode meshend radio-off fixed
```

Configuring Radio Mode for URWB from CLI

To configure Radio mode for URWB, use the following CLI commands:

To select the operating function of the wireless interface, use these CLI commands. Device allows mixed Fluidity and fixed infrastructure combinations for different interfaces.

1. Configure the wireless with radio interface number <1 or 2>.

   ```
   Device# configure dot11Radio <interface>
   ```

2. Configure an operating mode for the specified interface.

   ```
   Device# configure dot11Radio <interface> mode {fixed|fluidity|fluidmax}
   ```

   Fluidity - This interface operates the device in Fluidity, either as a mobility infrastructure or as a vehice mode.

   Fixed - This interface operates in fixed infrastructure mode (no Fluidity).

   Fluidmax - This interface operates in Fluidmax P2MP mode. More parameters can be specified to configure the Fluidmax operating features, for example: Primary/Secondary role and cluster ID.

3. Set Fluidmax role for Fluidmax interface mode.

   ```
   Device# configure dot11Radio <interface>mode {fixed|fluidity|fluidmax} {primary |
   secondary}
   ```

   Primary - set Fluidmax role to primary

   Secondary - set Fluidmax role to secondary

4. To end the current configuration, use the following CLI command:

   ```
   Device (configure dot11Radio <interface>mode{fixed|fluidity|fluidmax}) # end
   Device# wr
   ```

Note When at least one interface is set to Fluidity mode, the device operates globally in Fluidity mode. If all interfaces are set to fixed, Fluidity is disabled.

Configuring AMPDU from CLI

To configure an aggregated MAC protocol data unit's (ampdu) length and priority, use the following CLI commands:

```
Device# configure dot11radio <interface> ampdu length <length>
```

length: <0-255> integer number – microseconds.

```
Device# configure dot11radio <interface> ampdu priority {enable | disable}
```

enable: enable ampdu tx priority.

disable: disble ampdu tx priority.

```
Device# configure dot11radio <interface> ampdu priority [enable]
```

0: ampdu tx priority for index 0.

1: ampdu tx priority for index 1.

2: ampdu tx priority for index 2.

3: ampdu tx priority for index 3.

4: ampdu tx priority for index 4.

5: ampdu tx priority for index 5.

6: ampdu tx priority for index 6.

7: ampdu tx priority for index 7.

all: ampdu tx priority for all indexes (index 0 to 7)

Configuring Frequency from CLI

To configure an operating frequency, use the following CLI command:

```
Device# configure dot11radio <interface> frequency <frequency>
```

frequency: <0-7125> operating frequency in MHz

Configuring Maximum Modulation Coding Scheme Index from CLI

To configure maximum modulation coding scheme (MCS) index, use the following CLI command:

```
Device# configure dot11radio <interface> mcs <maxmcs>
```

Set maximum MCS index in integer or string AUTO. For AUTO, the background process automatically configures the maxmcs.

Maxmcs values:

< 0-11 > Maximum mcs index 0 to 11.

Word AUTO

Note If High Efficiency mode is disabled, set the MCS index value ranging from zero to nine. If High Efficiency mode is enabled, set the MCS index value as 10 or 11.

Configuring Maximum Number of Spatial Streams Index from CLI

To configure maximum number of spatial streams (NSS) index, use the following CLI command:

```
Device# configure dot11radio <interface> spatial-stream <maxnss>
```

Set maximum spatial stream number in integer or string AUTO. For AUTO, the background process automatically configures the maxnss.

Maxnss values:

< 1-4 > Maximum nss index 1 to 4.

Word AUTO

Note Catalyst IW9165 supports up to two spatial streams and Catalyst IW9167 supports up to four spatial streams. The maximum number of spatial streams configured must be same or less than the number of antennas enabled.

Configuring Rx-SOP Threshold from CLI

To configure receiver start of packet (Rx-SOP) threshold, use the following CLI command:

```
Device# configure dot11radio <interface> rx-sop-threshold
```

<0 - 91> Enter rx-sop- threshold (0: AUTO, VALUE: -VALUE dBi).

Configuring RTS Mode from CLI

To disable ready to send (RTS) mode, use the following CLI command:

```
Device# configure dot11radio <interface> rts <disable>
```

Disable: Disables the RTS protection.

To enable RTS with threshold value, use the following CLI command:

```
Device# configure dot11radio <interface> rts enable <threshold>
```

Threshold: Threshold range <0 - 2346>.

Configuring WMM Mode from CLI

To configure wireless multimedia (WMM) mode, use the following CLI command:

```
Device# configure dot11radio <interface> wmm [bk|be|vi|vo]
```

[bk|be|vi|vo]: Represents the class-of-service (CoS) parameters.

be: Best-effort traffic queue (CS0 and CS3).

bk: Background traffic queue (CS1 and CS2).

vi: Video traffic queue (CS4 and CS5).

vo: Voice traffic queue (CS6 and CS7).

To clear wireless stats counters, use the following CLI command:

```
Device# configure dot11Radio <interface> wifistats <clear>
```

Clear: Clear wireless stats counters.

Configuring NTP from CLI

To configure the NTP server address, use the following CLI command:

```
Device# configure ntp server <string>
```

String - IP address or domain name.

Example:

```
Device# configure ntp server 192.168.216.201
```

To configure the NTP authentication, use the following CLI command:

```
Device# configure ntp authentication none
Device# configure ntp authentication md5 <password> <keyid>
Device# configure ntp authentication sha1 <password> <keyid>
```

none - disable the NTP authentication md5|sha1 - authentication method.

Example:

```
Device# configure ntp authentication md5 test1234 65535
```

Note Optional, the md5 password and keyid should match NTP server's md5 password and keyid.

To configure a new password using a GUI or CLI, the password should match the following criteria:

- The password length range is from 8 to 20 characters.
- The following special characters are not allowed:
  - ' (apex)
  - " [double apex]
  - ` [backtick]
  - $ [dollar]
  - = [equal]
  - \ [backslash]
  - # [number sign]
  - whitespace

To enable or disable the NTP service, use the following CLI command:

```
Device# configure ntp { enable|disable }
```

To configure the NTP timezone, use the following CLI command:

```
Device# configure ntp timezone <string>
```

Example:

```
Device# configure ntp timezone Asia/Shanghai
```

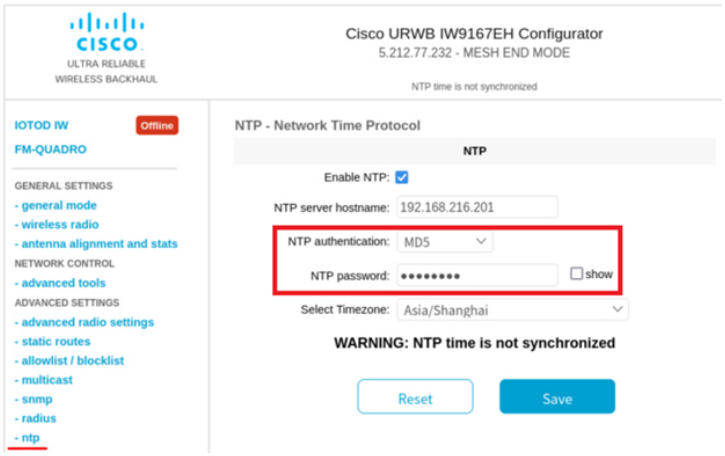
To validate the NTP configuration and status, use the following show commands:

```
Device# show ntp config
NTP status: enabled
NTP server: 192.168.216.201
authentication: MD5
password: test123
keyid: 5
timezone: Asia/Shanghai

Device# #show ntp (Using this command to check if device can sync up time with NTP server)
Stratum Version Last Received  Delay    Offset  Jitter    NTP server
1          4      9sec ago    1.840ms -0.845ms 0.124ms 192.168.216.201
```

Configuring NTP using GUI

The following image shows the GUI of NTP:



Validating Radio Mode for URWB

To validate Radio mode, use the following show commands:

```
Device# show dot11Radio <interface> config
```

Example:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
```

```
Channel : 157
Channel width : 40 MHz
```

```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
```

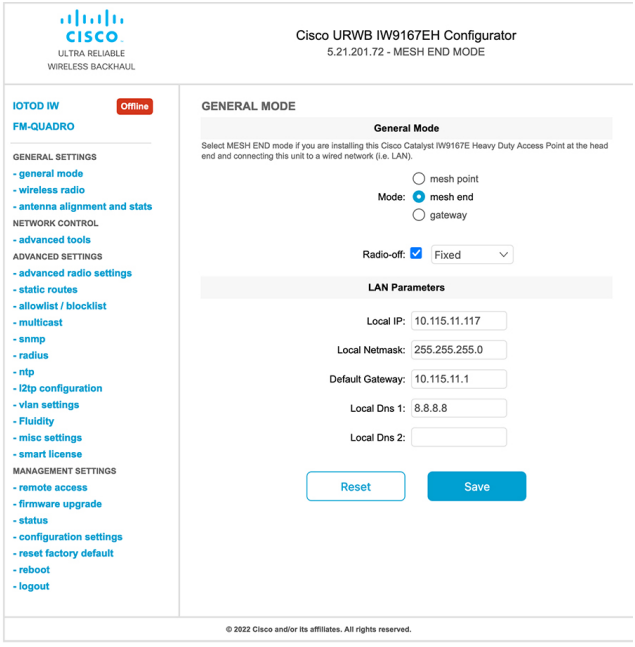
To change the Radio mode of vehicle access point (mobility client) to Fixed or Fluidmax, configure Fluidity role as infrastructure using CLI:

```
Device# configure fluidity id infrastructure
```

.

Configuring Radio-off Mode using GUI

To configure **Radio-off** mode, choose either **Fixed** or **Fluidity** mode as shown. Select mode as **mesh end**, if you are installing the Catalyst IW9167E access point at the head end and connecting this device to a wired network such as LAN.

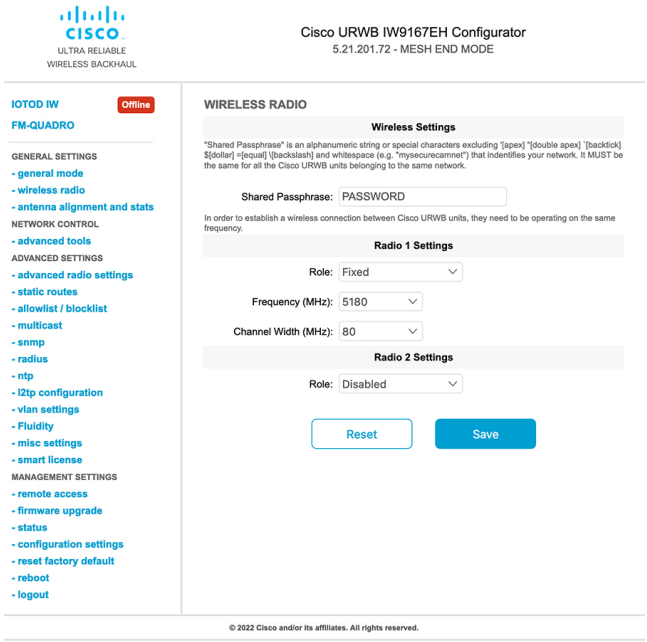


Configuring Radio Mode using GUI

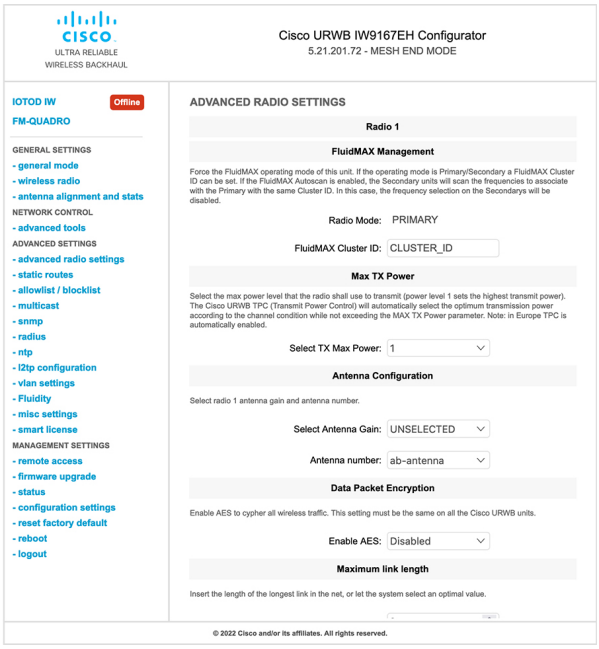
To establish a wireless connection the operating frequency should be same between the devices.

To configure a Radio mode using GUI, follow these steps:

1. Set the operating mode for specified radio (Radio1 and Radio2) interface.

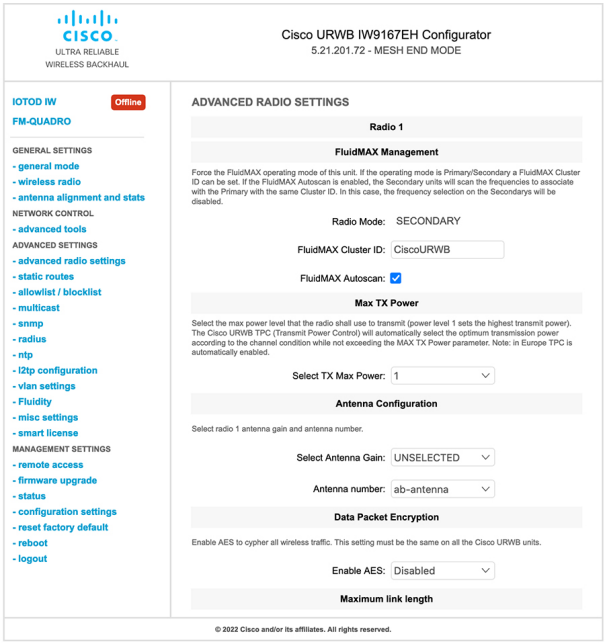


2. In the **WIRELESS RADIO** section, choose Radio 1 Role as **Fluidmax Primary** with FluidMAX Cluster ID. In this scenario, the frequency selection for the Primary is enabled and Secondary is disabled. In the **ADVANCED RADIO SETTINGS** window, go to **Max TX Power** section, and choose power level as 1 from the **Select TX Max Power** drop-down list and URWB transmission power control (TPC) automatically selects the optimum transmission power.



Note In Europe TPC is automatically enabled.

3. In the **WIRELESS RADIO** section, choose Radio 1 Role as **Fluidmax Secondary** with FluidMAX Cluster ID. In the **ADVANCED RADIO SETTINGS**, if you check the **FluidMAX Autoscan** check box, the secondary devices scan the frequencies to associate with the Primary with the same Cluster ID. In this case the frequency selection on the Secondary is in disable mode. In the **Max TX Power** section, and choose power level as 1 from the **Select TX Max Power** drop-down list and URWB TPC automatically selects the optimum transmission power.



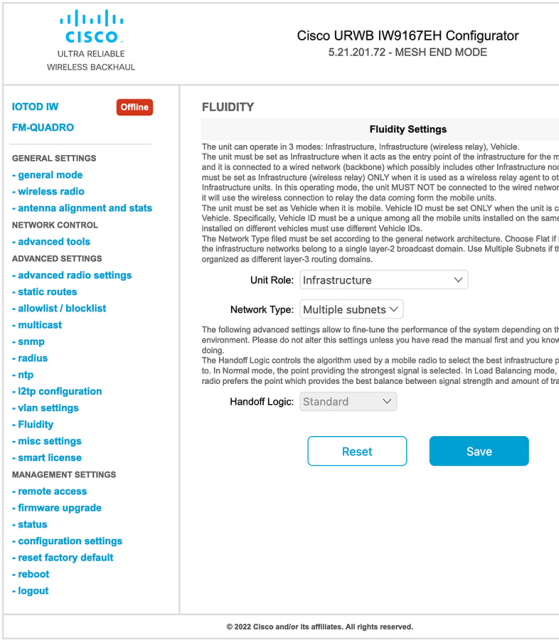
Note In Europe TPC is automatically enabled.

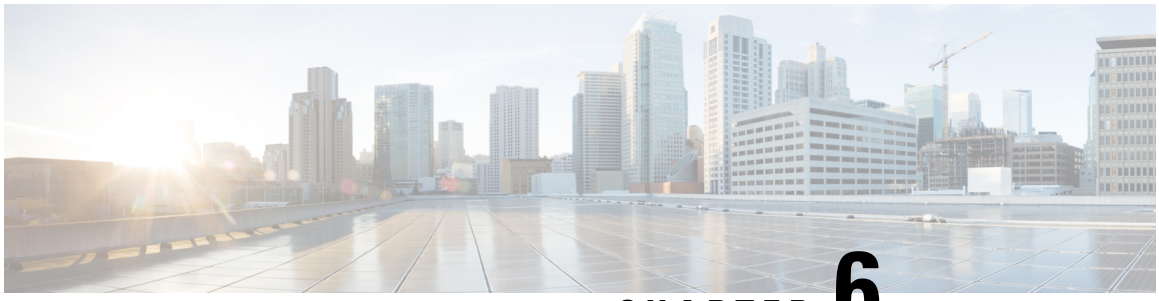
4. In the **Fluidity Settings** section, choose **Unit Role** as **Infrastructure** from the drop-down list, When the device acts as the entry point of the infrastructure for the mobile vehicles or choose unit role as **Infrastructure (wireless relay)** only when it used as a wireless relay agent to other infrastructure unit or choose unit role as a **Vehicle** when it is mobile.
5. Choose network type based on the to the general network architecture:
   a. Choose **Flat** mode from **Network Type** drop-down list, if the network belongs to single layer-2 broadcast domain.

      or

   b. Choose **Multiple subnets** if the network belongs to single layer-3 broadcast domain.


CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
IOTOD IW
Offline
FM-QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
WIRELESS RADIO
Wireless Settings
"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
Shared Passphrase: PASSWORD
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.
Radio 1 Settings
Role: Fluidity
Frequency (MHz): 5180
Channel Width (MHz): 80
Radio 2 Settings
Role: Disabled
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.


CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
IOTOD IW
Offline
FM-QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
FLUIDITY
Fluidity Settings
Unit Role: Infrastructure
Network Type: Multiple subnets
Handoff Logic: Standard
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.



CHAPTER 6

Configuring Radio Antenna Settings

Configuring Radio Antenna Settings

The Catalyst IW9167E supports eight external antennas with eight N-type female connectors to support multiple antenna options. The antenna ports 1, 4, and 5 can support self-identifying antennas (SIA). Radio 1 connects to ports 1 to 4, and Radio 2 connects to ports 5 to 8. For more information on antennas, see Antennas and Radios.

The Catalyst IW9165E supports four external antennas with Reverse-polarity SMA (RP-SMA) (f) connectors. Radio 1 connects to antenna ports 1 and 2, Radio 2 connects to antenna ports 3 and 4, and antenna ports 1 and 3 can support SIA antennas.

The Catalyst IW9165D has a built-in directional antenna and supports two external antennas with N-type (f) connectors. Radio 1 connects to the internal antenna. Radio 2 connects to antenna ports 1 and 3. Antenna port 3 can support SIA antenna.

The following sections describe the CLI commands to manage antenna port and gain on each antenna for different Radio mode:

Configuring Antenna Gain

To configure an antenna gain, use the following CLI command:

Set the maximum antenna gain value in integer or string UNSELECTED.

For UNSELECTED, the background process automatically configures the minimum supported antenna gain.

Note Once the SIA is connected, gain sets automatically without any input.

```
Device# configure dot11radio <interface> antenna gain <gain>
gain:
<1-19> antenna gain in dBi
WORD UNSELECTED
Device# write
```

Configuring Transmit and Receive Antennas

To configure a transmission chain, use the following CLI command:

Note Catalyst IW9165 does not support abcd-antenna mode.

```
Device# configure dot11radio <interface> antenna < A >
configure antenna chains (A) in use as follows
a-antenna - configure dot11 antenna a
ab-antenna - configure dot11 antenna ab
abcd-antenna - configure dot11 antenna abcd
Device# write
```

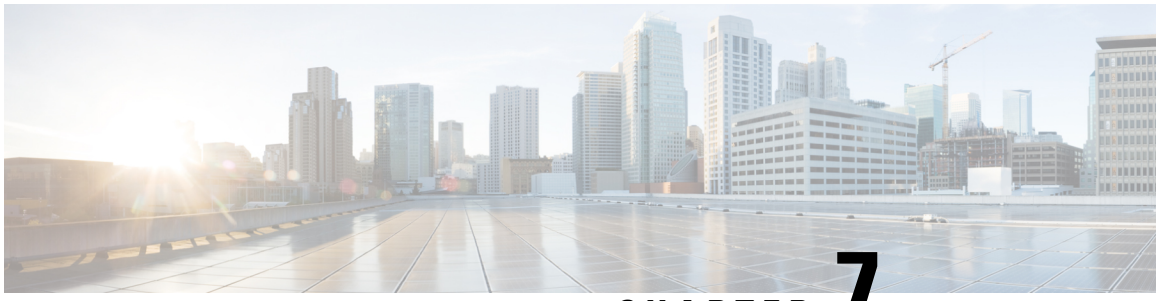
Configuring Transmission Power

To configure a transmission power, use the following CLI command:

Set the maximum transmission power level. For AUTO, the background process automatically configures the maximum allowed power level one.

Note Eight is the lowest power level and one is the highest power level.

```
Device# configure dot11radio <interface> txpower-level <level>
txpower level:
<1-8> tx power level value
WORD AUTO
Device# write
```



CHAPTER 7

Configure and validate radio channel and bandwidth

Configuring Operating Channel from CLI

To configure operating channel, use the following CLI commands:

1. Configure the wireless device with radio interface number < 1 or 2 >

   ```
   Device# configure dot11Radio <interface>
   ```

2. Set the operating channel id and the valid range is from 1 to 256

   ```
   Device# configure dot11Radio <interface> channel <channel id>
   ```

3. To end the current configuration, use the following CLI command:

   ```
   Device (configure dot11Radio <interface> channel <channel id>)# end
   ```

   Example:

   ```
   Device# configure dot11Radio [1|2] channel <1 to 256>
   ```

Configure channel bandwidth from CLI

1. Configure the wireless device with radio interface number <1 or 2>.

   ```
   Device#configure dot11Radio <interface>
   ```

2. Set channel bandwidth in MHz.
   - Radio 1 supports 20, 40, and 80 MHz bandwidths.
   - Radio 2 supports 20, 40, 80, and 160 MHz bandwidths.

```
Device#configure dot11Radio [1|2] band-width [20|40|80|160]
```

3. Returns to privileged EXEC mode.

```
Device (configure dot11Radio [1|2] band-width [20|40|80|160])#end
```

Validating operating channel and bandwidth from CLI

To validate radio channel and bandwidth, use the following show command:

```
Device# show dot11Radio <interface> config
```

Example:

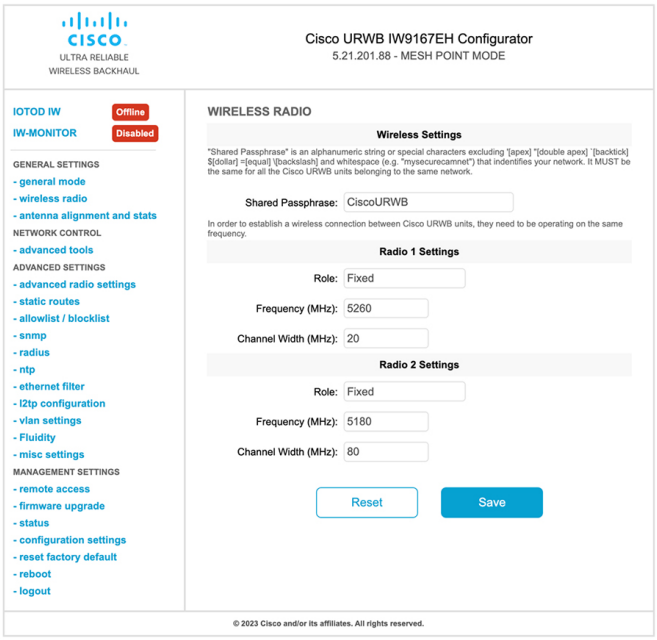
```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz

Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
Channel : 157
Channel width : 40 MHz
```

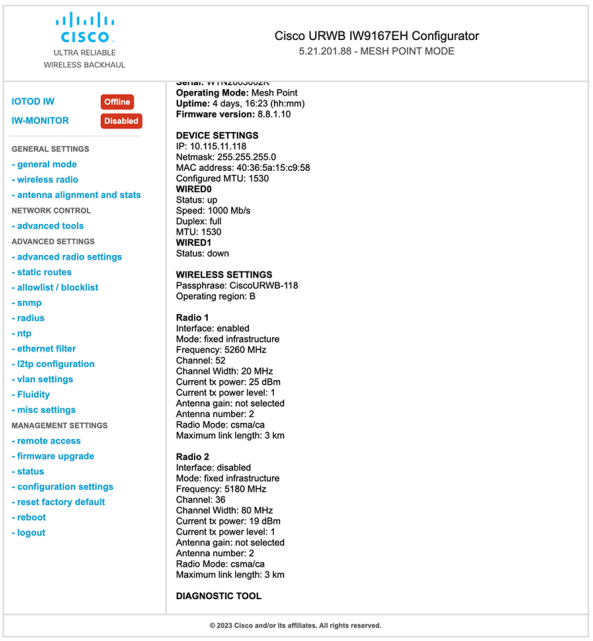
Configure radio channel and bandwidth from GUI

To configure Radio channel and bandwidth using GUI, set the operating channel ID, Radio mode as Fluidity or fixed infrastructure and set the Radio frequency range and bandwidth.

Following image shows the configuration of Radio channel and bandwidth:



Following image shows the status of Radio channel and bandwidth configuration and specific information of each wireless interface.



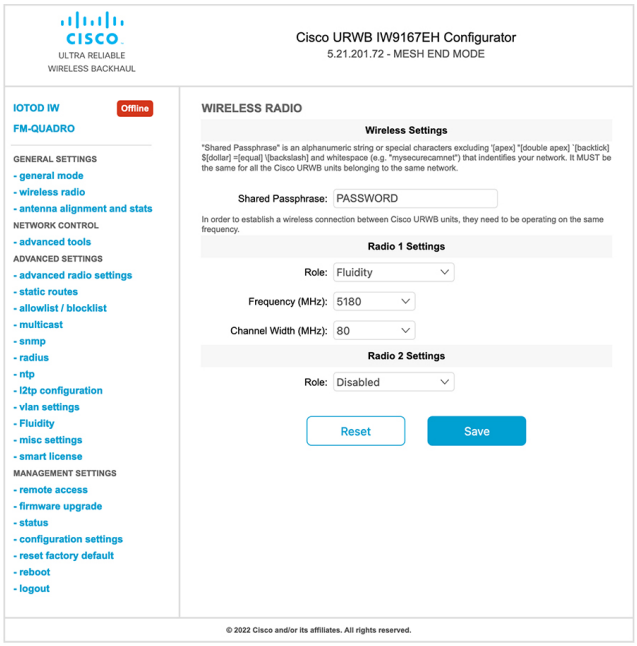
Configure Fluidity using GUI

To configure a Fluidity mode using GUI, follow these scenarios:

1. In the **GENERAL SETTINGS**, click **wireless radio**.

The **WIRELESS RADIO** window appears.

2. Choose Radio mode as **Fluidity** from the **Role** drop-down list.



Once you choose Radio role as **Fluidity**, go to **Fluidity** settings. To go to Fluidity, follow these steps:

1. In the **ADVACED SETTINGS**, click **Fluidity**.

   The **FLUIDITY** window appears.

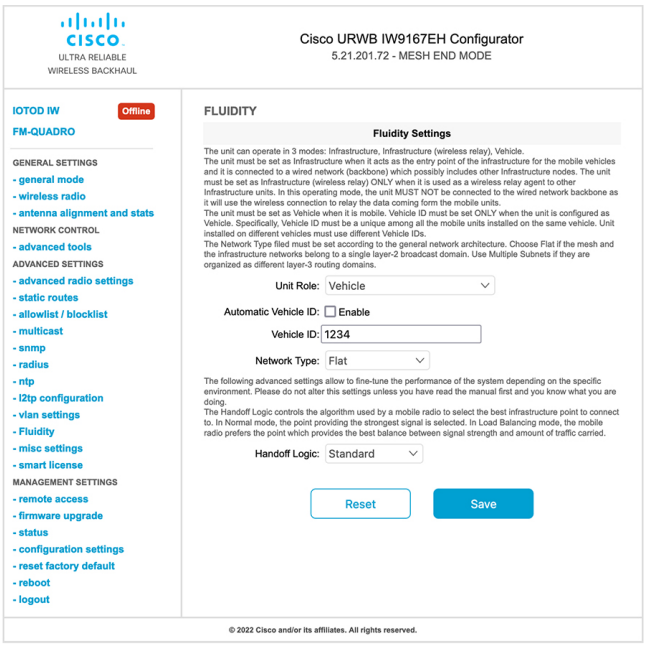
2. In the **Fluidity Settings**, choose **Unit Role** from the drop-down list. Make device role as any one of following mode:

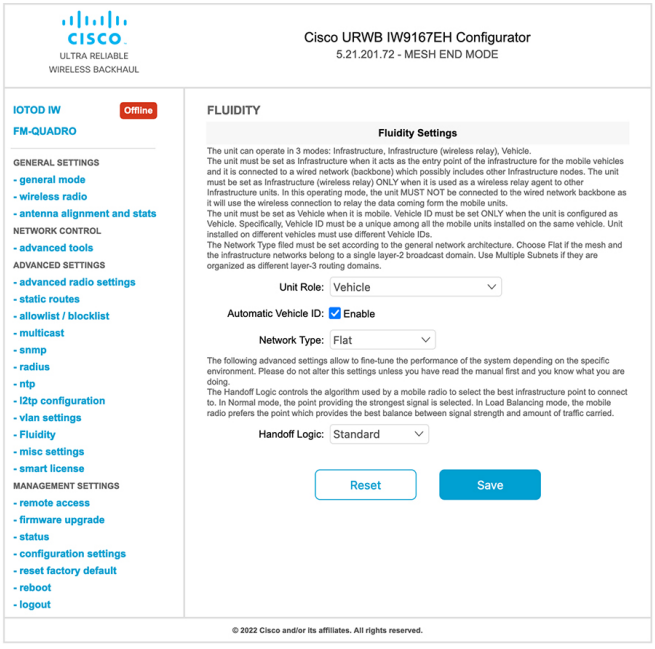
   - Infrastructure
   - Infrastructure (wireless relay)
   - Vehicle

Note

- Vehicle ID must be unique among all the mobile devices installed on the same vehicle.
- If the device installed on different vehicles must use different Vehicles IDs'.

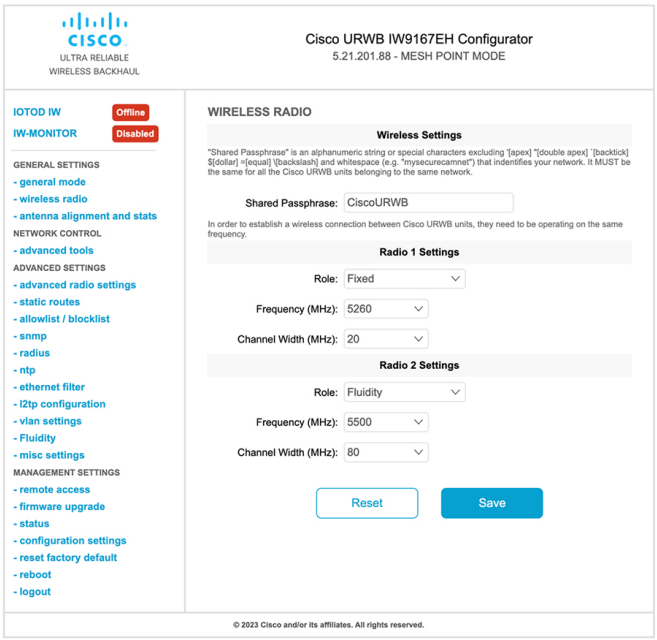
3. Check the **Automatic Vehicle ID** check box to automatically set Vehicle ID for mobile units.

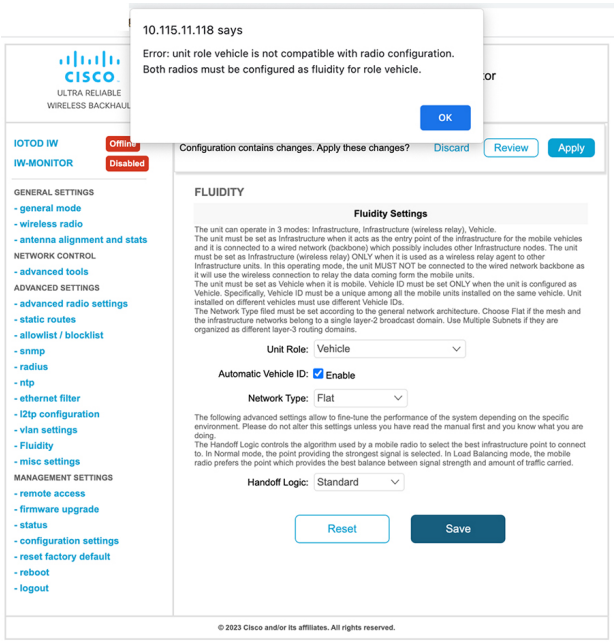




Following Fluidity configuration shows wireless interface device role configured as infrastructure mode:

The following image shows, both radios must be configured as Fluidity for role Vehicle. if one wireless interface is configured in fixed mode and the other one is configured in Fluidity mode then unit role Vehicle cannot be selected.





Configure fluidity using CLI

To enable Fluidity, use the following CLI commands:

Note At least one radio interface should be in Fluidity mode.

```
Device# configure dot11Radio <interface> mode fluidity
```

Example to enable Fluidity for radio 1:

```
configure dot11Radio 1 mode fluidity
```

If the desired Fluidity role is Vehicle both radios should be in Fluidity mode:

```
configure dot11Radio 1 mode fluidity
configure dot11Radio 2 mode fluidity
```

Configuring fluidity role using CLI

To configure Fluidity role (infra or client), use the following CLI commands:

1. Configure the Fluidity role (infrastructure or mobile).

   ```
   Device# configure fluidity id
   ```

2. Configure Fluidity id mode.

   ```
   Device# configure fluidity id {mode}
   Mode is one of the following values
   vehicle-auto - vehicle mode with automatic vehicle ID selection
   vehicle ID - (alphanumeric) vehicle mode with manual ID.
   infrastructure - infrastructure mode
   wireless-relay - wireless infrastructure with no ethernet connection to the backhaul
   ```

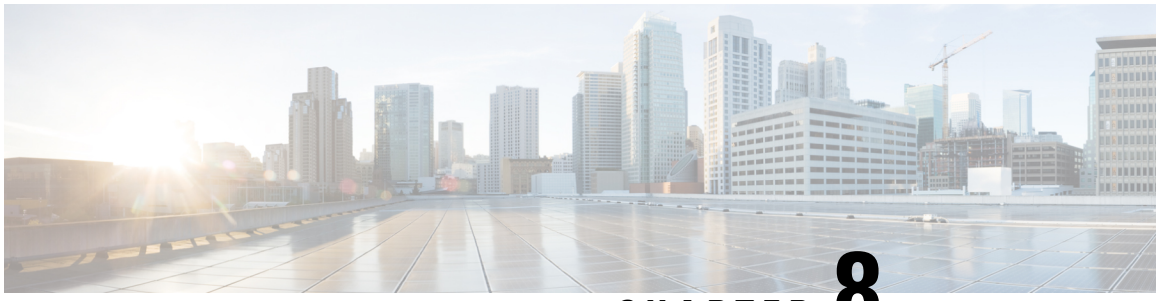
3. To end this configuration, use the following CLI command:

   ```
   Device (configure fluidity id {mode}) # end
   ```

   ```
   Device# wr
   ```

   Example:

   ```
   Device# configure fluidity id [vehicle-auto | infrastructure | vehicle-id |
   wireless-relay]
   ```



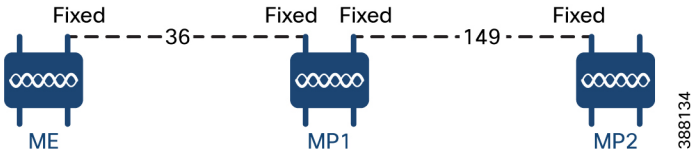
CHAPTER 8

Configuring and Validating of Point-to-Point Relay Topology

Configuring and Validating of Point-to-Point Relay Topology

The following image shows two radio interfaces on a single device (MP1) to implement a point-to-point relay topology:

Figure 1: point to point relay topology



To configure point-to-point relay topology, follow these scenarios:

1. Configure Mesh End (ME), MP1 on channel 36 and MP2 on the default channel 149.
2. Continue from step 1 configuration.
3. Enable the second slot interface on Mesh Point (MP2) again and wait 30 seconds to implement the point-to-point relay topology for two radio interfaces on a single device.

Configuring Point to Point Relay Topology from CLI

To configure a point-to-point relay topology, use the following CLI commands:

1. Configure the wireless device with radio interface number <1 or 2>.

   ```
   Device# configure dot11Radio <interface>
   ```

2. Set wireless interface admin state to enable or disable mode.

```
Device# configure dot11Radio <interface> > {enable | disable}
```

3. Configure an operating mode for the specified interface (fixed or Fluidity or Fluidmax).

```
Device# configure dot11Radio <interface> > [enable | disable] mode { fluidity | fixed |
 fluidmax }
```

4. Set the operating channel for the specified interface and the operating channel id valid range is between 1 to 256.

```
Device# configure dot11Radio <interface> > [enable | disable] mode [fluidity | fixed |
fluidmax] channel <channel id>
```

5. To end this configuration, use the following CLI command:

```
Device (configure dot11Radio <interface> > {enable | disable} mode {fluidity | fixed |
fluidmax} channel <channel id>) #end
```

Example:

```
Device#configure dot11Radio <2> {enable | disable} mode {fluidity} channel <36>
```

Example for point-to-point relay topology configuration:

Mesh End (ME) Configuration

```
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fixed
Device#configure dot11Radio 2 channel 36
```

Mesh Point (MP1) Configuration

```
Device#configure fluidity id infrastructure
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fixed
Device#configure dot11Radio 1 channel 36
Device#configure dot11Radio 2 enable
Device#configure dot11Radio 2 mode fixed
Device#configure dot11Radio 2 channel 149
```

MP2 Configuration

```
Device#configure fluidity id infrastructure
Device#configure dot11Radio 1 enable
Device#configure dot11Radio 1 mode fixed
Device#configure dot11Radio 1 channel 149
```

Validating Point to Point Relay Topology from CLI

To validate point-to-point relay topology configuration, use the following show commands:

```
Device# show dot11Radio <interface> config
```

Mesh End (ME) Statistics

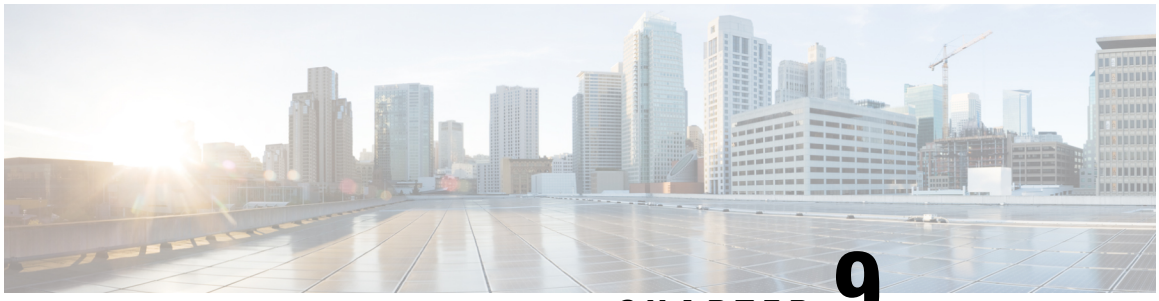
```
Device#show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

Mesh Point (MP1) Statistics

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

MP2 Statistics

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
```



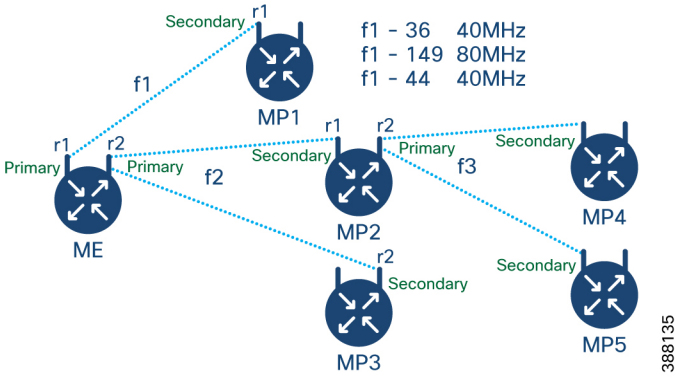
CHAPTER 9

Configure and Validate Fluidmax Topology

Configure and Validate Fluidmax (point to multipoint) Topology

For fixed infrastructure, any wireless interface can be configured to operate in Fluidmax mode to implement point-to-multipoint connections. Each interface uses an independent set of Fluidmax parameters, allowing for great flexibility in the network topologies that can be implemented. As an example, the below image explains two cascaded point-to-multipoint clusters where the ME (Mesh End) node uses both radios in Fluidmax Primary mode to serve several secondary clients (MP1 (Mesh Point), MP2, and MP3) on two different frequencies. For MP2, the first radio operates in Fluidmax secondary mode to connect to the ME, while the second interface is configured as Fluidmax Primary to serve more downstream clients (MP4 and MP5).

Figure 2: Two cascaded Fluidmax Topology



Configuring Point to Multipoint Topology from CLI

To configure a Fluidmax (point to multipoint) Topology use the following commands.

```
Device# configure dot11Radio <interface>
```

Interface - <0-3> Dot11Radio interface number.

```
Device# configure dot11Radio <interface> {enable | disable}
```

Enable or disable - Set wireless interface admin state to enable or disable at runtime

```
Device# configure dot11Radio <interface> mode {fluidity | fixed | fluidmax } { primary |
secondary }
```

Mode - operating mode for the specified interface (Fluidity or fixed or Fluidmax)

Primary | secondary - Fluidity, Fixed and Fluidmax role for the unit, either primary or secondary.

```
Device# configure dot11Radio <interface> channel <channel id>
```

Channel - Set the operating channel id <1 – 256>.

```
Device# configure dot11Radio <interface> band-width <channel bandwidth>
```

Bandwidth - channel bandwidth in MHz and currently supported values are 20, 40, 80, 160.

```
Device#wr
```

Example of point to multipoint (Fluidmax) topology configuration

ME (Mesh End) Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax primary
Device# Configure dot11Radio 1 channel 36
Device# Configure dot11Radio 1 band-width 40
Device# Configure dot11Radio 2 enable
Device# Configure dot11Radio 2 mode fluidmax primary
Device# Configure dot11Radio 2 channel 149
Device# Configure dot11Radio 2 band-width 80
```

MP1 (Mesh point) Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax secondary
Device# Configure dot11Radio 1 channel 36
Device# Configure dot11Radio 1 band-width 40
```

MP2 Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax secondary
Device# Configure dot11Radio 1 channel 149
Device# Configure dot11Radio 1 band-width 80
Device# Configure dot11Radio 2 enable
Device# Configure dot11Radio 2 mode fluidmax primary
Device# Configure dot11Radio 2 channel 44
Device# Configure dot11Radio 2 band-width 40
```

MP3 Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax secondary
Device# Configure dot11Radio 1 channel 149
Device# Configure dot11Radio 1 band-width 80
```

MP4 Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax secondary
Device# Configure dot11Radio 1 channel 44
Device# Configure dot11Radio 1 band-width 40
```

MP5 Configuration

```
Device# Configure dot11Radio 1 enable
Device# Configure dot11Radio 1 mode fluidmax secondary
Device# Configure dot11Radio 1 channel 44
Device# Configure dot11Radio 1 band-width 40
```

Validate Point to Multipoint Topology using CLI

Use this command to validate the point-to-multipoint (Fluidmax) topology configuration.

```
Device# show dot11Radio <interface> config
```

Example:

ME (Mesh End) radio2

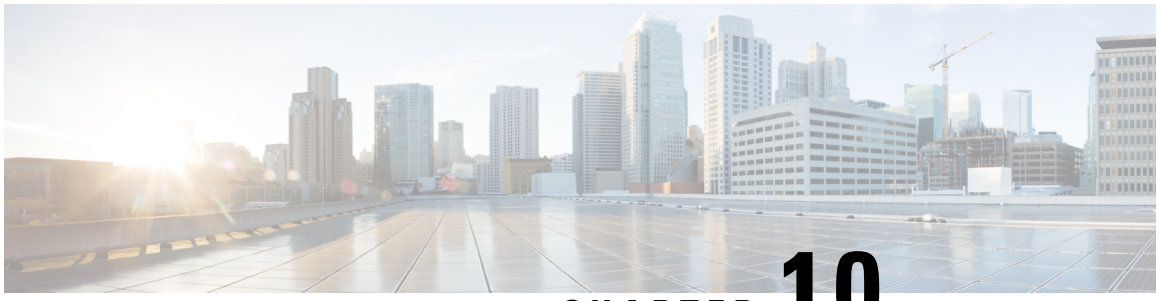
```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax primary
Frequency : 5745 MHz
Channel : 149
…….
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
```

MP2 (Mesh Point)

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5745 MHz
Channel : 149
…….
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax primary
Frequency : 5220 MHz
Channel : 44
Channel width : 40
…….
Fluidmax Configuration
Tower ID : 100
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
```

MP4 radio1

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5220 MHz
Channel : 44
Fluidmax Configuration
Tower ID : disabled
Cluster ID : fluidmesh
Automatic scan : enabled
Automatic scan threshold : disabled
```



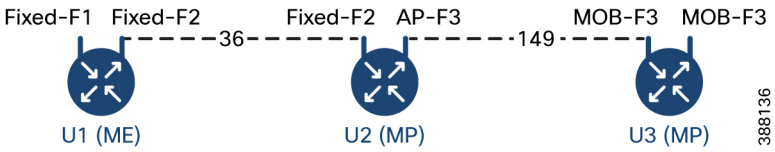
CHAPTER 10

Configuring and Validating Mixed Mode (Fixed infrastructure + Fluidity) Topology

Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology

The mixed mode configuration provides flexibility of configuration on multi-radio device with different frequencies. From the image, U2 is configured with one radio as fixed infrastructure and the second radio as a Fluidity access point to accept vehicle connections simultaneously. Both radio interfaces on U1 configured as fixed infrastructure when U3 has both radio interfaces configured as Fluidity. The wireless interface can also operate in Fluidmax mode without any restriction of the P2MP (Point-to-MultiPoint) role (Primary or Secondary) if fixed infrastructure role is suitable.

Figure 3: Mixed Mode Topologies



Configuring Mixed Mode Topology from CLI

To configure a mixed mode topology, use the following CLI command:

```
Device# configure fluidity id {vehicle-auto | vehicle ID | infrastructure | wireless- relay}
```

Fluidity id – Configure Fluidity role for the device

Vehicle-auto - Vehicle mode with automatic vehicle ID selection

Vehicle ID (alphanumeric) - Vehicle mode with manual ID

Infrastructure - Configure Infrastructure mode for the device

Wireless-relay - Wireless infrastructure with no ethernet connection to the backhaul

```
Device# configure dot11Radio <interface>
```

Interface - <0-3> dot11Radio interface number

```
Device# configure dot11Radio <interface> {enable | disable}
```

Enable or disable - Set wireless interface admin state to enable or disable at runtime

```
Device# configure dot11Radio <interface> mode {fluidity | fixed | fluidmax}
```

Mode - Operating mode for the specified interface (Fluidity or fixed or Fluidmax)

```
Device# configure dot11Radio <interface> channel <channel id>
```

Channel - Set the operating channel id <1 – 256>

```
Device# wr
```

Example:

U1 Configuration

```
Device# configure dot11Radio 2 enable
Device# configure dot11Radio 2 mode fixed
Device# configure dot11Radio 2 channel 36
```

U2 Configuration

```
Device# configure dot11Radio 1 enable
Device# configure dot11Radio 1 mode fixed
Device# configure dot11Radio 1 channel 36
Device# configure dot11Radio 2 enable
Device# configure dot11Radio 2 mode fluidity
Device# configure dot11Radio 2 channel 149
Device# configure fluidity id infrastructure
```

U3 Configuration

```
Device# configure fluidity id vehicle-auto
Device# configure dot11Radio 1 enable
Device# configure dot11Radio 1 mode fluidity
Device# configure dot11Radio 1 channel 149
```

Validating Mixed Mode Topology from CLI

To validate a mixed mode topology, use the following show commands:

```
Device# show dot11Radio <interface>config
```

U1 Statistics:

```
Device# show dot11Radio 2 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

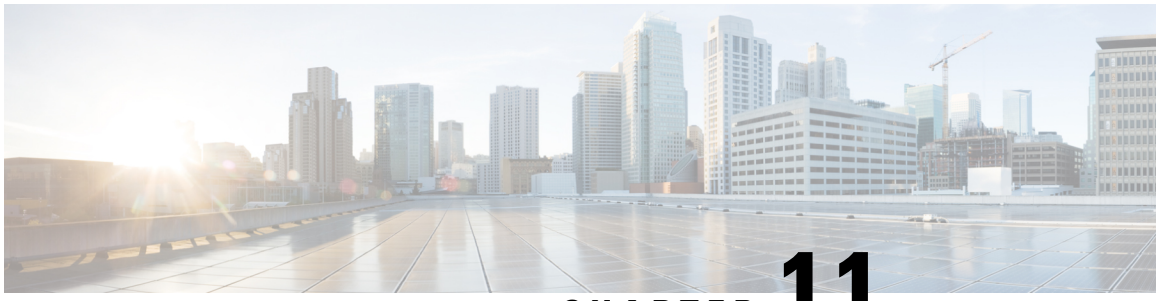
U2 Statistics:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
```

```
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidity
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```

U3 Statistics:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidity
Frequency : 5745 MHz
Channel : 149
……
Passphrase : Cisco
AES encryption : enabled
AES key-control : enabled
```



CHAPTER 11

Configure and Validate Fast Failover

Overview of Fast Failover

Fast failover is a specific type of failover configuration, where the system monitors server health and can quickly switch over when needed.

Fast Failover mechanism:

- Provides hardware redundancy and carrier-grade availability within URWB-based networks.
- In case of hardware failure, Fast Failover allows network to recover again within:
  - less than 30 seconds (varies as per network size) when Fluidmax is used.
  - less than 500 milliseconds when Fluidity is used.

Note Fast Failover is included in all the Network Licenses

Configure and Validate Fast Failover

Note Configure and validate fast failover is applicable for both the Fluidmax and Fluidity modes.

Before you configure the fast failover, use the following pre-conditions:

1. Ensure that both the primary and the backup primary node should have same configuration. This includes the same channel's parameters: frequency, channel width, and mode. If Fluidmax is enabled, ensure that the Cluster ID is the same for both nodes.

2. Enable fast failover on all devices in the network.

Note Fluidmax Fast failover is supported only on MP to MP or ME to ME with Ethernet backhaul.

Configure Fast Failover from CLI

Use this command to configure fast failover.

```
Device# configure modeconfig mode meshpoint
```

Modeconfig – Configure current operating mode of device. Mode could be mesh end(ME), mesh point(MP), or global gateway (L3).

```
Device# configure mpls fastfail status [enable | disable]
```

Mpls - Configure mpls data frame packets for specified device.

Fastfail - Configure the fast failover feature status (enable or disable).

```
Device# configure mpls fastfail timeout <0 – 65535>
```

Fastfail timeout - Set the fast failover timeout for device failure detection.

Use this command to set the preempt delay.

```
Device# configure mpls preempt-delay <0- 65535>
```

By default the preemption delay time is 70 seconds. During this period, the primary device actively gathers updates from the secondary device. This allows it to fully understand the network's current preemption delay status.

Note Radio interface setting must be same on both ME point to Multi point primaries.

Validate Fast Failover from CLI

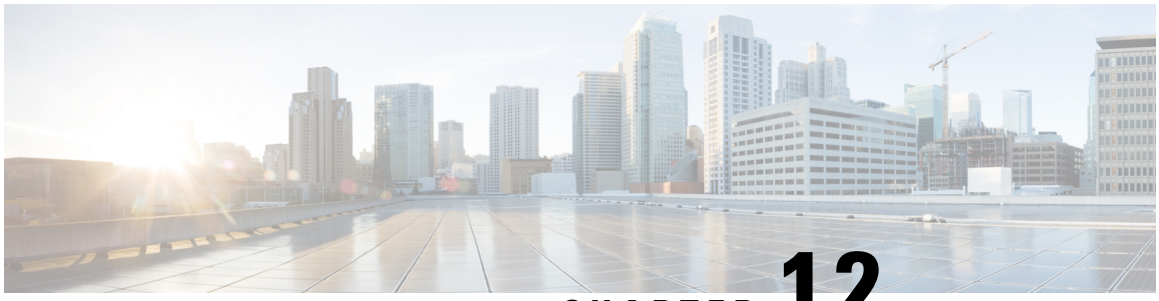
Use this command to validate fast failover.

```
Device# show mpls config
Device# show dot11Radio <interface> fluidmax (check Fluidmax Primary ID and working state)
```

Example:

```
Device# show mpls config
layer 2
unicast-fllod
arp-unicast:
reduce-broadcast:
cluster ID
MPLS fast failover: enabled
Node failover timeout: 100 ms
……
MPLS tunnels:
```

```
Idp_id 381877266 debug 0 auto_pw 1
Local_gw 5.21.201.116 global_gw 0.0.0.0 pwlist {}
```



CHAPTER 12

Configuring and Validating High Efficiency (802.11 ax)

Configuring and Validating High Efficiency

When High Efficiency (HE) is enabled, it is backward compatible with 802.11ac. To enable or disable 802.11ax HE, the following list is supported:

- URWB HE supports 20,40, and 80 MHz bandwidth for slot 1
- URWB HE supports 20,40,80, and 160 MHz bandwidth for slot 2
- URWB HE default setting is disabled
- HE negotiation is only supported between the devices with HE enabled

To enable HE mode, use the following CLI command:

```
Device# configure dot11Radio [1|2] high-efficiency enable
```

To configure maxmcs as 11, use the following CLI command:

```
Device# configure dot11Radio [1|2] mcs maxmcs 11 <mcs index in integer or string>
```

Note The default maxmcs is Nine.

To disable HE mode, use the following CLI command:

```
Device# configure dot11Radio [1|2] high-efficiency disable
default maxmcs is 9.
```

To validate HE mode, use the following show command:

```
Device# show dot11Radio 1 config
Maximum tx mcs : 9
High-Efficiency : Enabled
Maximum tx nss : 2
RTS Protection : disabled
guard-interval : 800ns
```

```
Device# show dot11Radio 2 config
Maximum tx mcs : 9
High-Efficiency : Enabled
Maximum tx nss : 2
RTS Protection : disabled
guard-interval : 800ns
```

```
Device# show eng-stats
```

WLAN1 Rx:

```
FC:58:9A:16F8:52 rate 1201 MCS 11/2 HE80/G1(800ns) ssn 48 rssi-48 received
```

WLAN1 Tx:

```
FC:58:9A:16F8:52 rate 1201 MCS 11/2 HE80/G1(800ns) sent 195612 failed 0
```

WLAN2 Rx:

```
FC:58:9A:16F8:13 rate 1201 MCS 11/2 HE80/G1(800ns) ssn 50 rssi-46 received
```

WLAN2 Tx:

```
FC:58:9A:16F8:13 rate 864 MCS 11/2 HE80/G1(800ns) sent 390797 failed 1
```

Configuring Global Gateway using GUI

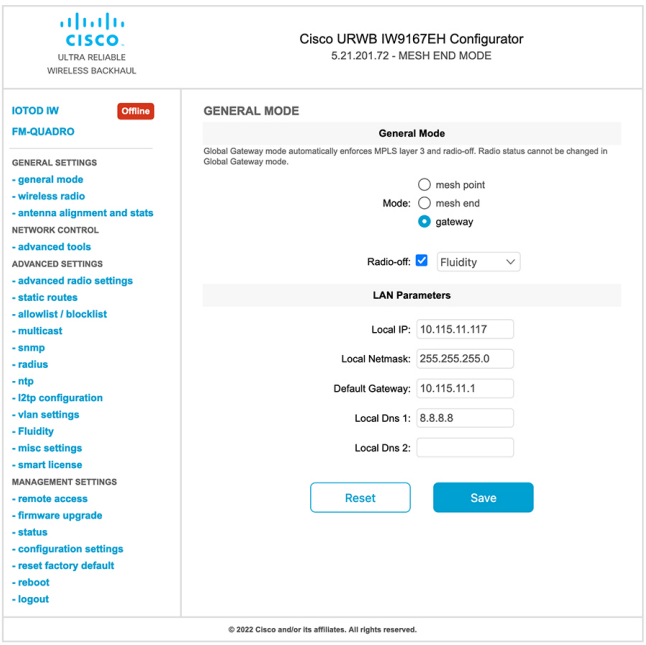
Global gateway mode automatically enforces the MPLS Layer 3. In this mode, Radio-off and Radio status cannot be changed.

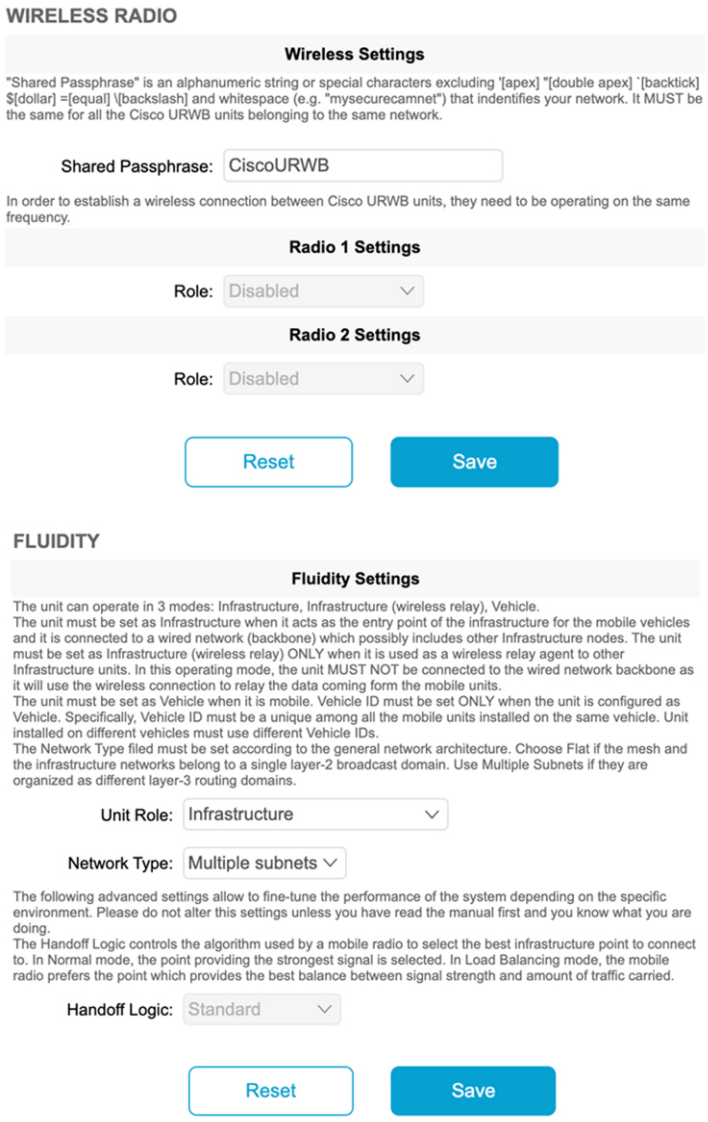
1. In the **GENERAL SETTINGS**, click **general mode**.

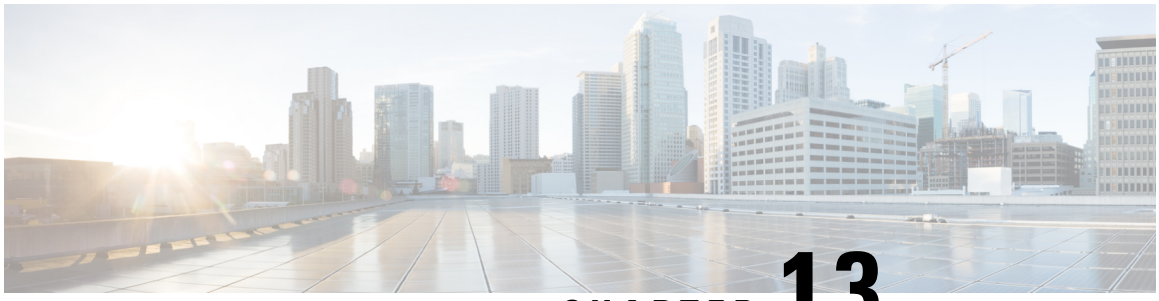
   The **GENERAL MODE** window appears.

2. Click **gateway** from **Mode**.

Following images shows the GUI configuration of global gateway mode:


ULTRA RELIABLE
WIRELESS BACKHAUL
Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
IOTOD IW
Offline
FM-QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
GENERAL MODE
General Mode
Global Gateway mode automatically enforces MPLS layer 3 and radio-off. Radio status cannot be changed in Global Gateway mode.
Mode:
mesh point
mesh end
gateway
Radio-off:
Fluidity
LAN Parameters
Local IP:
10.115.11.117
Local Netmask:
255.255.255.0
Default Gateway:
10.115.11.1
Local Dns 1:
8.8.8.8
Local Dns 2:
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.


WIRELESS RADIO
Wireless Settings
"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
Shared Passphrase:
CiscoURWB
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.
Radio 1 Settings
Role:
Disabled
Radio 2 Settings
Role:
Disabled
Reset
Save
FLUIDITY
Fluidity Settings
The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.
Unit Role:
Infrastructure
Network Type:
Multiple subnets
The following advanced settings allow to fine-tune the performance of the system depending on the specific environment. Please do not alter this settings unless you have read the manual first and you know what you are doing.
The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to connect to. In Normal mode, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.
Handoff Logic:
Standard
Reset
Save



CHAPTER 13

Configuring Guard Interval for HE (High Efficiency)

Configuring Guard Interval for HE (High Efficiency)

Longer guard intervals improve link reliability for long range outdoor deployments and the feature like guard interval supports URWB stacks.

To configure a guard interval, use the following CLI command:

```
Device# configure dot11Radio [interface] guard-interval [gi]
```

gi - Guard interval values are:

1600 - To configure 1600 ns guard interval (supported only in HE mode)

3200 - To configure 3200 ns guard interval (supported only in HE mode)

400 - To configure 400 ns guard interval (supported in HT and VHT modes)

800 - To configure 800 ns guard interval (default guard interval mode and disable mode in HT, VHT, and HE)

Example:

```
Device# configure dot11Radio 1 high-efficiency enable

Device# configure dot11Radio 1 guard-interval 1600

Device# configure dot11Radio 1 guard-interval 3200

Device# wr
```

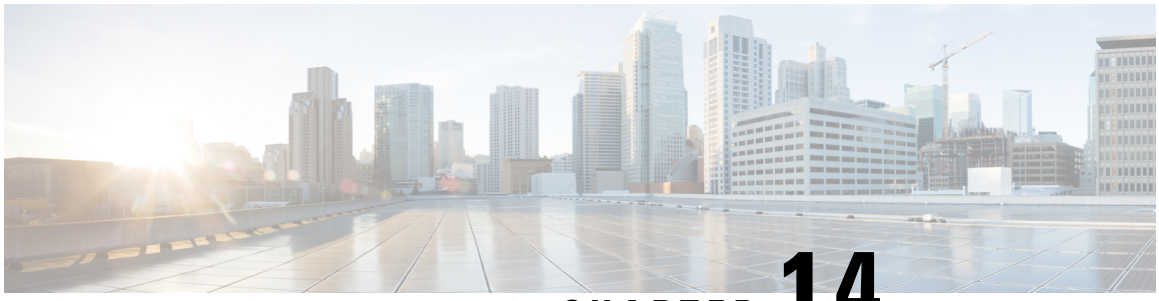
To validate a guard interval, use the following show commands:

```
Device# show dot11Radio 1 config
Maximum tx mcs: 9
High-efficiency : enabled
Maximum tx nss : 2
RTS protection : disabled
guard-interval : 1600 ns

Device# show dot11Radio 2 config
Maximum tx mcs: 9
High-efficiency : enabled
```

Configuring Guard Interval for HE (High Efficiency)

```
Maximum tx nss : 2
RTS protection : disabled
guard-interval : 3200 ns
```



CHAPTER 14

Configuring Indoor Deployment

Configuring Indoor Deployment

The Catalyst IW9167E and IW9165 support enabling and disabling of indoor deployment using CLI.

Note Before you enable the indoor deployment setting, ensure that the Catalyst IW9167E or IW9165 is set to indoor mode. As you can use the outdoor mode for indoors, but whereas the indoor mode is not suitable for outdoor because 5150–5350 MHz channels are indoor-related countries.

By default, the devices are set to outdoor mode.

To enable indoor deployment, use the following CLI command:

```
Device# configure wireless indoor-deployment enable
```

To disable indoor deployment, use the following CLI command:

```
Device# configure wireless indoor-deployment disable
```

To verify E indoor deployment, use the following show command:

For enabled indoor deployment

```
Device# show Dot11Radio {1|2} config
DFS region : E
DFS radar role : auto
Radar detected : 0
Indoor deployment : enable
```

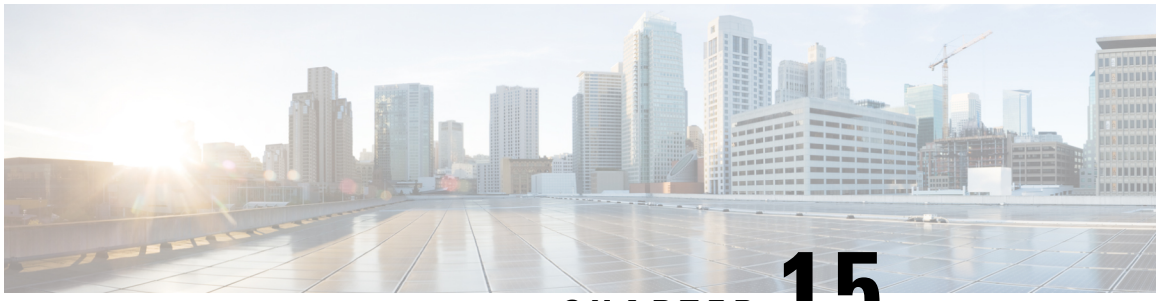
```
Device# show controllers Dot11Radio {1|2}
Radio info summary:
====================
Radio : 5.0 GHz
Carrier set : (-Ei) GB
Base radio MAC : FC:58:9A:15:B7:C0
Supported channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

For disabled indoor deployment

```
Device# show Dot11Radio {1|2} config
DFS region : E
```

```
DFS radar role : auto
Radar detected : 0
Indoor deployment : disable
```

```
Device# show controllers Dot11Radio {1|2}
Radio info summary:
====================
Radio : 5.0 GHz
Carrier set : (-E) GB
Base radio MAC : FC:58:9A:15:B7:C0
Supported channels:
100 104 108 112 116 120 124 128 132 136 140
```



CHAPTER 15

Configuring and Validating SNMP

Configuring and Validating SNMP

Simple network management protocol (SNMP) applications are used in URWB software for network management functionalities.

The SNMP client sends a request to the SNMP agent. The SNMP agent passes the request to the subagent. The subagent responds to the SNMP agent. The SNMP agent creates an SNMP response packet and sends it to the remote network management station that initiates the request.

Figure 4: SNMP Process

Configuring SNMP from CLI

To configure SNMP, use the following CLI commands:

Note

- SNMP CLI logic modified for SNMP configuration, before enabling the SNMP feature using CLI, you must configure all SNMP parameters.
- Disabling the SNMP feature automatically removes all related configurations.

To enable or disable SNMP functionality, use the following CLI command:

```
Device#configure snmp [enable | disable]
```

To specify the SNMP protocol version, use the following CLI command:

```
Device#configure snmp version {v2c | v3}
```

To specify the SNMP v2c community ID number (SNMP v2c only), use the following CLI command:

```
Device#configure snmp v2c community-id <length 1-64>
```

To specify the SNMP v3 username (SNMP v3 only), use the following CLI command:

```
Device#configure snmp v3 username <length 32>
```

To specify the SNMP v3 user password (SNMP v3 only), use the following CLI command:

```
Device#configure snmp v3 password <length 8-64>
```

To specify the SNMP v3 authentication protocol (SNMP v3 only), use the following CLI command:

```
Device#configure snmp auth-method <md5|sha>
```

To specify the SNMP v3 encryption protocol (SNMP v3 only), use the following CLI command:

```
Device#configure snmp encryption {des | aes | none}
```

Possible encryption values are des or aes. Alternatively, enter none if a v3 encryption protocol is not needed.

To specify the SNMP v3 encryption passphrase (SNMP v3 only), use the following CLI command:

```
Device#configure snmp secret <length 8-64>
```

To specify the SNMP periodic trap settings, use the following CLI command:

```
Device#configure snmp periodic-trap {enable | disable}
```

To specify the notification trap period for periodic SNMP traps, use the following CLI command:

```
Device#configure snmp trap-period <1-2147483647>
```

Notification value trap period measured in minutes.

To enable or disable SNMP event traps, use the following CLI command:

```
Device#configure snmp event-trap {enable | disable}
```

To specify the SNMP NMS hostname or IP address, use the following CLI command:

```
Device#configure snmp nms-hostname {hostname |Ip Address}
```

To disable SNMP configuration, use the following CLI command:

```
Device#configure snmp disabled
```

Once you disable SNMP, it clears all the sensitive information including credentials. You have to re-specify all the valid values again to enable SNMP.

Example of SNMP configuration:

CLI for SNMP v2:

```
Device#configure snmp v2 community-id <length 1-64>
Device#configure snmp nms-hostname hostname/Ip Address
Device#configure snmp trap-period <1-2147483647>
Device#configure snmp periodic-trap enable/disable
Device#configure snmp event-trap enable/disable
Device#configure snmp version v2c
Device#configure snmp enabled
```

CLI for SNMP v3:

```
Device #configure snmp nms-hostname hostname/Ip Address
Device#configure snmp trap-period <1-2147483647>
Device#configure snmp v3 username <length 32>
Device#configure snmp v3 password <length 8-64>
Device#configure snmp auth-method <md5|sha>
Device#configure snmp encryption <aes|des|none>
Device#configure snmp secret <length 8-64>
Device#configure snmp periodic-trap enable/disable
Device#configure snmp event-trap enable/disable
Device#configure snmp version v3
Device#configure snmp enabled
```

Validating SNMP from CLI

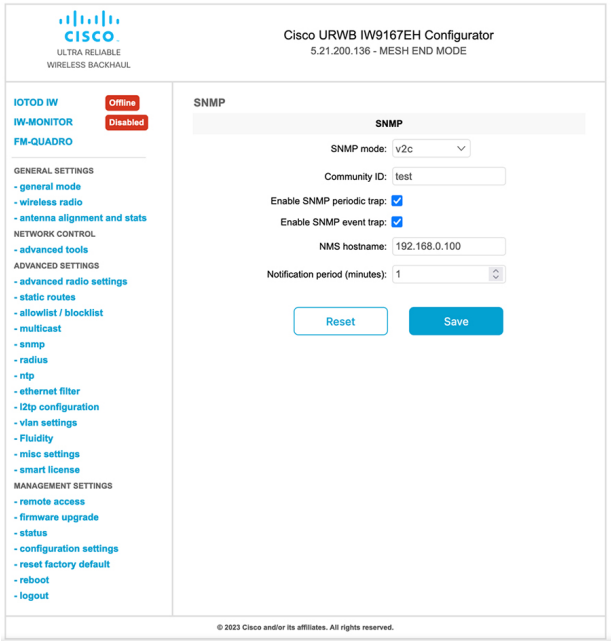
To validate the SNMP, use the following show command:

```
Device# show snmp
SNMP: enabled
Version: v3
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show snmp
SNMP: enabled
Version: v2c
Community ID: test
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show system status snmpd
Service Status
Service Name : snmpd
Loaded : loaded
Active : active (running)
Main ProcessID : 6437
Running Since : Mon 2022-09-19 14:45:27 UTC; 3h 34min ago
Service Restart : 0
```

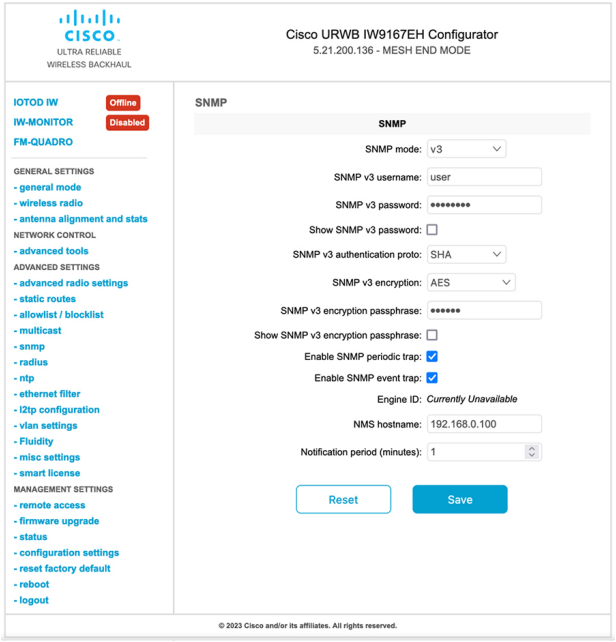
Configuring SNMP from GUI

The following images shows the configuration of SNMP from GUI

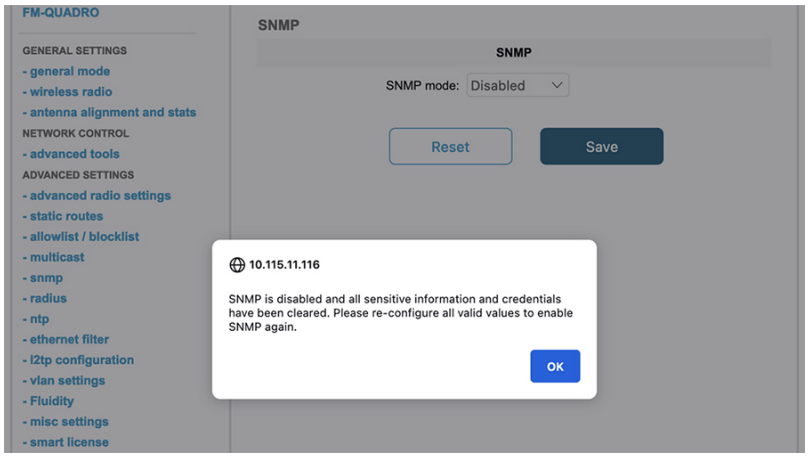
GUI for SNMP v2:

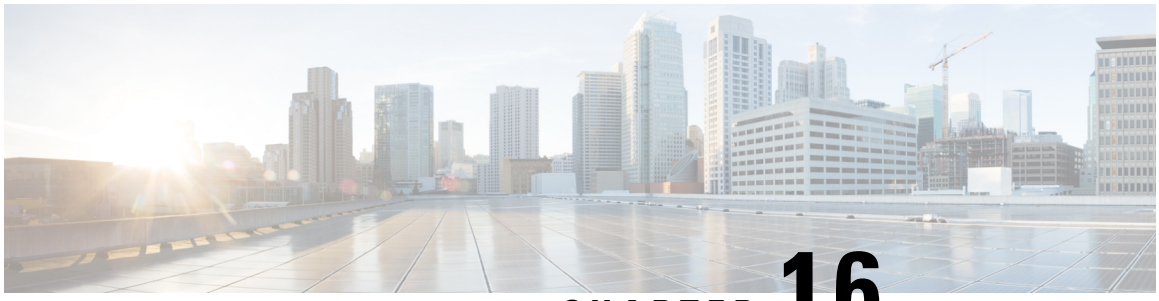


GUI for SNMP v3:



Disable SNMP via GUI


FM-QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
SNMP
SNMP
SNMP mode: Disabled
Reset
Save
10.115.11.116
SNMP is disabled and all sensitive information and credentials have been cleared. Please re-configure all valid values to enable SNMP again.
OK



CHAPTER 16

Multicast

Overview of multicast

AP supports multicast forwarding for Layer 2 and Layer 3 networks. You can configure multicast using either GUI or CLI. Multicast is a method of communication where data is sent from one source to multiple destinations simultaneously. Multicast transmissions can be point-to-multipoint or multipoint-to multipoint.

Note

- By default, only the multicast IP addresses specified below are forwarded across the URWB network.
- Multicast configuration is required only on mesh end devices.
- The multicast reserved IP address range is 224.0.0.0 to 239.255.255.255.

Reserved IP address range for multicast protocols

By default, multicast is enabled for these protocols within the specified IP address ranges:

Protocol	Reserved multicast IP address range
Universal plug and play (UPnP)	239.255.255.250
Open Shortest Path First (OSPF)	224.0.0.5 and 224.0.0.6
Internet Group Management Protocol (IGMP)	N/A

Advantages of multicast configuration

- It reduces the amount of bandwidth used by sending a single stream of data from one source to multiple destinations.

- It supports many devices without significantly increasing network load.
- It optimizes network performance for applications that require real-time data distribution.
- It maintains consistent quality by reducing the number of duplicate streams, helping to maintain consistent Quality of Service (QoS) for all recipient APs.

Configure multicast using GUI

Before you begin

- You can configure multicast only on the mesh end device.
- Ensure that you have a valid multicast group, netmask, and destination IP addresses.
- Ensure that you have a supported mesh end device to configure multicast.

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.
Once you have successfully logged into the GUI, the URWB configurator displays.

Step 4 In the **ADVANCED SETTINGS**, click **multicast** to open the **MULTICAST** window.

Step 5 In the **Add a new multicast route** section, enter these details:

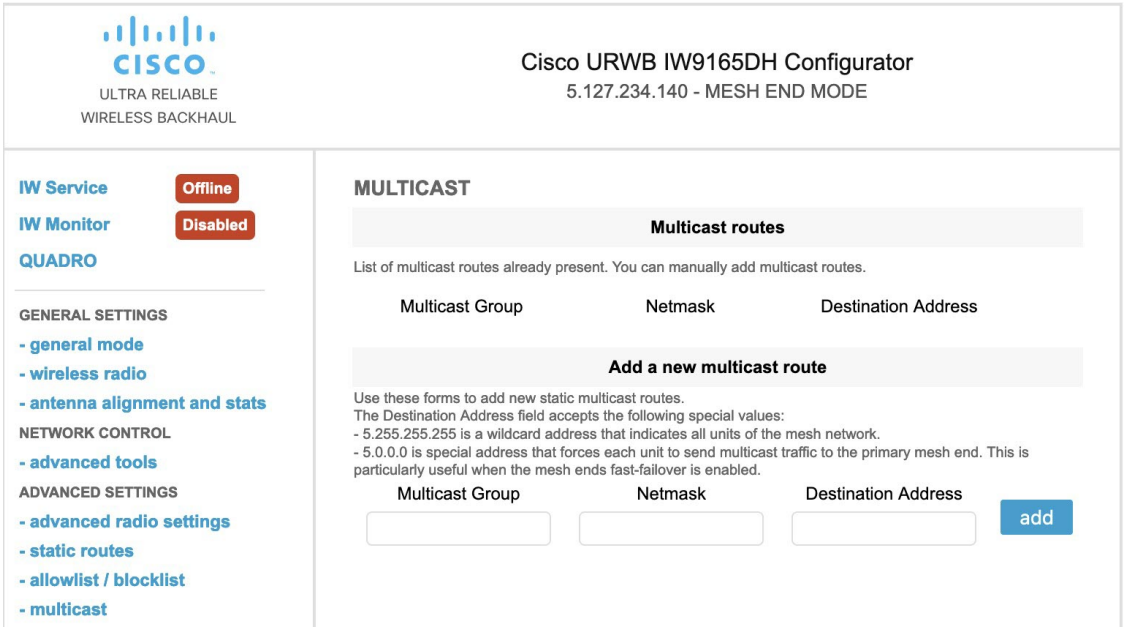
- Multicast IP address in the **Multicast Group** field.
- Netmask IP address in the **Netmask** field.
- Destination IP address in the **Destination Address** field.

Note
The **Destination Address** field accepts the following special values:

- 5.255.255.255 IP address in the **Destination Address** field: sends the data to all the mesh point devices over the mesh network. This is applicable only for the downstream data flow.
- 5.0.0.0 IP address in the **Destination Address** field: sends the data to the current primary mesh end device. This is useful, especially when the mesh end's fast failover is enabled. This is applicable only for the upstream data flow.

Tip
The netmask field allows you to specify block of multicast addresses. When you specify multiple multicast groups, the multicast IP address should reflect the network address for the group.

Step 6 Click **add**.
Once you have successfully added a rule, the new multicast route appears in the **Multicast routes** section.



Step 7 Click **Apply** to update the configuration.
AP reboots to apply the changes.

Configure multicast using CLI

Use the **configure multicast group add** *multicast-IP-address Netmask destination-IP-address* command to add the destination IP address.

Example:

```
Device#configure multicast group add 224.5.5.5 255.255.255.255 5.255.255.255
```

Note This configuration takes effect only after the reboot.

In Layer 3 mode, configure multicast rules on all mesh end devices and the global gateway. Use these different multicast IP addresses for upstream and downstream traffic:

- 224.5.5.5/5.0.0.0: sends the data to the current primary mesh end device. This is useful, especially when the mesh end's fast failover is enabled. This is applicable only for the upstream data flow.
- 224.5.5.6/5.255.255.255: sends the data to all the mesh point devices over the mesh network. This is applicable only for the downstream data flow.

Delete multicast using CLI

Use the **configure multicast group delete** *multicast IP-address Netmask meshID IP-address* command to delete the meshID IP address from the multicast group.

Example:

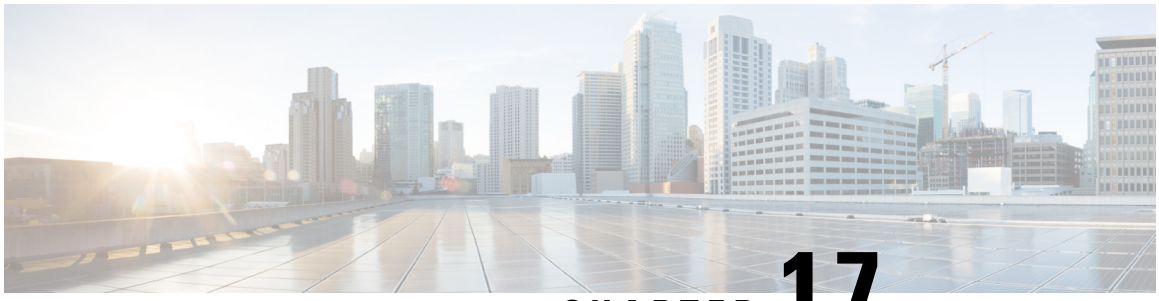
```
Device#configure multicast group delete 224.5.5.5 255.255.255.255 5.255.255.255
```

Note This configuration takes effect only after the reboot.

Verify multicast configuration using CLI

Use the **show multicast configuration** command to view the status of multicast configuration.

```
Device#show multicast configuration
Multicast Group 224.5.5.5/255.255.255.255
Destination Address 5.255.255.255
```



CHAPTER 17

Quality of Service

Overview of Quality of Service

Quality of Service (QoS) helps to prioritize certain types of network traffic over others. It maintains the quality and performance of critical applications, safety protocols such as, voice and video, which are sensitive to delays and packet loss. It involves classifying, marking, and managing data packets to provide different levels of service quality.

Traffic classification based on QoS

Traffic classification is the process of distinguishing different types of traffic by examining packet fields. During classification, the device performs a lookup and assigns a QoS label to the packet. This label indicates all QoS actions to be performed on the packet and identifies the queue from which the packet is sent. When QoS is enabled, the device can classify the priority of the packet. URWB devices do not apply QoS labels for incoming or outgoing data traffic on the URWB network. Instead, it recognizes existing QoS markings assigned by the traffic source or at other points in the network. URWB devices accept the markings applied at Layer 2 (PCP/VLAN) or Layer 3 (DSCP).

Advantages of QoS

- Prioritization: Manages traffic according to the QoS priority marked in the packet IP header.
- Bandwidth Management: Allocates network resources to ensure that high-priority applications have sufficient bandwidth.
- Latency Management: Minimizes delays in packet arrival time to maintain quality for time-sensitive applications.

QoS marking

QoS marking enables network devices to identify and handle packets according to their assigned priority. This process ensures that high-priority traffic is transmitted promptly and efficiently. QoS marking often uses the Differentiated Services Code Point (DSCP) or type of service (ToS) field in the IP header or the Priority Code Point (PCP) field in the VLAN header of an ethernet packet. These fields provide various priority levels. IW devices support eight priority levels, with 0 being the lowest priority and 7 being the highest. These 0 to 7 range is extracted from bits B5-B7 of the ToS value. ToS is the name for the complete 8-bit value found in an IP packet.

B7	B6	B5	B4	B3	B2	B1	B0
Priority			X	X	X	X	X

802.1p

802.1p is a standard developed by the IEEE as part of the broader 802.1Q specification. It addresses network traffic prioritization and QoS in Ethernet networks. This standard uses a 3-bit Priority Code Point (PCP) in the 802.1Q VLAN header to prioritize traffic.

QoS shaping

QoS shaping, also known as traffic shaping, is a network management technique used to control the flow of data across a network. It involves regulating the bandwidth available to different types of network traffic. This ensures that critical applications receive the necessary resources and prevents network congestion.

QoS configuration using CLI

By default, QoS feature is disabled on the device.

Enable or disable QoS using CLI

Use the **configure qos status enabled** command to enable the QoS processing on the device.

```
Device#configure qos status enabled
```

Note Use the **configure qos status disabled** command to disable the QoS configuration on the device.

Verify QoS configuration using CLI

Use the **show qos** command to verify the QoS configuration on the device.

Enabled:

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
```

```
qos-shaping disabled
qos-8021p disabled
```

Disabled:

```
Device#show qos
QoS: disabled
```

802.1p VLAN priority preference configuration using CLI

Enable or disable 802.1p VLAN priority preference using CLI

Use the **configure qos 8021p enabled** command to enable the 802.1p VLAN priority preference over DSCP for IP packets.

```
Device#configure qos 8021p enabled
```

Note Use the **configure qos 8021p disabled** command to disable the 802.1p on the device.

- If QoS 802.1p option is disabled, a URWB device first examines the QoS marking in the L3 header. If no marking is found there, it then checks the L2-VLAN header.
- If the QoS 802.1p option is enabled, an URWB device only considers the CoS value in the PCP field of the VLAN tag.

Verify 802.1p VLAN priority preference configuration using CLI

Use the **show qos** command to verify the QoS 802.1p configuration on the device.

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p enabled
```

Configure CoS remapping using CLI

The URWB system allows remapping of the QoS priority marks based on a network administrator's design. With this configuration you can change the priorities for one or more CoS values.

Use the **configure qos cos-map** *values* command to map CoS values of incoming packets to different CoS values.

```
Device#configure qos cos-map 0 1 2 3 4 4 4 4
```

In the CLI command example, CoS remapping is done as follows:

- CoS 0 remains 0

- CoS 1 remains 1
- CoS 2 remains 2
- CoS 3 remains 3
- CoS 4 remains 4
- CoS 5, 6 7 is remapped to 4

Here the packets with CoS values of 5, 6, and 7 are remapped to 4, effectively giving them the same priority as packets originally marked with CoS 4.

With this command you can adjust the prioritization of network traffic by changing the CoS value of packets as they enter the network. This can help in managing bandwidth and ensuring that higher priority traffic is delivered more efficiently.

Important The URWB system manages the remapping process without altering the original marking. The remapped QoS priorities are only significant and valid within the URWB network.

Verify CoS remapping using CLI

Use the **show qos** command to verify the CoS remapping configuration on the device.

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 4 4 4 ]
qos-shaping disabled
qos-8021p disabled
```

Configure QoS shaping using CLI

Configure per-CoS rates

Use the **configure qos shaper-rates** *bandwidths* command to allocate and control bandwidth for different CoS on a network device.

```
Device#configure qos shaper-rates <eigth traffic rates, one for each CoS>
```

Note All eight bandwidths cannot be with zero.

Example:

```
Device#configure qos shaper-rates 30000 50000 50000 50000 0 0 0 0
```

In this example, configure bandwidth for each CoS value.

- CoS 0 is assigned with a rate of 30,000 kbps,

- CoS 1 to 3 is assigned with a rate of 50,000 kbps, and
- CoS 4 to 7 are set to 0 kbps, 0 means unlimited rate (no bandwidth restriction).

Enable or disable QoS shaping

Use the **configure qos shaping enabled** command to enable the QoS shaping on the device.

```
Device#configure qos shaping enabled
```

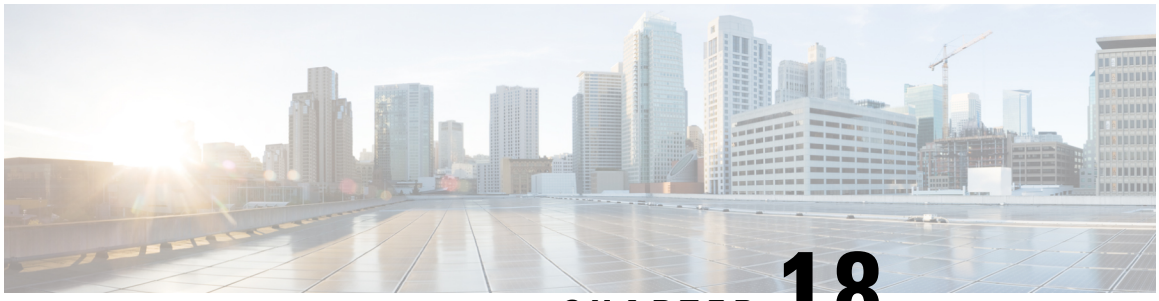
Note

- Use the **configure qos shaping disabled** command to disable the QoS Shaping on the device.
- If the network is running a throughput-restricted license, the sum of the bandwidths of all classes must not exceed the licensed throughput limit.

Verify QoS shaping using CLI

Use the **show qos** command to verify the QoS shaping configuration on the device.

```
Device#show qos
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping enabled
Shaper rates (Kbps): 30000 50000 50000 50000 0 0 0 0
qos-8021p disabled
```



CHAPTER 18

Frequency Scan

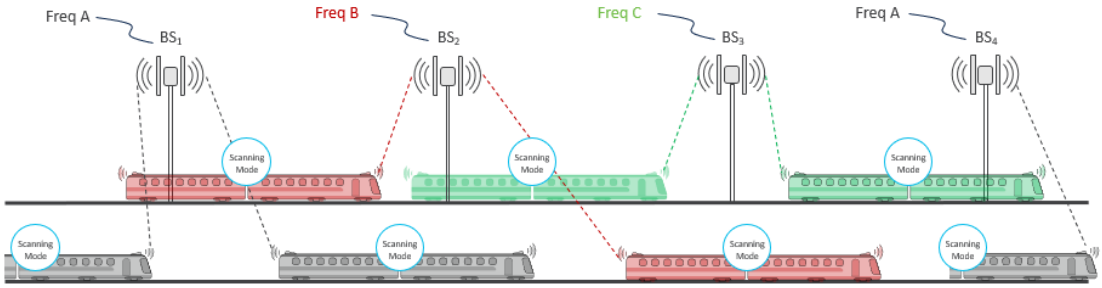
Frequency scan

URWB devices support two types of frequency scans:

1. Fluidity frequency scan
2. Fluidmax frequency scan

Overview of Fluidity frequency scan

Fluidity frequency scan is designed for scenarios involving high-density mobility environments using multiple frequencies on the infrastructure side to reduce self-interference and improve wireless channel capacity and performance. It helps to ensure continuous and seamless connectivity as these devices move across different network areas, facilitating smooth transitions between APs. When the current signal strength is weak, the device starts searching for a frequency with a better signal to maintain a stable connection. This feature is applicable in all high-density mobility environments, such as train-to-ground, mining, and port terminals.



For effective frequency scanning, a mobile device typically requires at least two radios:

- Radio 1: Maintains the current connection with the network.
- Radio 2: Performs scanning for better available frequencies without disrupting the existing connection on Radio 1.

Scanning can be performed in two modes:

- Periodic scan: Automatically conducted by the device at regular intervals to find the best available channel frequencies.
- Signal-triggered (threshold) scan: When the current device's signal strength drops below a specified minimum Signal-to-Noise Ratio (SNR) threshold value, the mobile device begins searching for another device with a stronger signal.

This dual-radio configuration allows continuous connectivity while optimizing connection quality.

Note

- Frequency scan is applicable only to fluidity vehicle devices, not to infrastructure devices.
- If the scan-periodic and scan-isolation parameters are set to zero, the frequency scan feature is disabled.

Configure Fluidity frequency scan using CLI

Use these commands to configure and manage Fluidity frequency scan on the device.

Clear the Fluidity frequency scan list using CLI

Use the **configure fluidity scan list clear** command to clear the Fluidity frequency scan list on the device.

```
Device#configure fluidity scan list clear
```

Configure channels for Fluidity frequency scan list using CLI

Use the **configure fluidity scan list** *pairs of channel numbers, bandwidths* command to configure list of channels and their bandwidths.

```
Device#configure fluidity scan list 100 20 108 20
```

Note For valid channel numbers and their bandwidths, refer topics Configure operating channel from CLI and Configure channel bandwidth from CLI.

Configure Fluidity frequency scan isolation time using CLI

Use the **configure fluidity scan isolation** *time* command to configure the isolation time of Fluidity frequency scan.

```
Device#configure fluidity scan isolation 3000
```

Note

- The isolation time valid range is from 0 to 65535.
- When the signal strength falls below a certain SNR threshold value for a continuous period of 3000 milliseconds, the device initiates scanning for better connectivity options.
- Use the **configure fluidity scan isolation disabled** command to disable the Fluidity frequency scan isolation mode on the device.

Configure SNR threshold for Fluidity frequency scan using CLI

Use the **configure fluidity scan rssi-threshold** *value* command to configure the SNR threshold for Fluidity frequency scan isolation mode.

```
Device#configure fluidity scan rssi-threshold 50
```

Note

- The device connects only to infrastructure devices that meet the specified minimum signal strength.
- The SNR threshold value valid range is from 0 to 100.
- Use the **configure fluidity scan rssi-threshold disabled** command to disable the SNR threshold.

Configure Fluidity frequency periodic scan time using CLI

Use the **configure fluidity scan periodic** *scan interval time* command to configure the periodic scan time on the device.

```
Device#configure fluidity scan periodic 5000
```

Note

- The specified time interval is in milliseconds.
- The periodic scan time valid range is from 0 to 65535. For best results, the minimum recommended value is 1500. This value should consider the number of channels configured.
- Use the **configure fluidity scan periodic disabled** command to disable the periodic frequency scan.

Onboard radios Fluidity frequency allocation using CLI

On the same channel

Use the **configure fluidity scan vehicle-frequency locked** command to lock the radio interfaces of onboard devices to operate on the same channel.

```
Device#configure frequency scan vehicle-frequency locked
```

On the separate channels

Use the **configure fluidity scan vehicle-frequency open** command to allow radio interfaces of onboard devices to operate on the separate channels.

```
Device#configure fluidity scan vehicle-frequency open
```

Verify Fluidity frequency scan configuration using CLI

Use the **show fluidity config command** to verify the Fluidity frequency scan on the device.

```
Device#show fluidity config
Fluidity enabled
Fluidity interface: 1
Vehicle ID: automatic, current ID: 89235672 current role: mobile primary unit
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
Rssi low/high zones threshold: 35
Color: enabled, current: 0
Color min RSSI threshold: 20
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan list: 5200@20 5240@20
Scan isolation time: 300 ms
Current Frequency: 5180 MHz
Current Channel Width: 20 MHz
Critical RSSI threshold for autoscan: disabled
Periodic autoscan interval: disabled
Vehicle frequency: open
Large network optimization: enabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
Quadro telemetry: enabled
```

Overview of Fluidmax frequency scan

Fluidmax frequency scan is typically used for devices in static or semi-static network environments. These are often devices that require stable and reliable connections in fixed locations or areas where the network environment doesn't change frequently. Such environments could include industrial sites, remote monitoring stations, or any setting where maintaining a consistent and interference-free connection is crucial.

Verify Fluidmax frequency scan status using GUI

Before you begin

Note In the wireless radio settings, you can select the radio role as Fluidmax secondary either for Radio 1 or Radio 2.

Procedure

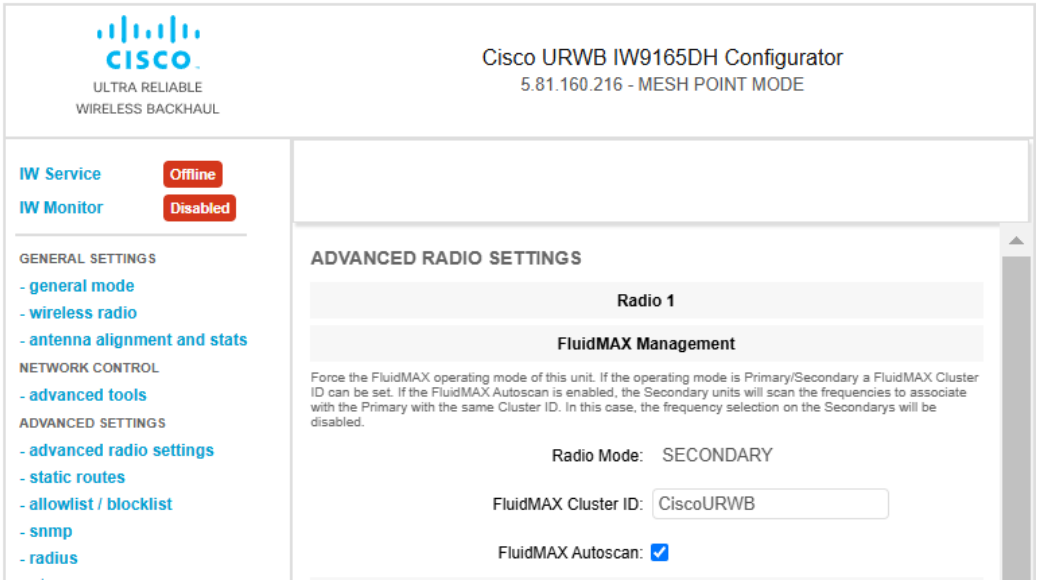
Step 1 Launch the computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter the username and password in the respective fields.

Step 3 Click **Login**.
Once you successfully log into the GUI, the URWB configurator displays.

Step 4 In the **ADVANCED SETTINGS**, click **advanced radio settings** to open the **ADVANCED RADIO SETTINGS** window.

Note
If the **FluidMAX Autoscan** checkbox is checked, the status is enabled; if unchecked, the status is disabled.



Configure Fluidmax frequency scan using CLI

Use these commands to configure Fluidmax frequency scan on the device.

Enable or disable Fluidmax frequency scan using CLI

Use the **configure dot11Radio** *slot number* **mode fluidmax automatic-scan enable** command to enable the Fluidmax frequency on the radio.

```
Device#configure dot11Radio 1 mode fluidmax automatic-scan enable
```

Note Use the **configure dot11Radio** *slot number* **mode fluidmax automatic-scan disable** command to disable the Fluidmax frequency on the radio.

Configure threshold value for Fluidmax frequency scan using CLI

Use the **configure dot11Radio** *slot number* **mode fluidmax** *threshold value* command to configure the Fluidmax threshold value on the radio.

```
Device#configure dot11Radio 1 mode fluidmax threshold 90
```

Note

- The Fluidmax threshold value valid range is from 0 to 100.
- If auto-scan is enabled, it triggers when the signal from the master falls below the specified threshold value.

Verify Fluidmax frequency scan configuration using CLI

Use the **show dot11Radio 1 config** command to verify the Fluidmax scan on the device.

```
Device #show dot11Radio 1 config

Interface: enabled

Mode: fluidmax secondary

Frequency: 5200 MHz
Channel: 40
Channel width: 20 MHz
Antenna number: 2
TX power level: 2
TX power: 14 dBm
Antenna gain: 15 dBi
Maximum tx mcs: 9
High-efficiency: disabled
Maximum tx nss: 2
RTS protection: 512
guard-interval: 800 ns
ampdu max length: 255
distance: 3000 m

The ampdu Tx
priority 0: enabled
priority 1: enabled
priority 2: enabled
priority 3: enabled
priority 4: enabled
```

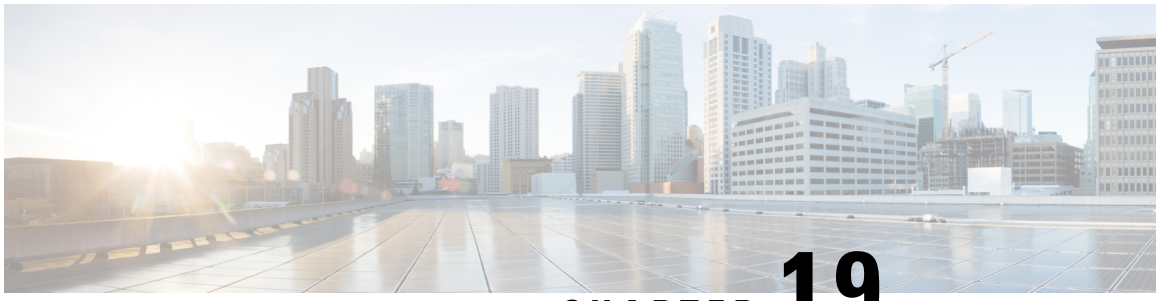
```
priority 5: enabled
priority 6: disabled
priority 7: disabled

Fluidmax configuration
Tower ID: disabled
Cluster ID: CiscoURWB
Automatic scan: enabled
Automatic scan threshold: disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase: 58ac1e597fda4e37bc0c2472d8c8c69f
AES encryption: disabled
AES key-control: disabled
Key rotation: disabled
Key rotation timeout: 0(second)

DFS region: B
DFS radar role: auto
Radar detected: 0
Indoor deployment: disable
Rx-SOP Threshold: 0 dBm(AUTO)
Max packet retries: 32
High throughput 4.9Ghz: disabled
```



CHAPTER 19

Configuring and Validating Key Controller (Wireless Security)

Configuring and Validating Key Controller (Wireless Security)

To support wireless security to standard Wi-Fi Protected Access (WPA) protocols, a key rotation strategy is implemented for Catalyst IW9167E. The key controller protocol is a packet exchange between two devices, in which different stages of the process correspond to different states of each device. The algorithm flow is controlled by a set of timers scheduled periodically to generate new Pairwise Transient Key/Group Transient Key for packet encryption. The more frequently keys are updated, the lesser amount of information is leaked in the event of an attack.

Configuring Key Controller from CLI

To configure a key controller, use the following CLI commands:

1. To enable Advanced Encryption Standard (AES) on Radio, use the following CLI command:

   ```
   Device# configure dot11Radio <interface> crypto aes enable
   ```

2. To enable key controller, use the following CLI command:

   ```
   Device #configure dot11Radio <interface> crypto key-control enable
   ```

3. To enable key rotation, use the following CLI command:

   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation enable
   ```

4. To set key rotation timer, use the following CLI command:

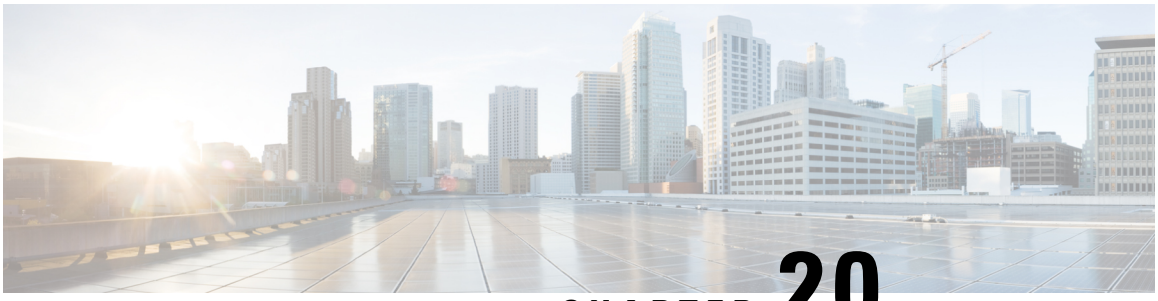
   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation 3600
   ```

Note By default, AES mode is disabled. Configuration should be same on all devices.

Validating Key Controller from CLI

To validate a key controller, use the following show command:

```
Device# show dot11Radio X crypto
AES encryption: enabled
AES key-control: enabled
Key rotation: enabled
Key rotation timeout: 3600(second)
```

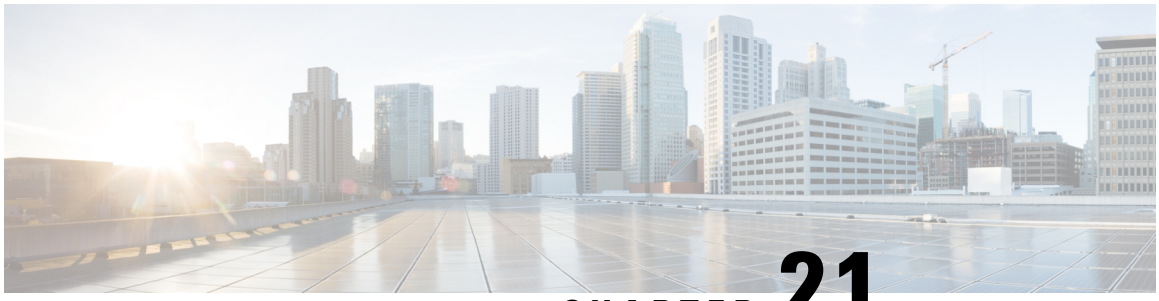


CHAPTER 20

Smart Licensing

Smart Licensing Support

The Smart Licensing chapter is replaced by a new standalone guide called Smart Licensing on the Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points. This guide contains updated information related Smart licensing for access point running in URWB mode.



CHAPTER 21

Configuring Layer 2 Mesh Transparency

Configuring Layer 2 Mesh Transparency

Layer 2 mesh transparency feature allows you to select the ether type for a specific protocol. To forward the ether-types, use CLI or GUI to enable or disable the network. The following list of reserved ether-types cannot be configured:

Table 4: List of reserved ether-types

Ether-type (range)	Forwardable	Additional information
0x0000 – 0x05FF	User-configurable	Ethernet-I frames. STP and CDP are subject to other configuration options
0x0800	Yes	IPv4
0x0806	Yes	ARP (IPv4)
0x0900 – 0x09FF	No	URWB signaling protocols
0x8100	Yes	IEEE 802.1Q VLAN encapsulation
0x8847 – 0x8848	No	MPLS
0xFFFF	No	IANA reserved

The following functionalities are supported using the URWB data plane mesh network when used in MPLS Layer 2 mode.

- The Layer 2 mesh transparency feature forwards non-IPv4 Layer 2 protocols across the URWB network by selectively filtering which ether-types are permitted.
- Ether-types present in URWB network are detected and reported automatically.
- Ability to add and remove ether-types from the allowlist.

- Ability to configure full transparency (enable all Layer 2 protocols) in a convenient manner.
- Both CLI and GUI are supported.

Configuring and Verifying Layer-2 Protocols Forwarding Using CLI

To configure a Layer 2 protocol forwarding, use the following CLI command:

To add an ethernet type to allowlist, use the following CLI command:

```
Device# configure mpls ether-filter allow-list add

<0x0-0xffff> ether-type value
         all allow all ether-types
```

Example:

```
Device# configure mpls ether-filter allow-list add 0x86DD

Device# show mpls config
        ...
        Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
        ...
```

To delete an ethernet type from allowlist, use the following CLI command:

```
Device# configure mpls ether-filter allow-list delete
         <0x0-0xffff> ether-type value
```

Example:

```
Device# configure mpls ether-filter allow-list delete 0x86DD

Device# show mpls config
        ...
        Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
        ...
```

To clear all ethernet types from allowlist, use the following CLI command:

```
Device# configure mpls ether-filter allow-list clear
```

Example:

```
Device# show mpls config
                ...
                Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
                ...
        Device# configure mpls ether-filter allow-list clear
        Device# write
        Device# reload

        Device# show mpls config
        ...
        Ethernet Filter allow-list: none, ethernet-I block
        ...
```

To add all ethernet types to allowlist, use the following CLI command:

```
Device# configure mpls ether-filter allow-list add all
```

Example:

```
Device# configure mpls ether-filter allow-list add all

        Device# show mpls config
        ...
        Ethernet Filter allow-list: all, ethernet-I block
```

Note The **all** keyword is used to set the ether filter in all-pass mode (fill allowlist with single entry 0x0000).

To clear list of detected ether-types, use the following CLI command:

```
Device# configure mpls ether-filter table clear
```

Example:

```
Device# show mpls ether-filter
                Ether-type Direction Description
                0x8899      INGRESS    ---
                0x86DD      INGRESS    IPv6
        Device# configure mpls ether-filter table clear
                Cisco-81.160.136#show mpls ether-filter
                Ether-type Direction Description
                0x8899      INGRESS    ---
```

Note The detection process works in background after clearing the detected ethernet types.

To configure Ethernet – I protocol, use the following CLI command:

```
Device# configure mpls ether-filter ethernet-I forward
```

Example:

```
Device# configure mpls ether-filter ethernet-I forward

Deive# show mpls config
        ...
        Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I forward
        ...


Device# configure mpls ether-filter ethernet-I block
```

Example:

```
Device# configure mpls ether-filter ethernet-I block

         Device# show mpls config
         ...
         Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I block
```

To verify list of allowed ether-types, use the following show command:

```
Device# show mpls config
```

Example:

```
Device# show mpls config
                ...
                Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
                ...
```

To verify list of detected ether-types, use the following show command:

```
Device# show mpls ether-filter table
```

Example:

```
Device# show mpls ether-filter table
                Ether-type   Direction   Description
                0x8899        INGRESS       ---
                0x86DD        INGRESS       IPv6
```

Configuring Layer-2 Protocol Forwarding using GUI

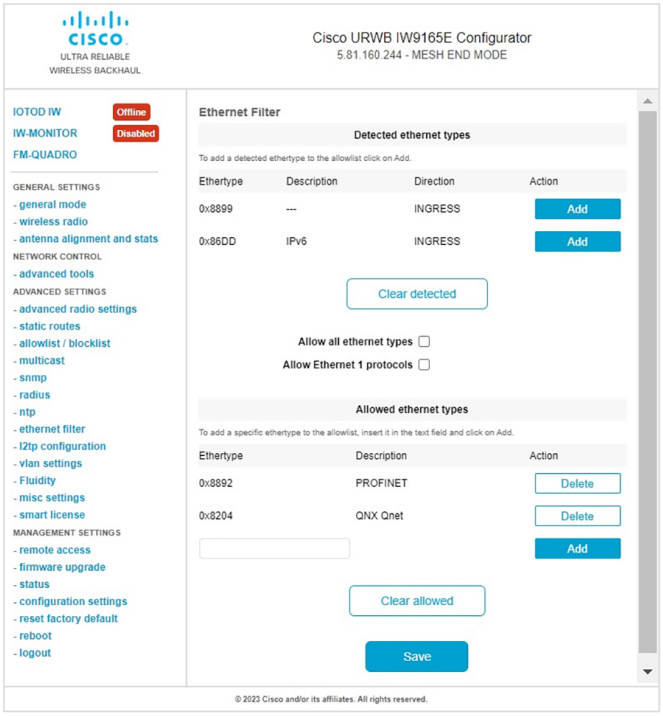
To add specific and detected ether types to the allowlist, follow these steps:

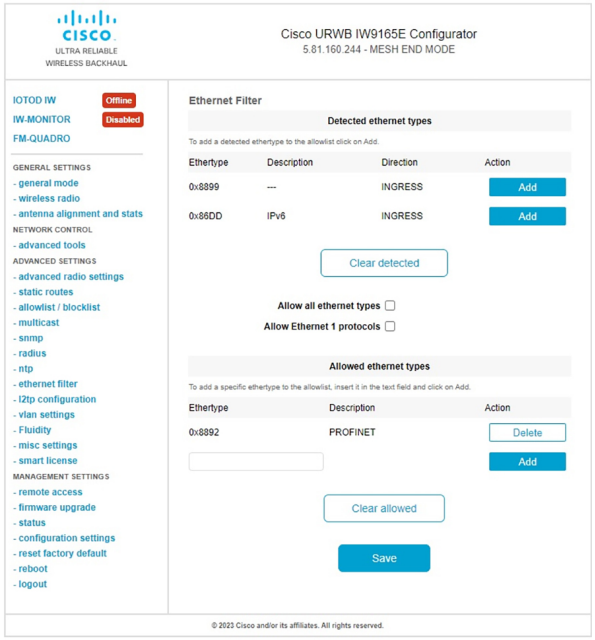
1. In the **ADVANCED SETTINGS**, click **ethernet filter**.

   The **Ethernet Filter** window appears.

2. Click **Add** to add an ether types to the allowlist in the **Detected ethernet types** section.
3. Once it is added, you can see the added ether types reflected in the **Allowed Ethernet type** section.
4. In the **Allowed ethernet types** section, to add a specific ether type to the allowlist, enter the **Ethertype** name in the text box and click **Add**.

The following images show the specific and detected ether types added to the allowlist:





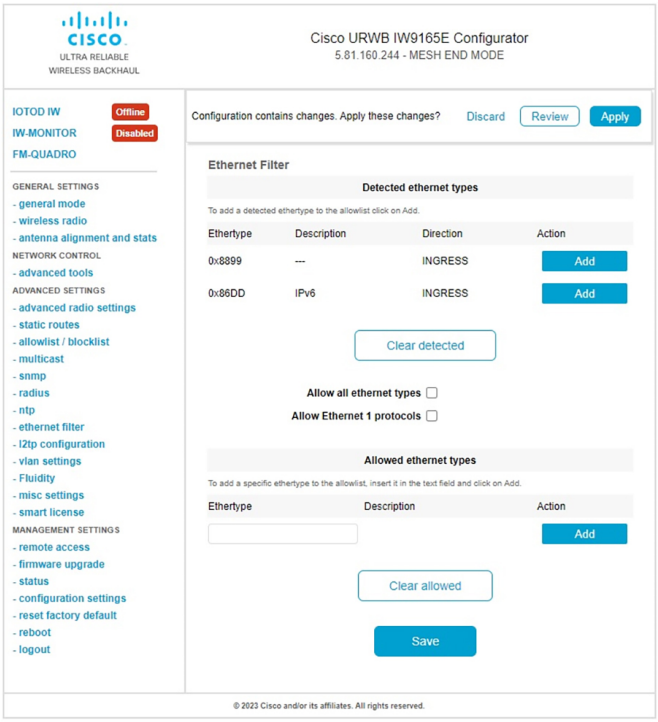
To clear all allowed ethernet types from the allowlist, follow these steps:

1. In the **ADVANCED SETTINGS**, click **ethernet filter**.

   The **Ethernet Filter** window appears.

2. Click **Clear allowed** in the **Allowed ethernet types** section to clear all the ethernet types from the allowlist.
3. Once you click **Clear allowed**, you can see all ethernet types cleared from allowlist.

The following image shows all allowed ethernet types cleared from the allowlist:



To clear all detected ethernet types from the allowlist, follow these steps:

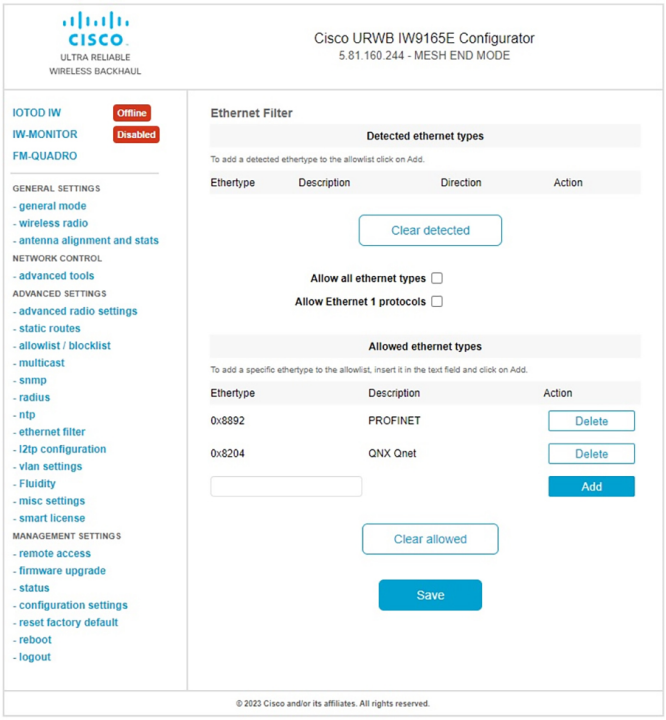
1. In the **ADVANCED SETTINGS**, click **ethernet filter**.

   The **Ethernet Filter** window appears.

2. Click **Clear detected** in the **Detected ethernet types** section to clear the detected ethernet types from allowlist.

3. Once you click **Clear detected**, you can see ethernet types cleared in the **Detected ethernet types** section.

The following image shows all detected ethernet types cleared from the allowlist:



To add or allow all ethernet types to the allowlist, follow these steps:

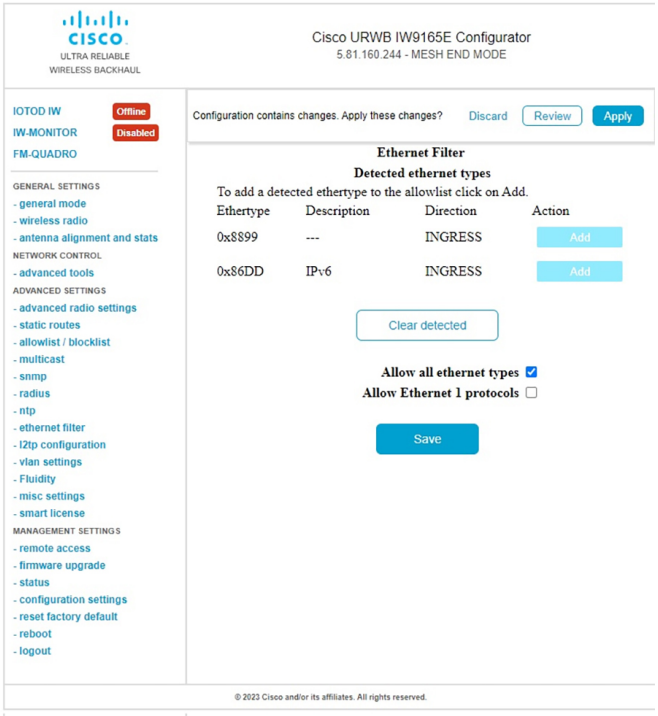
1. In the **ADVANCED SETTINGS**, click **ethernet filter**.

   The **Ethernet Filter** window appears.

2. Check the **Allow all ethernet types** check box in the **Ethernet Filter** section to allow all ethernet type to allowlist.

3. Click **Save** and then **Apply** to change the configuration.

The following image shows adding of all ethernet types to the allowlist:



To configure an ethernet 1 protocol, follow these steps:

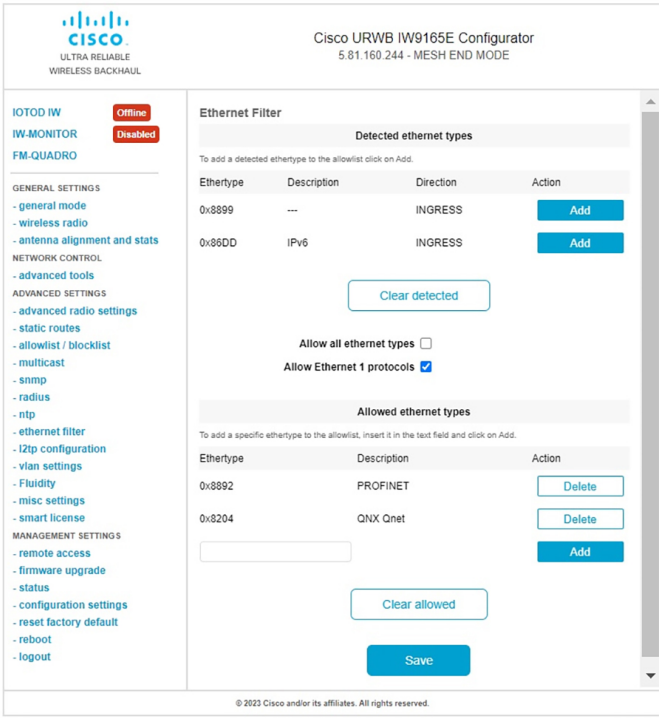
1. In the **ADVANCED SETTINGS**, click **ethernet filter**.

   The **Ethernet Filter** window appears.

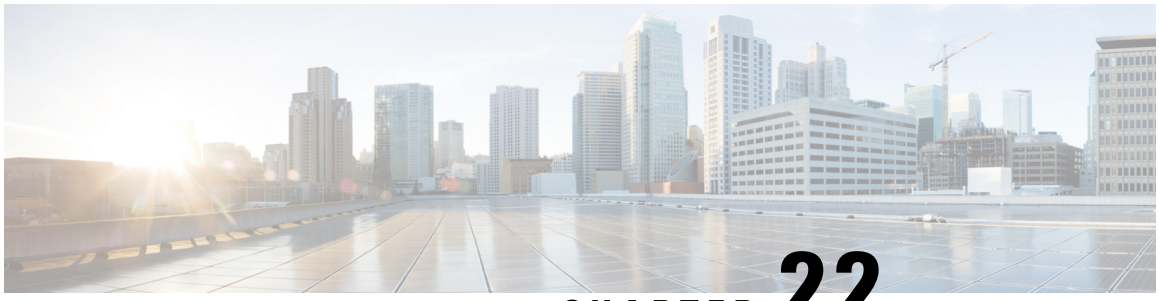
2. Check the **Allow Ethernet 1 protocols** check box in the **Ethernet Filter** section to enable ethernet 1 protocol mode.

3. Click **Save** and then **Apply** to change the configuration.

The following image shows the configuration of allowing an ethernet 1 protocol:


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
ULTRA RELIABLE WIRELESS BACKHAUL
IOTOD IW
Offline
IW-MONITOR
Disabled
FM-QUADRO
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
Ethernet Filter
Detected ethernet types
To add a detected ethertype to the allowlist click on Add.
Ethertype
Description
Direction
Action
0x8899

INGRESS
Add
0x86DD
IPv6
INGRESS
Add
Clear detected
Allow all ethernet types
Allow Ethernet 1 protocols
Allowed ethernet types
To add a specific ethertype to the allowlist, insert it in the text field and click on Add.
Ethertype
Description
Action
0x8892
PROFINET
Delete
0x8204
QNX Qnet
Delete
Add
Clear allowed
Save
© 2023 Cisco and/or its affiliates. All rights reserved.



CHAPTER 22

Configuring Multipath Operation

Overview of MPO

Fast-moving mobile systems expect high-speed connectivity onboard, which implies reliable wireless ground-to-vehicle communication without any interruptions. However, the dynamic nature of the network, the environmental radio frequency conditions and roaming under the various Wi-Fi standards lead to packet losses. Multipath Operation (MPO) enhances reliability by sending duplicate copies of packets across multiple wireless paths. This patented technology duplicates your high priority traffic up to 4x and it reduces hardware failures to increase availability, reduce latency, and lower the effects of interference.

MPO introduce an approach to establish multiple label switched paths (LSPs) between a mobile system and the backend infrastructure of a wireless network. The multiple LSPs enables high priority packets to be sent through redundant paths to reduce packet loss.

Working Functionality of MPO

MPLS has a single tunnel that connecting the home network with infrastructure and using a single wireless link between the vehicle and infrastructure. Multiple MPLS tunnels between vehicles and machines in the fixed infrastructure using different radio links, so you can install up to four different tunnels simultaneously that uses different radio links. Multiple MPLS tunnels protect the specific traffic and improve system reliability.

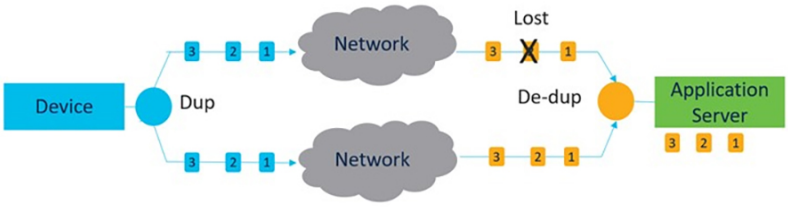
To protect the system from interference on wireless links, the control traffic is replicated over many MPLS tunnels, and copies of each packet are made and sent to various pathways. The receiver from the infrastructure side, receives more than one copy of the same packet after multiple copies of the traffic are produced and sent to parallel tunnels. However, without MPO functionality, if the wireless link fails, there is traffic loss. Multiple MPLS tunnels provide additional redundancy that receives the copy of the packet successfully even if the wireless link does not function due to interference and the corresponding copy of the packet is loss.

MPO Packet Duplication and Deduplication

For MPO, a duplicate packet is sent through several wireless channels (to various access points). This helps to ensure reliability, and the spatial diversity of the receiving access points greatly increases the chances of at least one of the copies to be received correctly. Deduplication is another aspect of MPO to remove any duplicates of a packet that are received along the different wireless paths.

As a result, the delivered packets currently have sequence numbers assigned to them, thereby allowing the deduplication algorithm to eliminate copies of any packets that it has already received.

The process of Duplication and Deduplication as shown:



Duplication and Deduplication algorithm performs the following:

- Address packet loss and asymmetric high/variable delay paths.
- Remove additional packet delays created by buffering.
- Remove duplicate and out of sequence packets.
- Improve CPU, resource, and memory efficiency.

Configuring MPO Features using CLI

Before you configure MPO, you must enable 802.1p-based QoS.

To configure the MPO features, use the following CLI commands:

```
Device# configure fluidity mpo
```

cos - Configure class-of-service (CoS) of traffic to protect with MPO redundancy (only one CoS at a time) and the valid cos range is from zero to seven and the default value is six.

path - Configure max number of simultaneous redundant path established by only mobile devices. Maximum path link valid range is from one to four and the default value is one.

rssi - Configure min RSSI threshold for a wireless link to be eligible as a redundant path(dB) (mobile devices only). Minimum rssi value valid range is from 0 to 96 and the default value is 20.

telemetry – Configure enable/disable specific MPO telemetry. Telemetry value one of the following: enabled: M=1 or disabled: M=0 (default).

```
Device# configure fluidity mpo status
```

disabled: Disable MPO duplication/deduplication.

rx-only: Set mpo status as rx-only. Deduplicate incoming MPLS traffic and do not duplicate outgoing traffic.

enabled: Enable MPO. Duplicate outgoing traffic and de-duplicate incoming MPLS traffic.

Example:

```
Device# configure fluidity mpo cos C ( C value from 0 to 7 (default 6))
Device# configure fluidity mpo path max N ( N value from 1 to 4 ( default 1))
Device# configure fluidity mpo rssi min R ( R value from 0 to 96 ( default 20))
Device# configure fluidity mpo telemetry T (T can be one of: enabled: M=1
                                              Disabled: M=0 (default))
Device# configure fluidity mpo status S ( S can be one of:
                                          enabled: E=1 F=1
                                          rx-only: E=1 F=0
                                          disabled: E=0 F=1 (default))
```

The following example shows the UDP Telemetry stream with MPO counters:

```
Device# configure fluidity mpo telemetry <enabled | disabled>
Device# configure telemetry server 192.168.0.200
Device# configure telemetry export enable
Device# configure fluidity mpo telemetry enabled
```

To verify an MPO configuration parameter, use the following show command:

```
Device# show fluidity mpo config
```

Example:

```
Device# show fluidity mpo config
                Status: enabled
                Path max links: 2
                RSSI min: 20
                CoS: 6
```

Verifying MPO Features using CLI (MPO Monitoring)

The output of the **show mpls config** command:

```
Device# show mpls config
                  5.42.42.43:
                  path_id : 0
                  ilm : 136000
                  nhlfe : 16:
                  lbr : 5.42.42.42
                  age : 6.980000028 { 5.42.42.42 5.42.42.43 }

                  path_id : 1
                  ilm : 136001
                  nhlfe : 18:
                  lbr : 5.42.42.42
                  age : 6.970000026 { 5.42.42.42 5.42.42.43 }
```

The output of the **show fluidity mpo statistics** command:

```
Device# show fluidity mpo statistics (on Mesh End)
           table-size 2:

             MAC address : 40:36:5A:15:C8:50        8C:89:A5:83:EB:71
             Tx-1        : 0                        208
             Tx-2        : 0                        208
             Rx-Accept-1 : 178                      0
             Rx-Accept-2 : 30                       0
             Rx-Drop-1   : 30                       0
             Rx-Drop-2   : 178                      0
             Lost-1-only : 0                        0
             Lost        : 0                        0
```

```
Device# show fluidity mpo statistics (on Mobile Primary unit)
            table-size 2:

            MAC address : 40:36:5A:15:C8:50        8C:89:A5:83:EB:71
            Tx-1        : 208                      0
            Tx-2        : 208                      0
            Rx-Accept-1 : 0                        182
            Rx-Accept-2 : 0                        26
            Rx-Drop-1   : 0                        26
            Rx-Drop-2   : 0                        182
            Lost-1-only : 0                        0
            Lost        : 0                        0
```

MAC address: Source L2 address of the external network device which is sending packets.

Tx-1 and Tx-2: Shows the total count of packets that are eligible for duplication.

Rx-Accept-1 and Rx-Accept-2: These counters represent, respectively, the number of packets received and dropped in the de-duplication process either on the primary path or secondary paths.

Lost-1-only: Number of packets received and accepted in the de- duplication process on the secondary paths but not on the primary path.

Lost: The cumulative number of packets lost on both primary path and secondary paths.

The output of the `show fluidity network` command:

```
Device# show fluidity network (on Mesh End and Mobile Primary)

                    unit 5.21.201.60  infrastructure meshend primary
                    vehicles 4  total_mobiles 5
                    infrastructure 1  backbone 0  meshend 5.21.201.60

                    Vehicle ID : + 85313616
                    Path : 0
                    Infrastr.ID : 5.21.201.60
                    Via : R1
                    Mobile ID : 5.21.200.80
                    Via : R2
                    H/O seq : 5710
                    H/O age : 36.597
                    #M: 2
                    Primary ID : 5.21.200.80
                    Secondary IDs : 5.21.201.204

                    Vehicle ID : + 85313616
                    Path : 1
                    Infrastr.ID : 5.21.201.60
                    Via : R2
                    Mobile ID : 5.21.201.204
                    Via : R2
                    H/O seq : 5711
                    H/O age : 5.909
                    #M: 2
                    Primary ID : 5.21.200.80
                    Secondary IDs : 5.21.201.204
```

Note Intermediate nodes (MP and mobile secondaries) have only a subset of paths.

MPO path ID 0: primary path, others: redundant paths.

The output of the **show eng-stats** command:

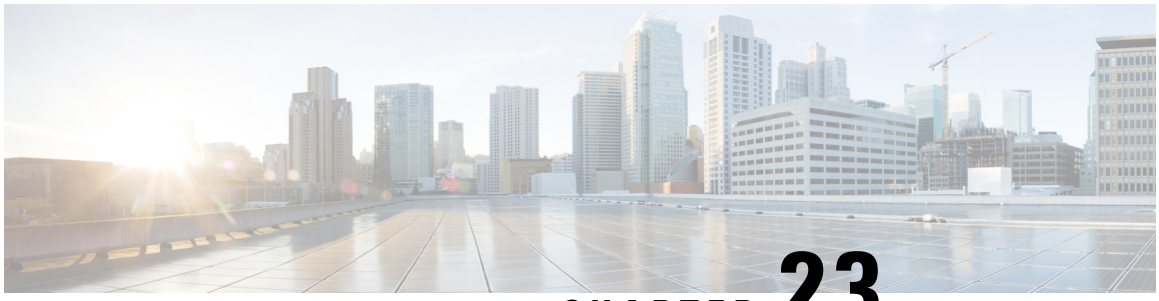
```
Device# show eng-stats (on mobile primary unit)
....
Fluidity role : primary
vehicle id : 0
static  : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile  : 4.21.200.80 [FC:58:9A:15:B9:13]
snr : 42
rssi : -54
dop : 40
chan : 132/40
handoff: 21.518258794
time : 2
Current:
ho_seq: 7  pending: false  age: 21.518303221  primary: 5.21.200.80
[0] - <3.21.201.60 - 4.21.200.80> status SUCCESS seq 6 id 0 age 59.469266332 rssi 42
[1] - <4.21.201.60 - 4.21.201.204> status SUCCESS seq 7 id 1 age 21.518317752 rssi 41
last primary: <3.21.201.60 - 4.21.200.80>
free ids: 7 6 5 4 3 2
current missing path mask: 1111110

HO Table
static  : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile  : 4.21.200.80 [FC:58:9A:15:B9:13]
rssi : 42
dop : 40
chan : 132/40
updated : 74
skip : 0

static  : 4.21.201.60 [FC:58:9A:15:C7:D3]
mobile  :  4.21.201.204 [FC:58:9A:15:E4:D3]
rssi : 41
dop : 40
chan : 100/40
updated : 18
skip : 0
rssi_delta : 6 3
threshold : 35
```

MPO Limitations

- Fast failover (< 500 ms) is not supported and planned in future releases.
- When MPO is enabled, some handoff features are not available:
  - Pole Ban and Pole Proximity
  - Coloring
  - Load balancing



CHAPTER 23

New Features in Cisco Catalyst IW Access Points, Release 17.12.1

The following URWB features are introduced in the release 17.12.1:

Enabling and Disabling Wired Interface

This feature allows wire interfaces to be disabled. It is not possible to disable both wire interfaces at the same time. Enable the wired interface configuration using CLI.

Enabling or disabling wired interface using CLI

To enable or disable specific wired interface, use the following CLI command:

```
Device# configure wired <0-1>
                disabled disable wired interface
                enabled enable wired interface
```

Example:

```
Device# configure wired 0 disabled
         Device# configure wired 1 enabled
         Device# write
         Device# reload
```

Error handling configuration

The following CLI commands shows the error when both interfaces are configured as disable mode:

```
Device # configure wired 0 disabled
         Device# configure wired 1 disabled
         ERROR: Interface wired0 is disabled, cannot disable both interfaces
```

Verifying enabling and disabling wired interface using CLI

To verify enable or disable state of wired interface, use the following show command:

```
Device# #show wired <0-1> config
```

Example:

```
Device# show wired 0 config
         WIRED0 status: enabled
Device# show wired 1 config
         WIRED1 status: disabled
```

Configuring Maximum Transmission Unit Settings

The maximum frame size that can be transported across the URWB network can be configured. This setting must be configured on every access point in the URWB network.

Configuring MTU setting using CLI

The following CLI command used for changing MTU value for wired interfaces:

```
Device# configure wired mtu
         <1530-1600> Unsigned integer set wired mtu
```

Example:

```
Device# configure wired mtu 1600
Device# write
Device# reload
```

Verifying MTU setting using CLI

To verify the MTU value for wired interfaces, use the following show command:

```
Device# show wired mtu
```

Example:

```
Device# show wired mtu
         Configured MTU: 1600
```

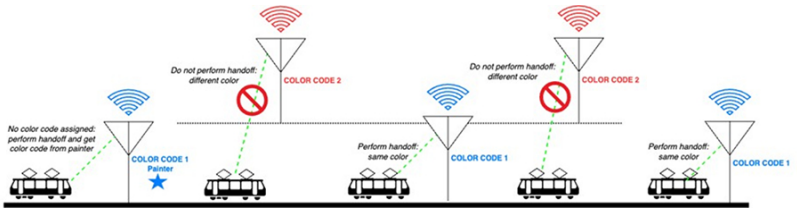
Configuring Fluidity Coloring

Fluidity Colouring enables wayside or outside devices (Fluidity infrastructure devices) to be given certain colour codes to enhance or drive the handoff process and with the standard configuration handoff decision is made based on RSSI (Received Signal Strength Indication).

Typical use case: When a train is travelling one side of the track in one direction (metro line with single tunnel for both track directions) and does not need to connect to the Access Point located on the opposite side of the tunnel, so mark the access point on each side with a different colour to prevent occasional handovers to infrastructure units on the opposite track.

Fluidity Coloring Logic

The following image explains the Fluidity coloring logic and painter is a key role for wayside or outside device (Fluidity infrastructure device):



The process of Fluidity coloring as follows:

- According to the colour code, painter notifies the Fluidity vehicle device which Fluidity infrastructure devices are suitable for the handoff.
- The Fluidity vehicle device ignores the colour settings and continues to use the standard handoff mechanism (based on RSSI level) until it detects a painter.
- The moment the Fluidity vehicle device completes the handoff on a Fluidity infrastructure device with the painter configuration, it starts only considering Fluidity infrastructure devices with the same colour code or other painters Fluidity infrastructure devices.
- Multiple Fluidity infrastructure devices acting as painters are allowed.

The following table explains the Fluidity color role and its corresponding options:

Table 5: Fluidity Coloring Role

Fluidity Coloring Role	Options
Wayside painter (Fluidity infstrastructure device)	Only one color code can be assigned to a Fluidity infstrastructure device configured as a painter
Wayside standard (Fluidity infstrastructure device)	A non-painter Fluidity infstrastructure device can be configured with multiple color codes
Fluidity vehicle	Only one color can be assigned to Fluidity vehicle device

Configuring Fluidity Coloring using CLI

To configure a fluidity color mode, use the following CLI command:

```
Device# configure fluidity color mode
                Disabled: disable coloring
                Enabled: enable coloring

Device# configure fluidity color value
WORD quoted list of colors from 1 to 7 or "p X" for painter (e.g. "1 2 6","4", "p 1").
"clear" to reset
```

Example (painter):

```
Device# configure fluidity color mode enabled
Device# configure fluidity color value "p 1"
Device# write
Device# reload
```

Example (non-painter):

```
Device# configure fluidity color mode enabled
Device# configure fluidity color value "3 4 5"
```

```
Device# write
Devie# reload
```

Example (clear):

```
Device# configure fluidity color value clear
Device# write
Device# reload
```

Verifying Fluidity Coloring using CLI

To verify a fluidity color mode, use the following CLI command:

```
Device# #show fluidity config
```

Example (painter):

```
Device# show fluidity config
                ...
                Color: enabled, current: p 1
                ...
```

Example (non-painter):

```
Device# show fluidity config
                ...
                Color: enabled, current: 3 4 5
                ...
```

Example (clear):

```
Device# show fluidity config
                ...
                Color: enabled, current: 0
                ...
```

Configuring Fluidity Coloring RSSI Threshold

The Fluidity vehicle device temporarily ignore the Fluidity colouring settings if there is a coverage hole and the current RSSI is less than the configured RSSI threshold. In this case, the Fluidity vehicle device keep it's Fluidity colouring settings and ignores them until it receives a handoff from a Fluidity infrastructure device that has the current colour code. The Fluidity vehicle device reset it's Fluidity colouring settings to the default value (no colour) after four consecutive handoffs on a Fluidity infrastructure device with colour codes different from the present value.

Configuring Fluidity Coloring RSSI Threshold using CLI

```
Device# configure fluidity color rssi-threshold
         <0-96> COLOR_RSSI_THRESHOLD
```

Example:

```
Device# configure fluidity color rssi-threshold 55
Device# write
Device# reload
```

Verifying Fluidity Coloring RSSI Threshold using CLI

```
Device# show fluidity config
```

Example:

```
Device# show fluidity config
                ...
```

```
Color: enabled, current: 0
Color min RSSI threshold: 55
```

Configuring IW Monitor Management

The URWB release 17.12.1 introduces support for IW Monitor. It is a stand-alone on-premise monitoring application supporting the following features:

Table 6: IW Monitor features support in release 17.12.1

Feature	Description
IW Monitor log for RADIUS (Remote Authentication Dial-In User Service)	Radius authentication attempts by mobile units are logged to IW Monitor
IW Monitor log CLI SSH access	SSH connections attempts are logged to IW Monitor
IW Monitor log Web UI access	Web UI logins are logged to IW Monitor
IW Monitor log ethernet link change	Physical link changes of LAN ports are buffered and logged to IW Monitor
IW Monitor log configuration change	Changes applied to the unit configuration through CLI or Web UI are logged to Monitor

The on-premises IW Monitor supports the following primary capabilities:

- Dashboard to monitor network status.
- Topology view of the network.
- Real time and history charts for wireless KPIS (Key Performance Indicators).
- Real time performance monitoring.
- Process the telemetry data sent by IW devices.
- Network events logging.

Release 17.12.1 provides following support for IW Monitor dashboard:

- Attach and detach functions.
- Telemetry protocol support.
- CLI and Web UI management.

Detaching IW Monitor Management using CLI

IW Monitor doesn't require any configuration, and access points are added to the IW Monitor. Use the following CLI to detach the device from the IW Monitor server and troubleshoot the connection.

```
Device# configure monitor
        detach : detach MONITOR action
```

Example:

```
Device# configure monitor detach
```

Verifying IW Monitor Management using CLI

To verify a monitor management, use the following show command:

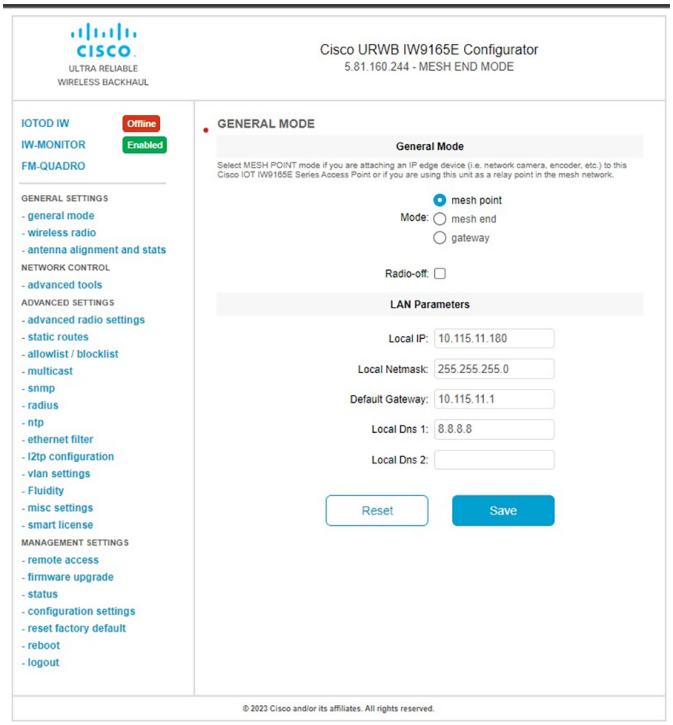
```
Device# show monitor
```

Example:

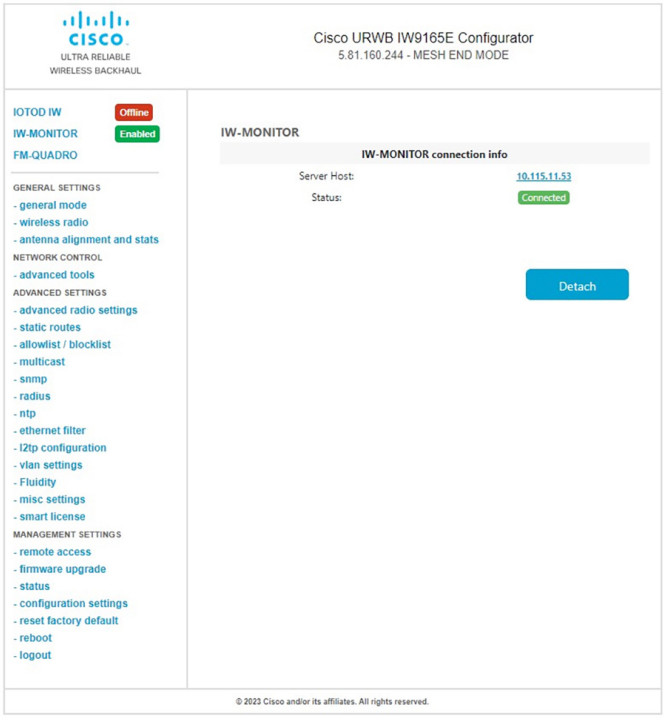
```
Device# show monitor
IW MONITOR: enabled
Status: Connected
```

Configuring IW Monitor Management using Web UI

The following image shows the **IW MONITOR** option is activated or enabled in the **Cisco URWB IW9165E or IW9167E Configurator** window to configure a IW Monitor management:



After enabling **IW-MONITOR** option, you can see **IW-MONITOR connection info** as shown in the following image:



Configuring URWB Telemetry Protocol

The URWB Telemetry Protocol allows for custom external monitoring of real-time wireless performance. Third-party and custom applications can be written to use this data. Pre-defined structured UDP packets sent at regular intervals contain various network metrics. Each access point exports data for its radios.

Each access point exports data for its radios. This data can be interpreted live by the receiving application or captured and processed later.

For more information about the protocol format, contact Cisco Support to request URWB Telemetry Protocol reference document..

The telemetry UDP packet contains the following information:

- Signal strength of packet.
- Packet throughput and migration rate.
- Number of transmission and retransmission.
- Modulation rate.
- Details of packet loss.
- Operating frequency of each radio.
- Information about the events that recording the network.

Configuration of URWB Telemetry Protocol Using CLI

By default, the telemetry data is disabled. To generate the telemetry packet, use the following CLI command:

To set the IP address and UDP port of the receiver, use the following CLI command (Multicast addresses are supported):

```
Device# configure telemetry server <dest IP [port]>
```

To enable or disable the URWB Telemetry Protocol transmission to the configured receiver, use the following CLI command (multicast addresses are supported):

```
Device# configure telemetry server <dest IP [port]>
```

To enable or disable raw UDP telemetry transmission to the configured server, use the following CLI command:

```
Device# configure telemetry export [ enable | disable ]
```

Example:

```
Device# configure telemetry export enable
Device # configure telemetry server 10.115.11.56 1234
Device # write
Device # reload
```

Note

- Make sure the IP address is configured before executing the **export enable** CLI command. If not, the command rejects with an error please configure the telemetry server IP first.
- The IP server is simultaneously set to 0.0.0.0 (the port value is unchanged) when you execute the **export disable** CLI command.

To verify telemetry configuration, use the following CLI command:

```
Device# show telemetry config
Telemetry export: enabled, current (live): disabled
Telemetry server: 10.115.11.56 1234, current (live): 0.0.0.0 30000
```

Live Configuration of URWB Telemetry Protocol Using CLI

```
Device# configure telemetry live
Export : enable/disable telemetry export
Server : set telemetry server IP address (and port)
```

Server configuration is mandatory before you enable the live telemetry export.

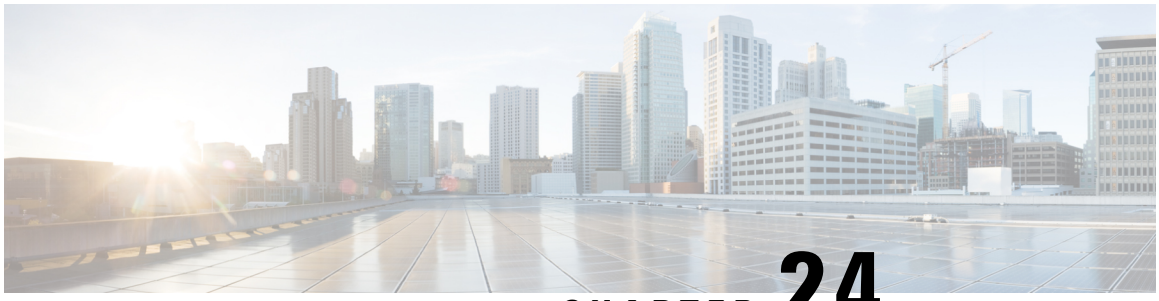
Example:

```
Device# configure telemetry live export enable
Error: please configure the telemetry server IP first
```

Example (telemetry export after server configuration):

```
Device# configure telemetry live server 10.115.11.56 1234
Device # configure telemetry live export enable
Device # show telemetry config
Telemetry export: enabled, current (live): enabled
Telemetry server: 10.115.11.56 1234, current (live): 10.115.11.56 1234
```

Note The command immediately affects the current configuration when the live modifier is specified. If live modifier is not used, only the configuration file is changed.



CHAPTER 24

LED Pattern for Catalysts IW9167 and IW9165

LED Pattern for Catalyst IW9167

The Catalyst IW9167E follows the below LED pattern during booting process (Blinking green) during a normal booting process:

Table 7: Definition of Booting LED Pattern

Events	LED State
Boot loader status sequence: DRAM memory test in progress DRAM memory test OK Board initialization in progress Initialization FLASH file system FLASH memory test OK Initializing Ethernet Ethernet OK Starting AP OS Initialization Successful	Blinking green
When you press the reset button for less than 20 seconds	Blinking red
When you press the reset button for more than 20 seconds	Solid red

Events	LED State
When reset button is released Or When you press the reset button for more than 60 seconds	Blinking green

Once the access point boots up, the Catalyst IW9167E follows these below LED patterns:

Table 8: Definition of URWB OS LED Pattern

AP State	LED State
General warning: Insufficient inline power	Cycling through red, green, and amber
Provisioning mode: Fallback	Blinking amber
Provisioning mode: DHCP	Amber
SNR(Signal to Noise Ratio) Excellent (>=25 dB)	Blinking green
SNR Good (15<=X<25 dB)	Fade-in green
SNR Bad (10<=X<15 dB)	Fade-in amber
SNR Unbearable (<10 dB)	Fade-in red

LED Pattern for Catalyst IW9165

The Catalyst IW9165E has tri-color red, green, and blue LED. The Catalyst IW9165D has red, green, and amber LED with three brightness levels. The access point is flexible with brightness levels. The controller CLI or GUI controls the brightness with eight different settings.

System LED's in the URWB stack have following patterns to indicate URWB states:

Table 9: LED pattern for URWB states

AP State	LED State
Fallback	Blinking amber or blue
DHCP	Amber or blue

RSSI LED

The Catalyst IW9165 supports a bi-color green and amber LED to show the RF Receive Signal Strength Indicator (RSSI). The RSSI LED does not have different brightness level.

Table 10: RSSI LEDs

Yellow LED	Green LED	Description
Blink	Off	RSSI < - 86 dBm
On	Off	RSSI is - 86 to - 81 dBm
Off	Blink	RSSI is - 81 to - 71 dBm
Off	On	RSSI > - 71 dBm

The following table shows the LED functionalities for the Catalyst IW9165E:

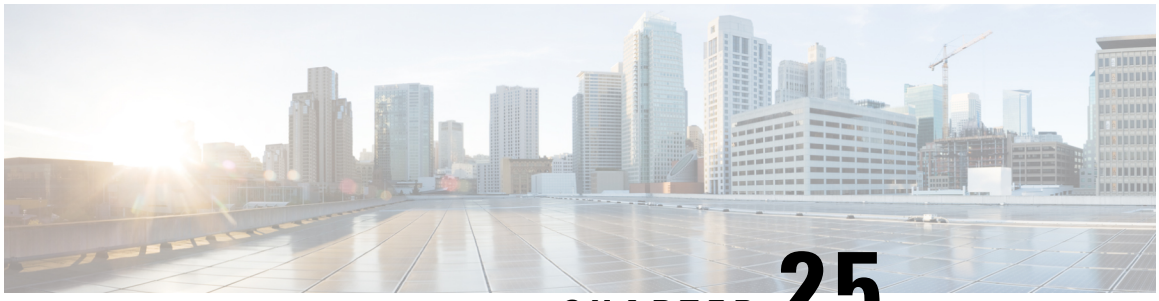
Table 11: URWB LED function for the Catalyst IW9165E

LED Function Label	Color/State	Description (Default = off)
System Status	Tricolor RGB	Indicates varies system status
RSSI	Yellow or Green	RSSI < - 86 dBm: yellow - 86 dBm =< RSSI =< - 81 dBM: blinking green RSSI > - 81 dBm: green
WAN GE	Green	Port is up with link
	Blinking Green	Link with activity
	Off	No link or port is Off
LAN GE	Green	Port is up with link
	Blinking Green	Link with activity
	Off	No link or port is Off
Digital IO 1-2	Yellow	Active as digital input or output
	Off	Inactive as digital input or output

The following table shows the LED functionalities for the Catalyst IW9165D:

Table 12: URWB LED function for the Catalyst IW9165D

LED Function Label	Color/State	Description (Default = off)
System Status	Tricolor RGA	Indicates varies system status
RSSI	Yellow or Green	RSSI < - 86 dBm: yellow - 86 dBm =< RSSI =< - 81 dBM: blinking green RSSI > - 81 dBm: green



CHAPTER 25

Fixed domains and country codes (ROW)

Configuring and Verifying Regulatory Domain from CLI

To configure country code for ROW (Rest of the World) domain, use the following CLI command:

```
Device# configure countrycode [countrycode]
```

Example:

```
Configure countrycode GB
```

The above CLI reports an error if the configured country code is not included in ROW and the wireless interface does not work properly if the country code is not configured.

Note Reboot the device before configuring other wireless parameters such as frequency, channel width, and after configuring country code. Setting the country code is only applicable for access points with the -ROW domain, such as IW9167EH-ROW.

To verify status of regulatory domain, use the following show command:

```
Device# show version | in Product
Product/Model Number: IW9167EH-ROW
```

To verify status of ROW (Rest of the World) country code, use the following show command:

```
Device# show dot11Radio <interface> config
```

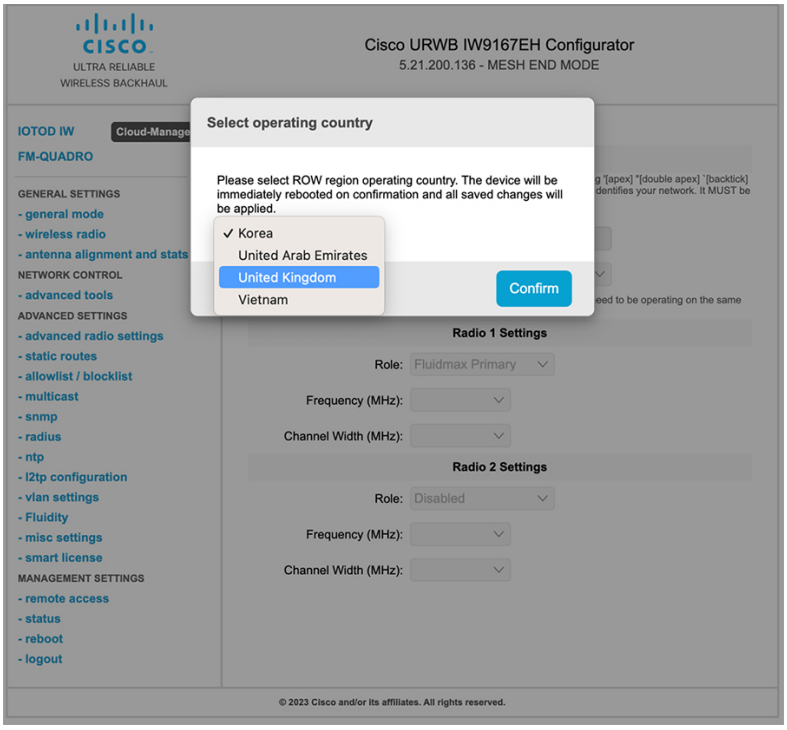
Example:

```
Device# show dot11Radio 1 config
…….
DFS region : GB
DFS radar role : auto
Radar Detected : 0
Indoor deployment: disable
```

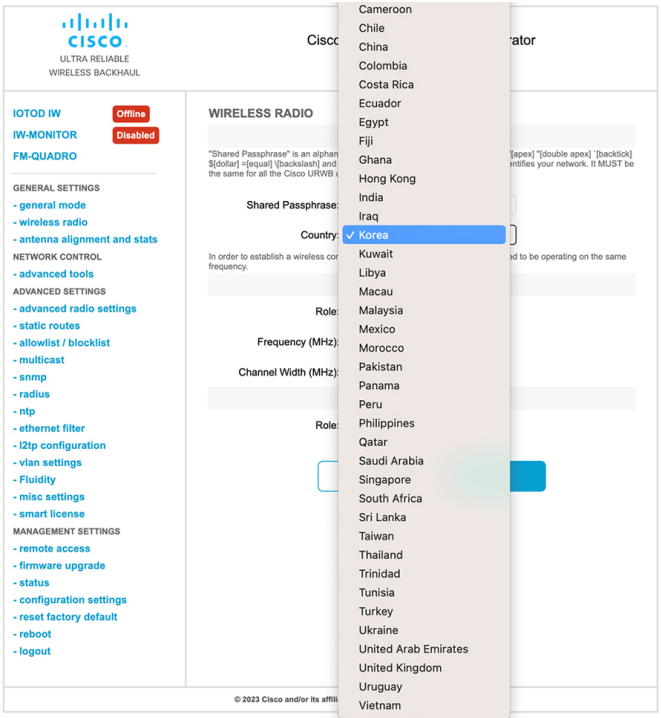
Configuring Regulatory Domain from GUI

Wireless interfaces fails to work if country code is not configured. To configure the regulatory domain:

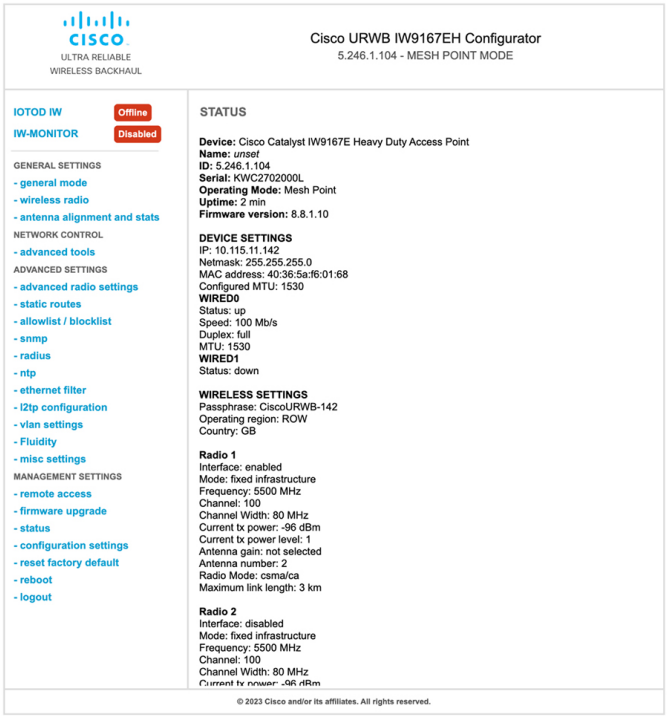
1. Click the **wireless radio** under **GENERAL SETTINGS** in the left-hand settings menu.
2. For ROW domain, if the country code is not selected, the following pop-up appears:



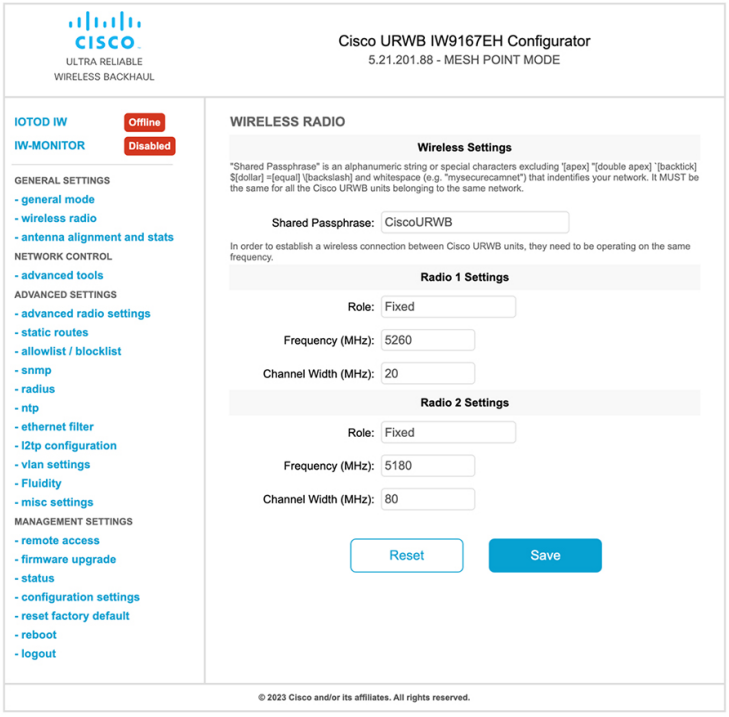
3. To select a country code, click the pop-up displays in the below image then it redirects to Web UI wireless section for selecting country code. In the **Wireless Settings** section, choose country from drop-down list. A confirmation pop-up appears.



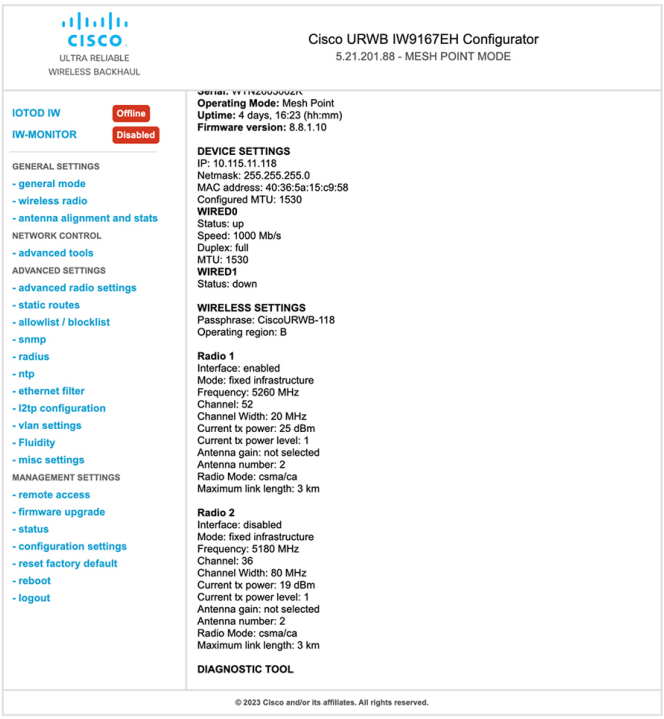
4. Click **Confirm**. A reboot confirmation screen appears.
5. Click **Yes**.
6. In the **MANAGEMENT SETTINGS**, click **status**. In the **STATUS** page, check the details of operating region and country for confirmation.



7. To establish a wireless connection between URWB devices, set a same operating frequency in radio units. Shared Passphrase must be the same for all the URWB devices belonging to the same network.



The below image shows the configuration of regularity domain from GUI:



Supporting Fixed Domains and Country Codes (ROW)

The ROW reg domain simplifies the domain management of the manufacturing process for all regulatory domains that do not have a specific domain mapped. The fixed domain and country code support for the Catalysts IW9167E, IW9165E, and IW9165D access points are described in this section.

Catalyst IW9167E Supported Fixed Domains

Domain	Indoor Deployment Support
A	No
B	*
E	Yes
F	No
Q	No
Z	No

Note Outdoor and indoor frequencies are the same for the B domain.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9167EH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9167E Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
KR (Korea)	No
VN (Vietnam)	*
GB (Great Britain)	Yes
IN (India)	No
PE (Peru)	No
PH (Philippines)	No

Note Only the listed country codes can be selected using CLI or Web UI.

For ROW domain, select the country code for the device to work.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9167EH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9165E Supported Fixed Domains

Domain	Indoor Deployment Support
A	Yes
B	*
E	Yes
Z	Yes

Note Outdoor and indoor frequencies are the same for the B domain.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9165E supports indoor deployment on domain A,E,Z and ROW(GB) only.
```

Catalyst IW9165E Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
GB (Great Britain)	Yes

Note Only the listed country codes can be selected using CLI or Web UI.

For ROW domain, select the country code for the device to work.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9165E supports indoor deployment on domain A,E,Z and ROW(GB) only
```

Catalyst IW9165D Supported Fixed Domains

Domain	Indoor Deployment Support
A	No
B	*
E	Yes
Z	No

Note Outdoor and indoor frequencies are the same for the B domain.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9165DH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9165DH Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
GB (Great Britain)	Yes

Note Only the listed country codes can be selected using CLI or Web UI.

For ROW domain, select the country code for the device to work.

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
                IW9165DH supports indoor deployment on domain E and ROW(GB) only.
```

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2023 Cisco Systems, Inc. All rights reserved.