Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.13.1

First Published: 2023-11-14

Last Modified: 2023-12-17

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

CHAPTER 1

CHAPTER 2

CHAPTER 3

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 Cisco Catalyst IW9167E, IW9165E, and IW9165D access points. UWRB is supported as part of the Unified Industrial Wireless (UIW) software. The release 17.13.1 introduces following new features:

- GNSS location information in the URWB Telemetry Protocol.
- TFTP firmware upgrade feature to perform an automatic firmware upgrade or a direct firmware upgrade.

Related Documentation

Documentation for the access point control and provisioning of wireless access points (CAPWAP) and workgroup bridge (WGB) modes of operation for the Catalyst IW9167 and IW9165 access points are available in the following URLs:

- Catalyst IW9167 Heavy Duty Access Point
- Catalyst IW9165E Rugged Access Point
- Catalyst IW9165D Heavy Duty Access Point

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

Initial Configuration of the Device in Provisioning Mode

Catalyst IW Access Points running Ultra-Reliable Wireless Backhaul (URWB) mode support configuration from Cisco IoT Operations Dashboard (IoT OD) or using local management interfaces. An access point (AP) with no configuration defaults to provisioning mode, which allows the initial configuration to be sent to the access point from IoT OD.

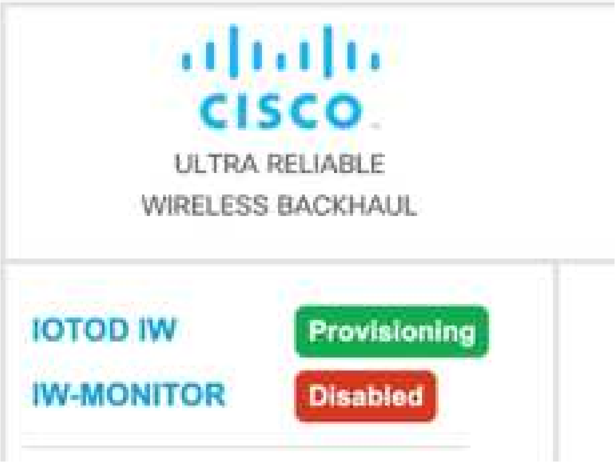
Provisioning mode is a special mode where the AP will attempt to request network configuration using dynamic host configuration protocol (DHCP) and connect to IoT OD. If network connectivity exists, the AP will connect to IoT OD. If there is no network connectivity, the AP can be configured locally using the Web UI or command line interface (CLI), accessible using the console port or SSH.

The DHCP server assigns a default gateway and domain name system (DNS) server. IoT OD uses DNS geo-location to direct AP in the United States to the US cluster. Other locations will be directed to the EU cluster. Ensure your IoT OD organization is configured to the correct cluster.

DHCP is only used in provisioning mode. A static IP address must be assigned for normal operation. If DHCP is unavailable and configuration through IoT OD is required, the IP address, subnet, default gateway, and DNS can be manually configured.

Note When the device is in provisioning mode, the AP attempts to get an IP address from a DHCP server. If the device fails to receive an IP address through DHCP, the AP reverts to a fallback IP address of 192.168.0.10/24.

- To verify if the device is in provisioning mode, go to the device configurator interface and check if the status of IoT OD IW is mentioned as provisioning in the green box:



ULTRA RELIABLE
WIRELESS BACKHAUL

IOTOD IW Provisioning

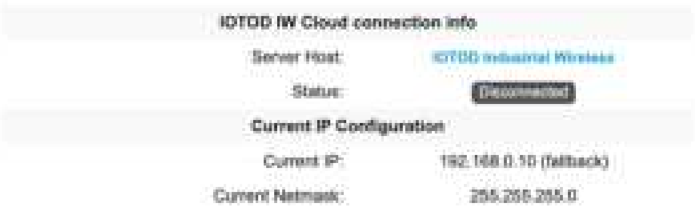
IW-MONITOR Disabled

- To verify if the device is in provisioning mode, use the following CLI command:

```
Device# show iotod-iw status
  IOTOD IW mode: Provisioning
  Status: Connected
```

- The device is in provisioning mode if the status of IoT OD IW is shown as **Provisioning**. Alternatively, if the status of IoT OD IW is shown as **Online** or **Offline**, choose between two further options:
  - To configure a new device, revert the wireless device to provisioning mode and reset the device, see Resetting the Device to Factory Default Using GUI, on page 8.
  - To change the connection settings with current configuration, see Configuring General Settings, on page 11.

If the device is in provisioning mode, the device configurator interface is shown as below:



IOTOD IW Cloud connection info

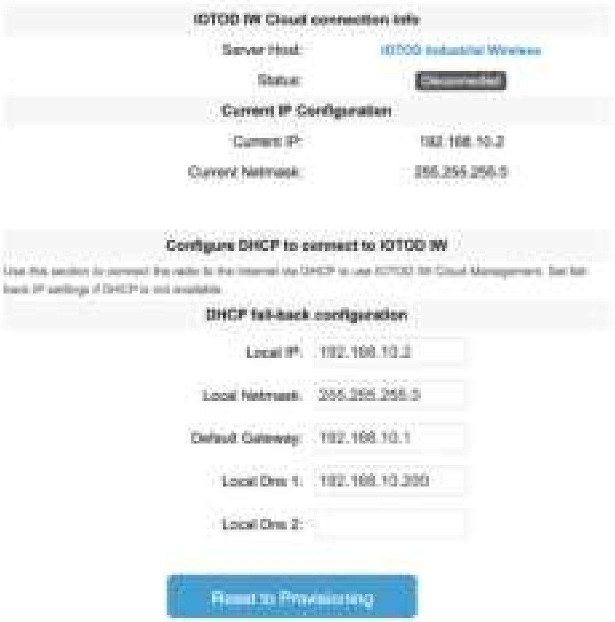
Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.0.10 (fallback)

Current Netmask: 255.255.255.0



IOTOD IW Cloud connection info

Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.10.2

Current Netmask: 255.255.255.0

Configure DHCP to connect to IOTOD IW

Use this section to connect the radio to the Internet via DHCP to use IOTOD IW Cloud Management. Set fall-back IP settings if DHCP is not available.

DHCP fall-back configuration

Local IP: 192.168.10.2

Local Netmask: 255.255.255.0

Default Gateway: 192.168.10.1

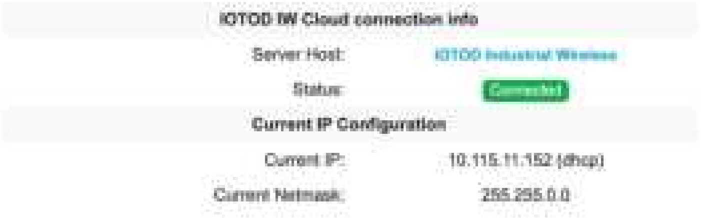
Local Dns 1: 192.168.10.200

Local Dns 2:

- When the device fails to receive an IP address from the DHCP server, it reverts to the fallback IP address (192.168.0.10/24).
- The device’s status and LEDs will blink continuously and LEDs will repeat this cycle until the device either enters a fallback condition, or enters **Online** or **Offline** mode. To know more about LED status, see LED Pattern for Catalyst IW9165, on page 126 or LED Pattern for Catalyst IW9167, on page 125.

Note DHCP is only used in provisioning mode. A static IP address must be assigned for normal operation.

Ensure that the device is connected to a network that supports DHCP. If the connection to IoT OD is successful, the cloud connection info status is shown as **Connected**.



IOTOD IW Cloud connection info

Server Host: IOTOD Industrial Wireless

Status: Connected

Current IP Configuration

Current IP: 10.115.11.152 (dhcp)

Current Netmask: 255.255.0.0

To configure a fallback address, use the following CLI command:

Note The IP, netmask, default gateway, primary DNS, and secondary DNS configuration (IP command) are allowed when provisioning mode is on.

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

For 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
```

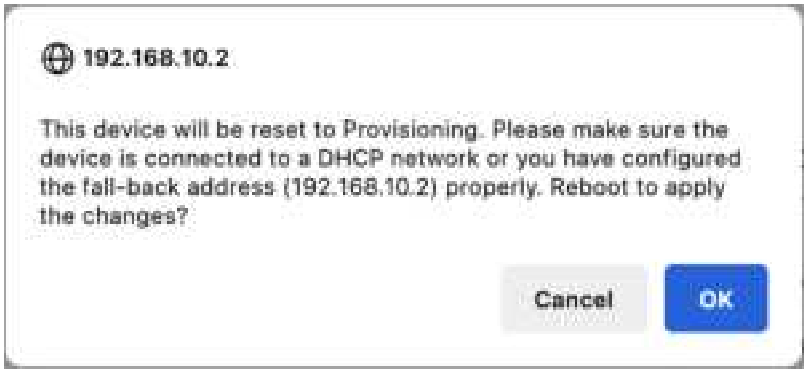
The device automatically sets the fallback address (192.168.0.10 by default or the configured IP address) if the device does not get an address from the DHCP server. If the device fails to connect to IoT OD IW, verify the following to reach IoT OD IW:

1. Check if the ethernet cable leading to the device is connected correctly.
2. Check if the local DNS server can fix the IP address of IoT OD IW cloud server and if the address can be reached.
3. Check if access point uses an outbound HTTPS connection on tcp/443 for the following domains:
    - device.ciscoiot.com
    - us.ciscoiot.com
    - eu.ciscoiot.com
4. If IoT OD IW is still offline, do a local (offline) configuration using the device's configurator interface.

If the device fails to connect to the network in provisioning mode, do the following:

1. Enter alternative **Local IP**, **Local Netmask**, **Default Gateway**, **Local Dns 1** and **Local Dns 2** values as needed, using IoT OD IW image and click the **Save fallback IP** button.

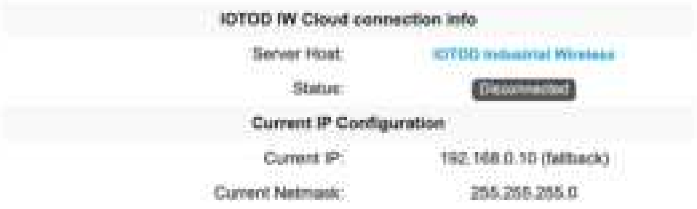
    A reboot confirmation pop-up appears:

    192.168.10.2

    This device will be reset to Provisioning. Please make sure the device is connected to a DHCP network or you have configured the fall-back address (192.168.10.2) properly. Reboot to apply the changes?

2. Click **OK** button or click **Reset** button to go back to IoT OD IW and adjust the settings.
    - If you click the **OK** button, the device reboots, but will remain in provisioning mode.
    - The device will attempt to connect to the network using the new connection values.
3. If the device cannot connect to the network using the **DHCP** settings, **IoT OD IW Cloud connection** info status shows as **Disconnected**.



IOTOD IW Cloud connection info

Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.0.10 (fallback)

Current Netmask: 255.255.255.0

.

4. To verify if the device is in provisioning mode and not connected to IoT OD, use the following CLI command:

```
Device#show iotod-iw status
 IOTOD IW mode: Provisioning
 Status: Disconnected
```

The following CLI example shows that the device is in provisioning mode and retrieved the IP address from the DHCP server:

```
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
```

The following CLI example shows the device in provisioning mode failing to retrieve the IP address from the DHCP server and using the default fallback IP address 192.168.0.10.

```
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
```

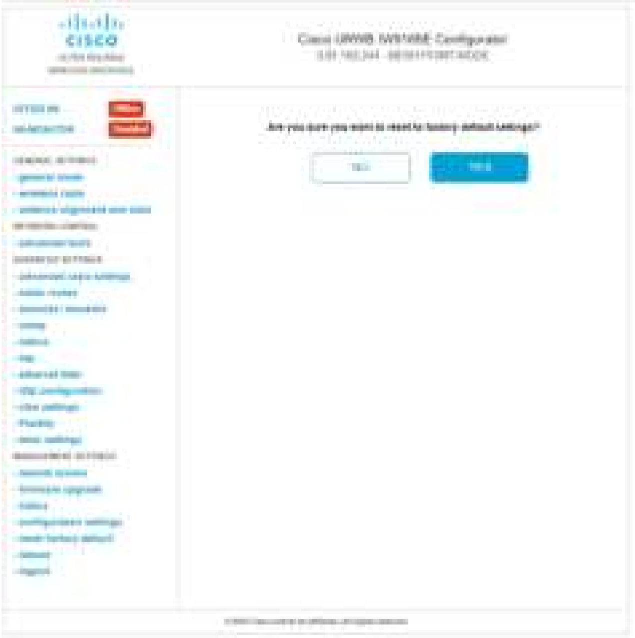
- Resetting the Device to Factory Default Using GUI, on page 8
- Rebooting the Device using GUI, on page 9
- Saving and Restoring the Device Settings, on page 10
- Configuring General Settings, on page 11
- Connecting to the Access Point Console Port, on page 12

Resetting 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 The hard reset will revert all device configuration settings, including the device IP address and administrator password to factory defaults. If you want to reboot the device instead, refer to Rebooting the Device using GUI, on page 9.

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



2. Click **YES** in the confirmation page. 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 as shown in Saving and Restoring the Device Settings, on page 10.

Note Do not do a hard reset unless the device needs to be reconfigured using its factory configuration as a starting point. A hard reset will reset the unit's IP address and administrator password and will disconnect the device from the network.

Resetting the Device to Factory Default Using CLI

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

```
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 perform reset of the 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 will be cleared as part of this process:

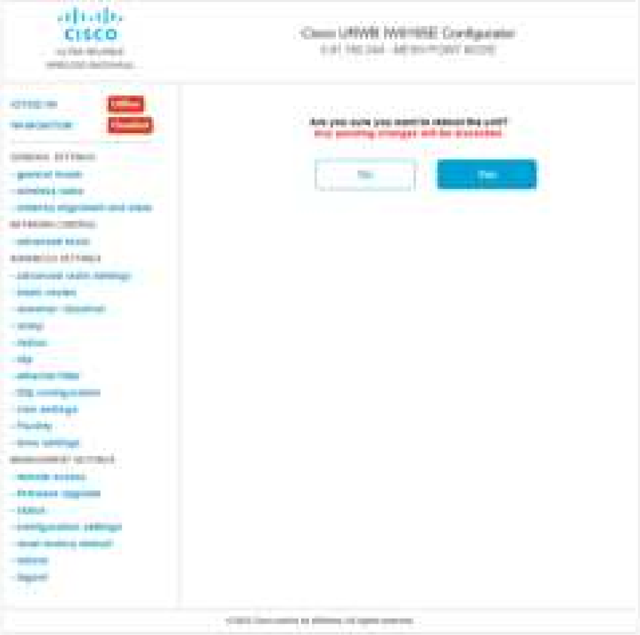
```
1) Config ,Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
5) Pktlogs
6) Manually created files
Do you want to proceed? (y/n)
```

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.

Rebooting the Device using GUI

To reboot the device (to re-start the device's operating system), do the following:

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



2. In the confirmation page, click **Yes**. To abort the reboot, click **No**.

Rebooting 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.

Saving and Restoring the Device Settings

Note Device software configuration files are not interchangeable with IoT OD configuration setup files.

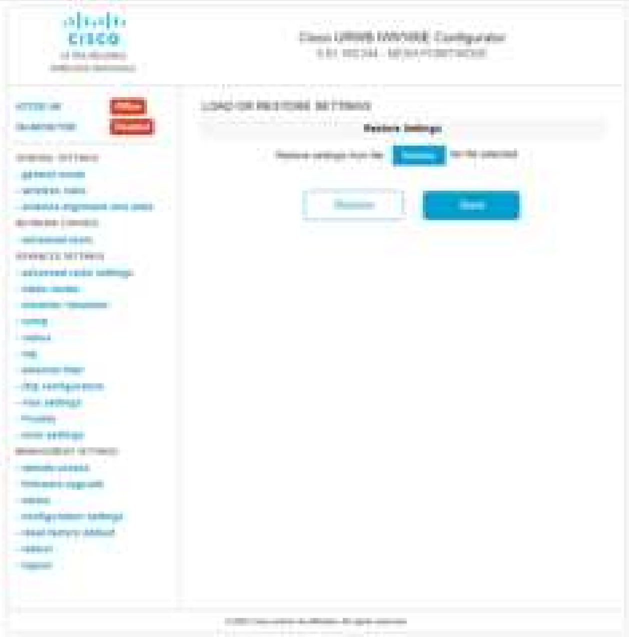
The **LOAD OR RESTORE SETTINGS** window allows you to:

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

Note Saved configuration files can be copied and used on multiple URWB units of the same type. Saved configuration files are used for configuration backup, which can speed up the redeployment if a damaged device is replaced with a device of the same type.

To download the device's existing configuration settings to your computer, do the following:

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



2. Click **Save** to download the device configuration (*.CONF) file to your computer.

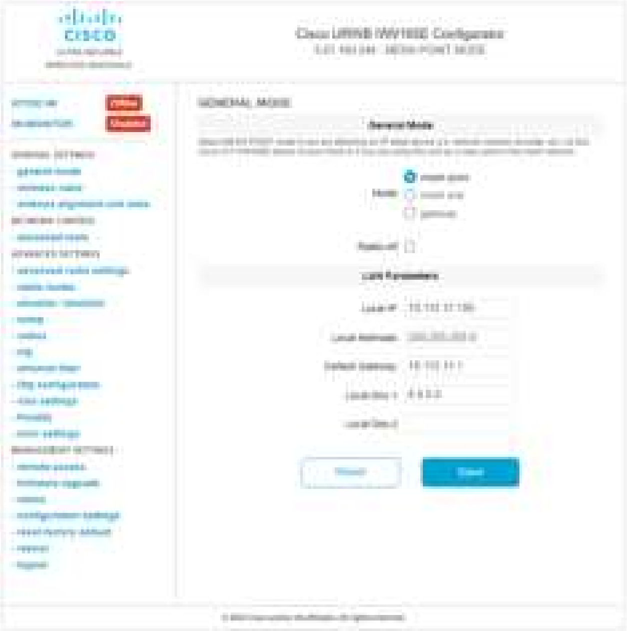
To upload a saved configuration file to the device, do the following:

1. Click **Browse** to find the configuration (*.CONF) file you want to upload to the device.
2. Click **Restore** to apply the configuration settings to the device.

Configuring General Settings

To change the **General Mode** settings, do the following:

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 unit. This device performs control and administrative functions, such as license management. This is necessary for correct network operation, even if the network consists only of two devices.

If needed, change the device's operational mode by clicking one of the following mode:

- **Gateway** - This mode is used for advanced Layer 3 mobility deployments and it is not used in most networks.
- **Mesh Point** - This mode is used 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 where 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.

Configuring 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
```

Changing the LAN Parameters

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

1. When the **General Mode** window is opened for the first time, the **Local IP** and **Local Netmask** LAN parameters will be 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**.

Configuring LAN Parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

```
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
```

Connecting to the Access Point Console Port

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. The following steps are used to open the CLI by connecting to the access point console port:

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. Use the following settings for the terminal emulator connection: 115200 baud rate, eight data bits, no parity, one stop bit, and no flow control.

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 the following default credentials to log in:

- Username: Cisco
- Password: Cisco

Note When your configuration changes are completed, you must remove the serial cable from the access point.

CHAPTER 3

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). URWB and WGB are both 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

Access points support two different software images access point OS which supports Catalyst Wi-Fi (AP) and Unified Industrial Wireless (UIW). To determine which software is running, use the following show command 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 software is running. If the show version displays `ap1g6j` or `ap1g6m`, it means the UIW software is running.

Run the following command to check if the access point is running in URWB mode:

```
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). The device's reset button needs to be pressed before it is turned on, not after device has been powered on and is operating.

- 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 from Wi-Fi mode (CAPWAP AP) to URWB mode and vice versa follow below procedures:

1. To convert from CAPWAP to URWB mode or from WGB/uWGB to URWB mode enter the following CLI command. Access Point will reboot and boot with URWB mode.

   ```
   configure boot mode urwb
   ```

2. To convert from URWB to CAPWAP mode or from WGB/uWGB to CAPWAP mode enter the following CLI command. Access Point will reboot and boot with Cisco CAPWAP Access Point mode.

   ```
   configure boot mode capwap
   ```

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

   ```
   configure boot mode wgb
   ```

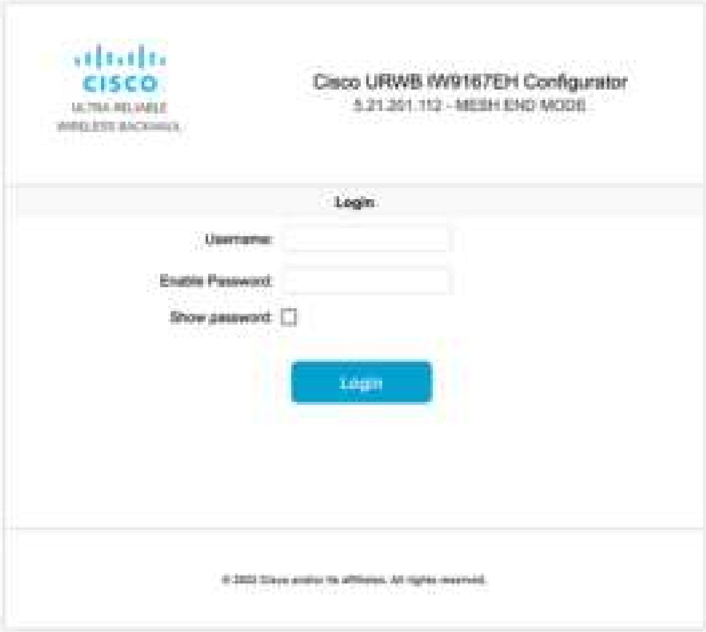
Note Image conversion performs full factory reset (any configuration and data will be removed completely).

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>/

2. After successfully open the login page, you will see the Catalyst IW9167E or IW9165 configurator as below.



ULTRA RELIABLE WIRELESS BACKHAUL

Cisco URWB IW9167EH Configurator

5.21.201.112 - MESH END MODE

Login

Username:

Enable Password:

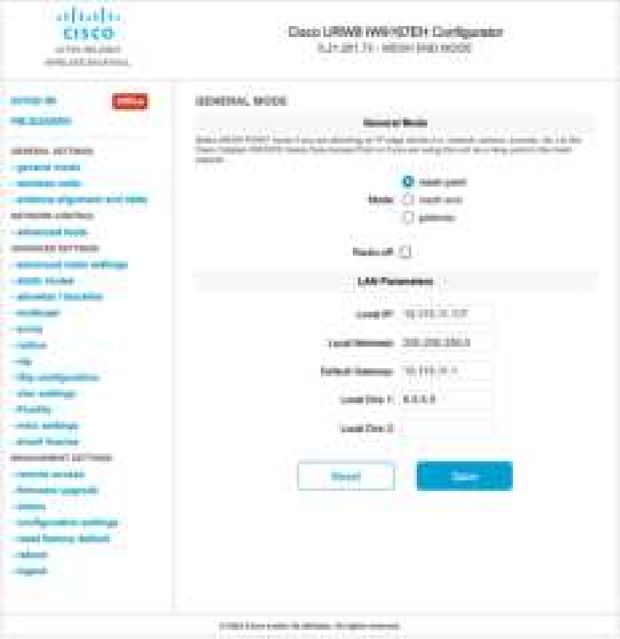
Show password: □

Login

© 2023 Cisco and/or its affiliates. All rights reserved.

3. To access the configuration page, use the credentials as follows: **Username** and **Enable password**.

4. After successfully logging into the Web UI, you will see the URWB configurator as shown:



Cisco URWB IW9167EH Configurator

GENERAL MODE

General Mode

Mode: ● mesh point ○ mesh end ○ gateway

Radio off □

LAN Parameters

Local IP:

Local Netmask: 255.255.255.0

Default Gateway:

Local Dns 1: 8.8.8.8

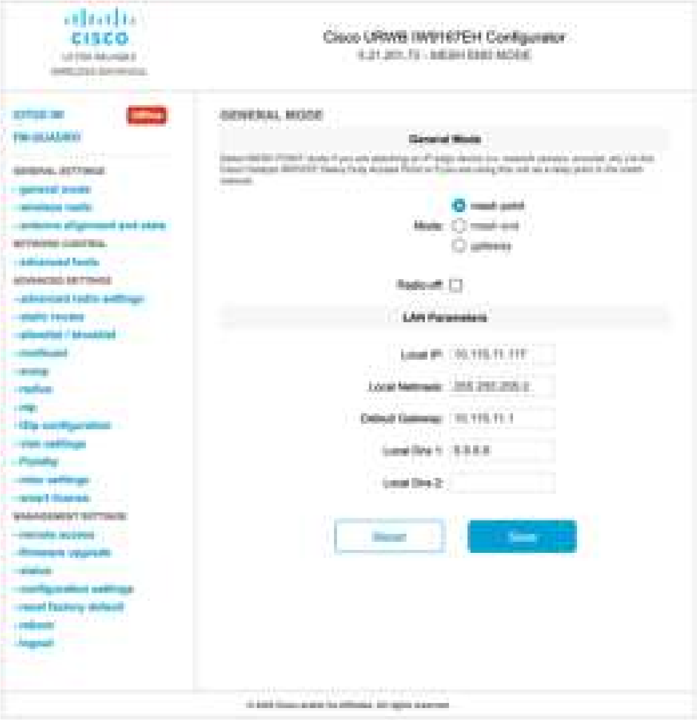
Local Dns 2:

Reset

Save

URWB Catalyst IW9167E Configuration from GUI

The following image shows the GUI configuration of URWB Catalyst IW9167E layout:



Mode: ● mesh point ○ mesh end ○ gateway

Radio off: □

Local IP: 10.115.11.111

Local Netmask: 255.255.255.0

Default Gateway: 10.115.11.1

Local Dns 1: 8.8.8.8

Local Dns 2:

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 so after the `write` command is entered, re-boot the device for the current configuration to take effect. To make the configuration effective, use the following CLI comments to write the configuration and reload the device.

```
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)

Configuring IoT OD Online and Offline Mode from CLI

IoT OD (IoT Operations Dashboard) is the cloud management portal, and the device is connected to the online cloud through the network. In offline mode the device is configured in local mode by CLI and web UI, 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 web UI.
- Configure the device on IoT OD cloud service and select the configuration file exported from IoT OD IW and upload the configuration file by using upload configuration button at the end of IoT OD IW management page.

To activate or deactivate IoT OD IW (IoT Industrial Wireless) configuration capability, use the following CLI command:

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

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

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

Configuring Password (after first login) from CLI

When the device is turned to offline mode, it is required to set a strong password for the device after the first login. To configure a strong password from the CLI, the username and password should follow the procedures listed below:

- The username length is between one and 32 characters.
- The password length should be from eight to 120 characters.
- The password must contain at least one uppercase character, one lowercase character, one digit, and one punctuation mark.
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not permitted:

  " [double quote]

  ' [single quote]

  ? [question mark]
- The password should not contain three sequential characters.
- The password cannot contain the same three characters consecutively.
- The password cannot be the same as or the reverse of the username.

- A new password cannot be the same as the current or existing password.

Example:

The default credential is,

```
username: Cisco

password: Cisco

enable password: Cisco
```

To reset the credential with strong password, use the following sample credentials:

```
username: demouser

password: DemoP@ssw0rd

enable password: DemoE^aP@ssw0rd
```

Example of configuring strong password from 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, Please reset credentials

```
Current Password:Cisco

Current Enable Password:Cisco

New User Name:demouser

New Password:DemoP@ssw0rd

Confirm New Password:DemoP@ssw0rd

New Enable Password:DemoE^aP@ssw0rd

Confirm New Enable Password:DemoE^aP@ssw0rd
```

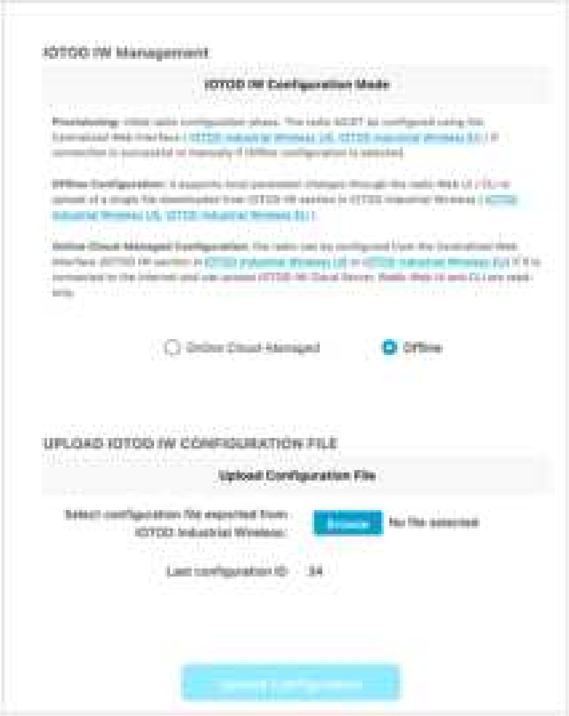
After credentials changed, Please re-login

```
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 real case or configuration, they are hidden behind asterisks (*).

Configuring IoT OD IW from GUI

The following image shows the GUI page of IoT OD IW management:



IOTOD IW Management

IOTOD IW Configuration Mode

Provisioning: Initial radio configuration phase. The radio MUST be configured using the Centralized Web Interface (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU) if connection is successful or manually if Offline configuration is selected.

Offline Configuration: it supports local parameter changes through the radio Web UI / CLI or upload of a single file downloaded from IOTOD IW section in IOTOD Industrial Wireless (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU).

Online (Cloud Managed) Configuration: the radio can be configured from the Centralized Web Interface (IOTOD IW section in IOTOD Industrial Wireless US or IOTOD Industrial Wireless EU) if it is connected to the internet and can access IOTOD IW Cloud Server. Radio Web UI and CLI are read-only.

○ Online Cloud-Managed ● Offline

UPLOAD IOTOD IW CONFIGURATION FILE

Upload Configuration File

Select configuration file exported from IOTOD Industrial Wireless: Browse No file selected

Last configuration ID: 34

CHAPTER 4

Configuring URWB Radio Mode

Configuring URWB Radio Mode

Each wireless interface can be configured to operate in a specific mode or disabled. Mode on Radio can be configured on the device will operate as a Fluidity or fixed infrastructure unit as specified by the parameter.

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

Table 1: Radio Mode Configuration

Radio Role	Mode on Radio*	Description
Fixed Infrastructure	Fixed Fluidmax primary Fluidmax secondary	P2P mode (point to point) P2MP (point to multipoint) mode (Fluidmax), P2MP P2MP mode (Fluidmax), 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 can be used according to 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. If radio-off is specified, all the wireless interfaces will be disabled.

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 MPLS (Multi-Protocol Label Switching) OSI layer. 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. Specify radio-off mode.

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

4. End of configuration.

   ```
   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 and procedure:

The below CLI commands used to select the operating function of the wireless interface also mixed Fluidity and fixed infrastructure combinations for different interfaces are allowed.

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 will operate in Fluidity mode, either as a mobility infrastructure or a vehice unit.

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

   Fluidmax - This interface will operate in Fluidmax P2MP mode. Additional parameters can be specified to configure the Fluidmax operating features (e.g., Primary/Secondary role, 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. End of configuration.

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

   ```
   Device# wr
   ```

Note When at least one interface is set to Fluidity mode, the unit will globally operate in Fluidity mode. If all interfaces are set to fixed, Fluidity will be disabled.

Configuring AMPDU using 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 commands:

```
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 commands:

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

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

Maxmcs values:

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

Word AUTO

Note The maximum MCS can be set between zero to nine if High Efficiency mode is disbled and maximum MCS can be set as 10 and 11 if High Efficiency mode is enabled.

Configuring Maximum Number of Spatial Streams Index from CLI

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

Set maximum spatial stream number in integer or string AUTO.

For AUTO, the background process automatically configures the maxnss.

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

Maxnss values:

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

Word AUTO

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

Configuring Rx-SOP Threshold from CLI

To configure Rx-SOP (Receiver Start of Packet) threshold, use the following CLI commands:

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

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

Configuring RTS Mode from CLI

To configure RTS (Ready to Send) mode, use the following CLI commands:

To disable RTS, use the following CLI command:

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

disable: disable rts protection.

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

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

threshold: threshold range <0 - 2346>.

Configuring WMM Mode from CLI

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

```
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 a NTP (Network Time Protocol) 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 a 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 NTP authentication md5|sha1 - authentication method.

Example:

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

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

password must be between 8 and 20 characters.

The following special characters are not allowed: ' [apex] " [double apex] ` [backtick] $ [dollar] = [equal] \ [backslash] # [number sign] and whitespace

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

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

To configure NTP timezone, use the following CLI command:

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

Example:

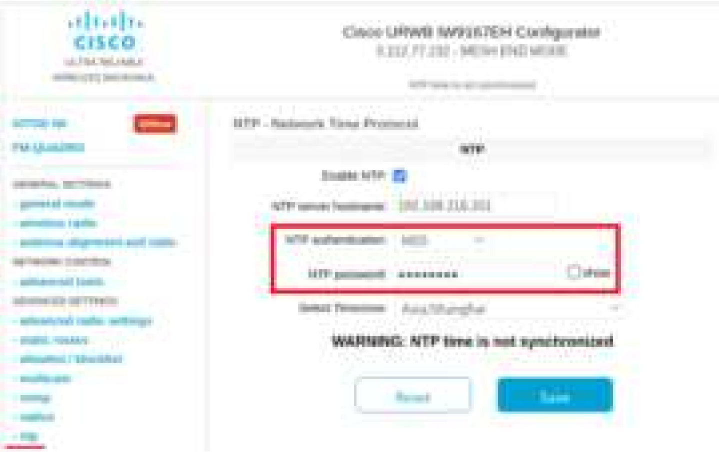
```
Device# configure ntp timezone Asia/Shanghai
```

To validate 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 from GUI

The following image shows the Web UI of NTP enhancement:



Cisco URWB IW9167EH Configurator

NTP - Network Time Protocol

NTP

Enable NTP ☑

NTP server hostname

NTP authentication MD5

NTP password ******** ○ show

Select Timezone Asia/Shanghai

WARNING: NTP time is not synchronized

Validating Radio Mode for URWB

To validate radio mode, use the following show commands:

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

Example:

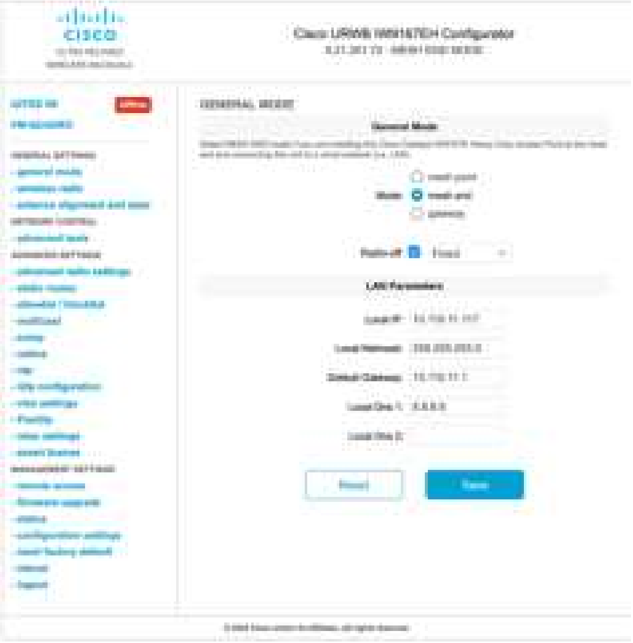
```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
Channel : 157
Channel width : 40 MHz
```

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

If need to change radio mode of vehicle access point (mobility client) to fixed or fluidmax, need to configure fluidity role as infrastructure by CLI configure fluidity id infrastructure.

Configuring Radio-off Mode from GUI

To configure a Radio-off mode, choose a fixed or fluidity mode as shown in the below image. Select a mesh end mode if you are installing the Catalyst IW9167E access point at the head end and connecting this unit to a wired network such as LAN.



Cisco URWB IW9167EH Configurator

GENERAL MODE

General Mode

Mode: ○ mesh point ● mesh end ○ gateway

Radio-off ☑ Fixed

LAN Parameters

Local IP: 10.115.11.117

Local Netmask: 255.255.255.0

Default Gateway: 10.115.11.1

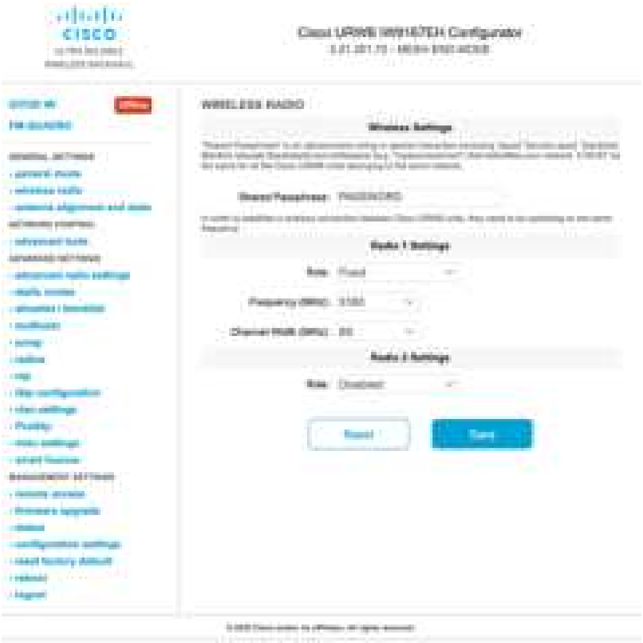
Local Dns 1: 8.8.8.8

Local Dns 2:

Configuring Radio Mode from GUI

To configure a radio mode from GUI, use the following procedures:

1. To establish a wireless connection the operating frequency should be same between the devices. To configure a Radio mode from GUI, set the operating mode for specified radio (Radio1 and Radio2) interface.



Cisco URWB IW9167EH Configurator

WIRELESS RADIO

Wireless Settings

Shared Passphrase: PASSWORD

Radio 1 Settings

Role: Fixed

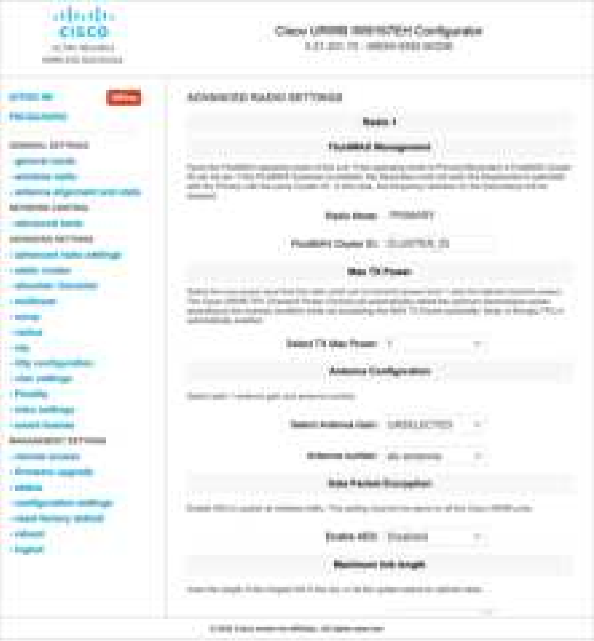
Frequency (MHz): 5180

Channel Width (MHz): 20

Radio 2 Settings

Role: Disabled

2. Set Radio 1 operating mode (role) as a Fluidmax Primary with FluidMAX Cluster ID. In this case the frequency selection on the Primary will be enabled and Secondary will be disabled. Select the maximum power level (power level 1 sets the highest transmit power) and URWB transmission power control (TPC) will automatically select the optimum transmission power.



ADVANCED RADIO SETTINGS

Radio 1

FluidMAX Management

Radio Mode: PRIMARY

FluidMAX Cluster ID: CLUSTER_ID

Max TX Power

Select TX Max Power: 1

Antenna Configuration

Data Packet Encryption

Enable AES: Disabled

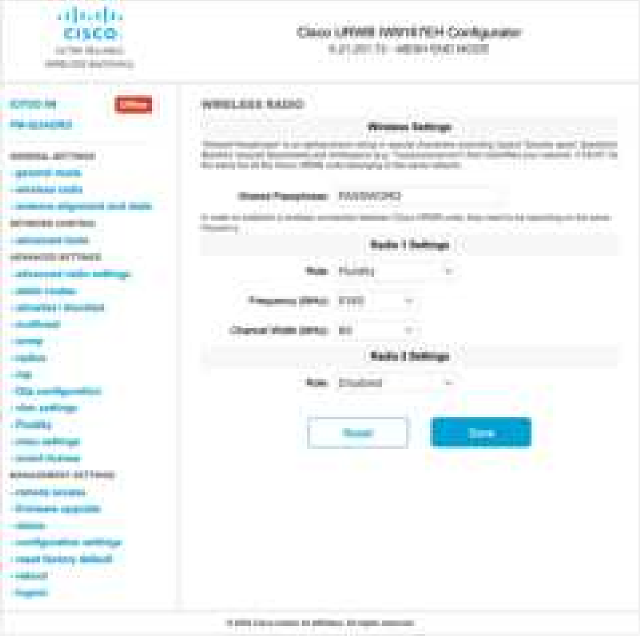
Maximum link length

> **Note** In Europe TPC is automatically enabled.

3. Set Radio 1 operating mode (role) as a Fluidmax Secondary with FluidMAX Cluster ID. If the FluidMAX Autoscan is enabled, the secondary units will scan the frequencies to associate with the Primary with the same Cluster ID. In this case the frequency selection on the Secondary will be disabled. Select the maximum power level (power level 1 sets the highest transmit power) and URWB transmission power control (TPC) will automatically select the optimum transmission power.

Note In Europe TPC is automatically enabled.

4. Choose unit role as Infrastructure when it 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. Choose network type set according to the general network architecture and choose flat mode if the network belongs single layer-2 broadcast domain or choose multiple subnets if the network belongs single layer-3 broadcast domain.



WIRELESS RADIO

Wireless Settings

[illegible]

Shared Passphrase: PASSWORD

[illegible]

Radio 1 Settings

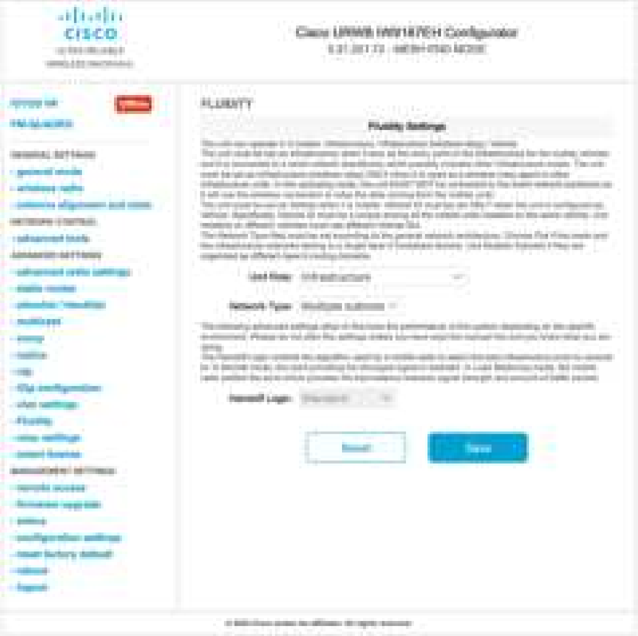
Role: Fluidity

Frequency (MHz): 5180

Channel Width (MHz): 40

Radio 2 Settings

Role: Disabled



FLUIDITY

Fluidity Settings

[illegible]

Unit Role: Infrastructure

Network Type: Multiple Subnets

[illegible]

Handoff Logic: Standard

CHAPTER 5

Configuring Radio Antenna Settings

Configuring Radio Antenna Settings

The Catalyst IW9167E supports eight external antennas with eight type-N female connectors to support multiple antenna options. The antenna ports 1, 4, and 5 can support self-identifying (SIA) antennas. 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 RP-SMA (f) connections. Radio 1 connects to antenna ports 1 and 2. Radio 2 connects to antenna ports 3 and 4. 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) connections. 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 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 will automatically configure the minimum supported antenna gain.

Note When a self-identifying antenna (SIA) is connected, gain is set 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 will automatically configure the maximum allowed power level 1 (8 is the lowest power level where as 1 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 6

Configuring Wired Interface

Enabling and Disabling Wired Interface

Configuring the wired interface is introduced from release 17.12.1 and this feature allows wire interfaces to be disabled. It is not possible to disable both wire interfaces at the same time. You can enable the wired interface using the 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
```

CHAPTER 7

Configuring and Validating Radio Channel and Bandwidth

Configuring Operating Channel from CLI

To configure operating channel, use the following CLI command:

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

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

2. Set the operating channel id between 1 to 256.

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

3. End of configuration mode.

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

   Example:

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

Configuring Channel Bandwidth from CLI

To configure channel bandwidth, use the following CLI commands and procedure:

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

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

2. Set channel bandwidth in MHz and currently supported bandwidth values are 20, 40, 80, 160 MHz. Radio 1 supports 20, 40 and 80 MHz bandwidths (example: configure dot11Radio 1 band-width). Radio 2 supports 20, 40, 80, and 160 MHz bandwidths (example: configure dot11Radio 2 band-width).

   ```
   Device# configure dot11Radio <interface> band-width [20|40|80|160]
   ```

3. End of configuration mode.

   ```
   Device (configure dot11Radio <interface> band-width [20|40|80|160])# end
   ```

   Example:

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

Validating Operating Channel and Bandwidth from CLI

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

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

Example:

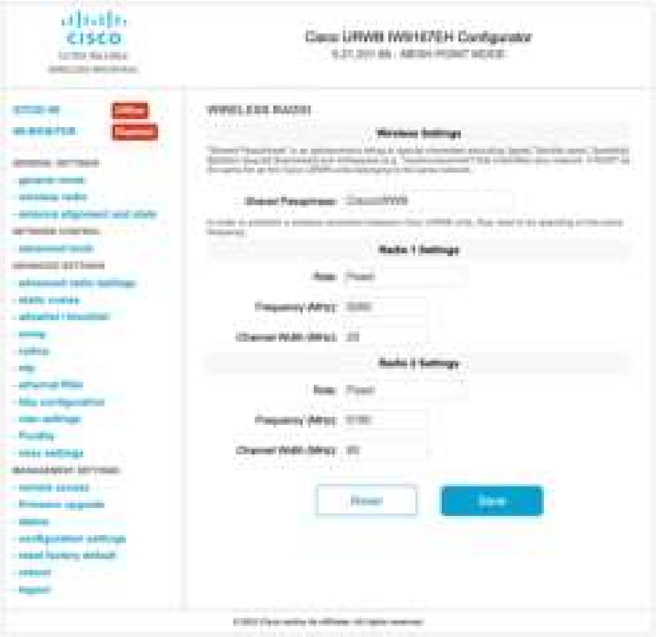
```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
```

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

Configuring Radio Channel and Bandwidth from GUI

To configure radio channel and bandwidth from GUI, set operating channel ID, radio mode as Fluidity or fixed infrastructure and set radio frequency range and bandwidth (supported bandwidth values are 20, 40, 80, 160 MHz) in MHz.

The below images show the configuration of radio channel and bandwidth.



Cisco URWB IW9167EH Configurator

WIRELESS RADIO

Wireless Settings

Shared Passphrase: CiscoURWB

Radio 1 Settings

Role: Fixed

Frequency (MHz): [illegible]

Channel Width (MHz): 20

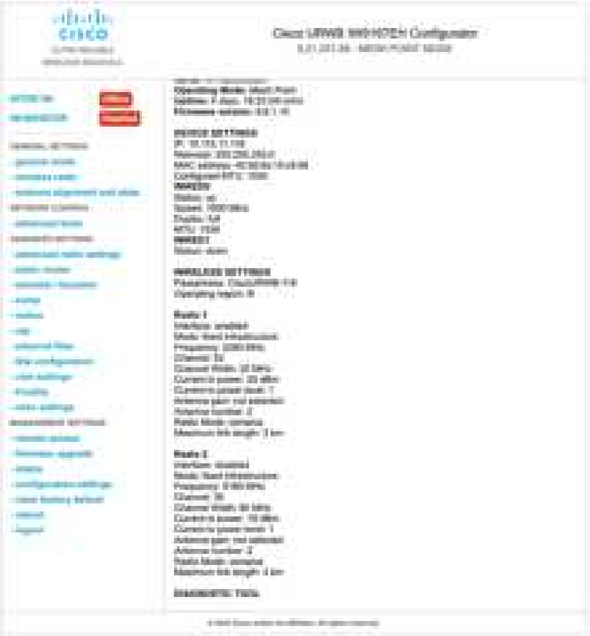
Radio 2 Settings

Role: Fixed

Frequency (MHz): [illegible]

Channel Width (MHz): [illegible]

The below image shows the status of radio channel and bandwidth configuration and specific information of each wireless interface.



Cisco URWB IW9167EH Configurator

Operating Mode: Mesh Point

DEVICE SETTINGS

WIRELESS SETTINGS

Radio 1

Interface: enabled

Radio 2

Interface: disabled

DIAGNOSTIC TOOLS

Configuring VLAN Settings

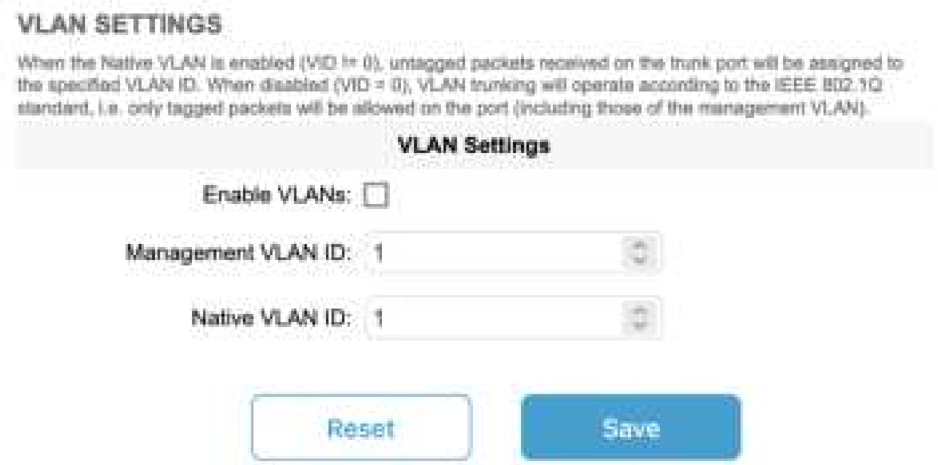
Default VLAN configuration parameters for the access point are:

Parameter	Default value
Management VLAN ID (MVID)	1
Native VLAN ID (NVID)	1

To connect the access point to a VLAN that is part of the local wireless network, follow these steps:

Step 1 In the **ADVANCED SETTINGS**, click **vlan settings**.

The **VLAN SETTINGS** window appears.



VLAN SETTINGS

When the Native VLAN is enabled (VID != 0), untagged packets received on the trunk port will be assigned to the specified VLAN ID. When disabled (VID = 0), VLAN trunking will operate according to the IEEE 802.1Q standard, i.e. only tagged packets will be allowed on the port (including those of the management VLAN).

VLAN Settings

Enable VLANs: □

Management VLAN ID: 1

Native VLAN ID: 1

Step 2 Check the **Enable VLANs** checkbox to connect the access point to a VLAN that is part of the local wireless network.

Step 3 Enter the management identification number of the VLAN in the **Management VLAN ID** field. For detailed info about vlan settings and packet management, see Rules for Packet Management.

Note The same Management VLAN ID must be used on all the access points that are part of the same mesh network.

Step 4 Enter the native identification number of the VLAN in the **Native VLAN ID** field.

Step 5 Click **Save**.

Rules for Packet Management

Traffic Management

The incoming data packets are classified based on the following parameter values:

Access port rules management for incoming packets with an access point in smart mode	
Untagged packet	If native VLAN is ON, then the packet is allowed (tagged with NVID) If native VLAN is OFF, then the packet is dropped
Tagged packet (any VID without any check)	Packet allowed with original tag

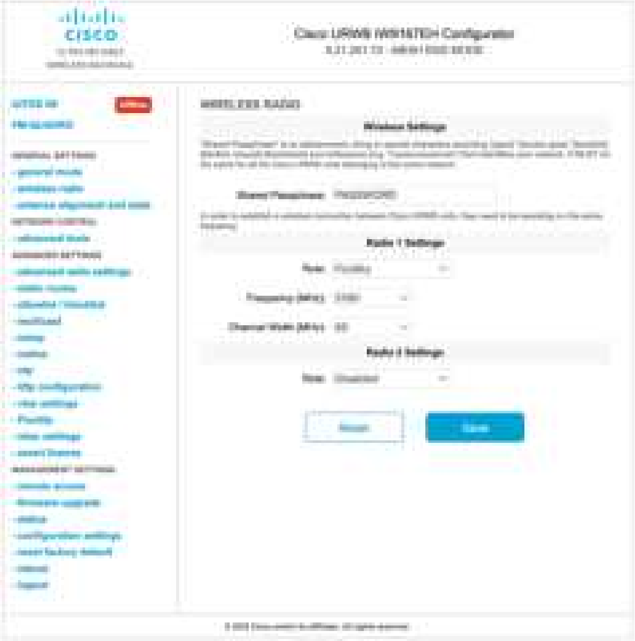
Access port rules management for outgoing packets with an access point in smart mode	
Packets from the access points (for example: IoT OD IW interface)	Packet tagged with MVID
Signaling traffic	Packet tagged with MVID
Tagged with valid VID (1–4094), but not with NVID	Packet allowed (tagged)
Tagged with null VID (0) or NVID	Packet allowed (untagged)

Note The packets transmitted through the Cisco VIC SFP+ interface is always tagged with a VLAN header. The interface transmits outgoing packets are classified as untagged with an IEEE 802.1p header with a VLAN ID tag of 0.

Configuring Fluidity using GUI

To configure a Fluidity mode from GUI, follow the below scenarios:

Set the radio role to Fluidity as shown:



Wireless Settings

Shared Passphrase: PASSWORD

Radio 1 Settings

Role: Fluidity

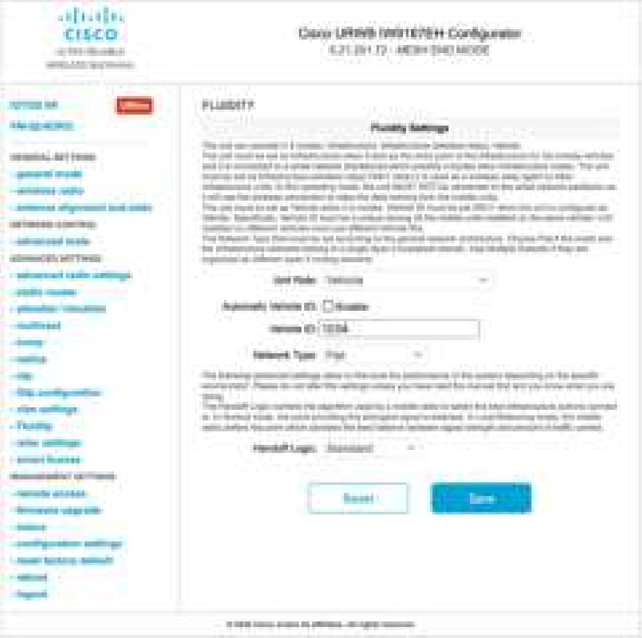
Frequency (MHz): 5180

Channel Width (MHz): 20

Radio 2 Settings

Role: Disabled

After setting radio role as Fluidity, make unit role as one of following mode that is infrastructure, infrastructure (wireless relay) and Vehicle. Vehicle ID must be a unique among all the mobile units installed on the same Vehicle and if unit installed on different vehicles must use different Vehicles ID's. Vehicle ID set automatically for mobile units if automatic vehicle ID enabled.



Cisco URWB IW9167EH Configurator

5.21.201.72 - MESH END MODE

FLUIDITY

Fluidity Settings

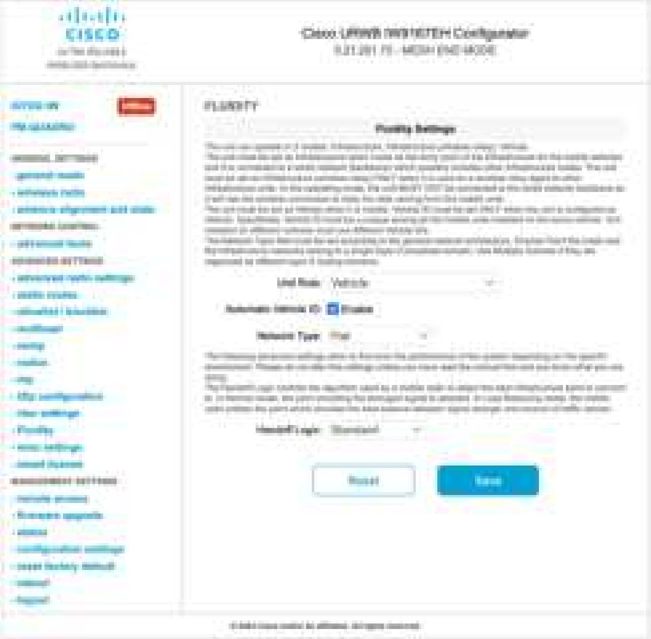
Unit Role: Vehicle

Automatic Vehicle ID: □ Enable

Vehicle ID: 1234

Network Type: Flat

Handoff Logic: Standard



Cisco URWB IW9167EH Configurator

5.21.201.75 - MESH END MODE

FLUIDITY

Fluidity Settings

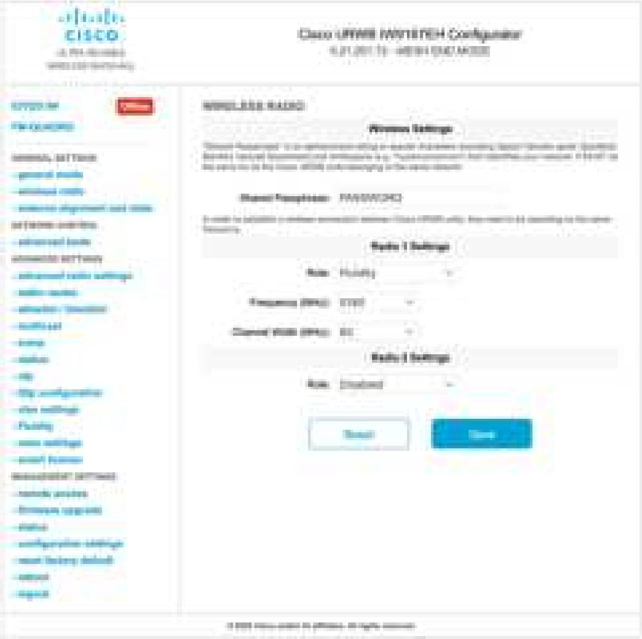
Unit Role: Vehicle

Automatic Vehicle ID: ☑ Enable

Network Type: Flat

Handoff Logic: Standard

The below GUI Fluidity configuration shows wireless interface unit role configured as infrastructure mode.



WIRELESS RADIO

Wireless Settings

Shared Passphrase: PASSWORD

Radio 1 Settings

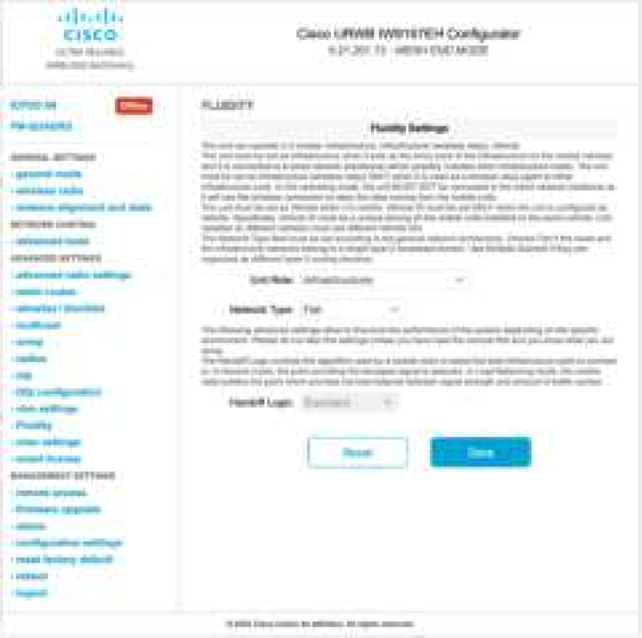
Role: Fluidity

Frequency (MHz): 5180

Channel Width (MHz): 80

Radio 2 Settings

Role: Disabled



FLUIDITY

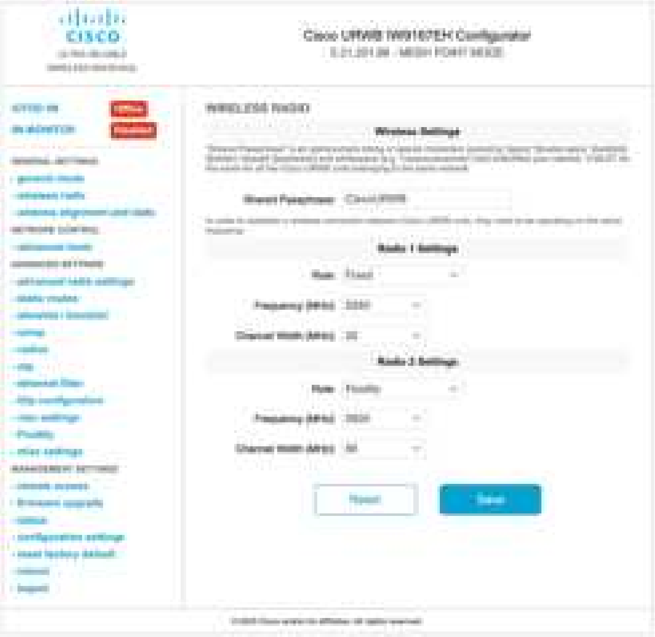
Fluidity Settings

Unit Role: Infrastructure

Network Type: Flat

Handoff Logic: Standard

The below GUI 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.



Cisco URWB IW9167EH Configurator

WIRELESS RADIO

Wireless Settings

Shared Passphrase: CiscoURWB

Radio 1 Settings

Role: Fixed

Frequency (MHz): [illegible]

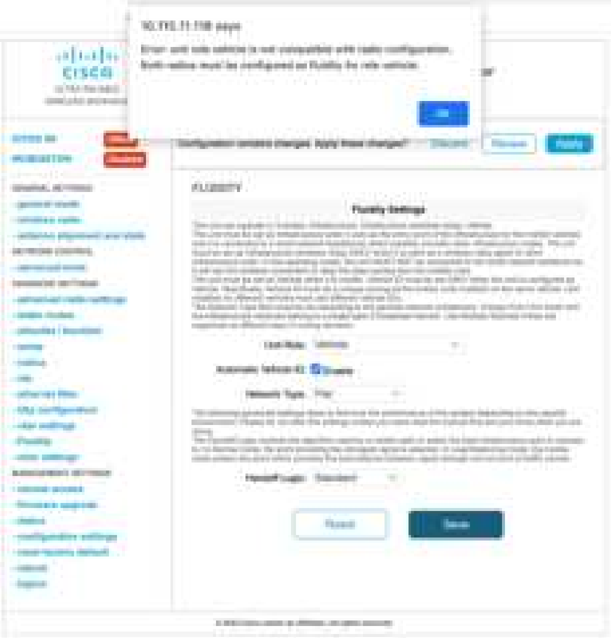
Channel Width (MHz): 20

Radio 2 Settings

Role: Fluidity

Frequency (MHz): [illegible]

Channel Width (MHz): 40



10.115.11.118 says

Error: unit role vehicle is not compatible with radio configuration. Both radios must be configured as fluidity for role vehicle.

FLUIDITY

Fluidity Settings

Unit Role: Vehicle

Automatic Vehicle ID: ☑ Enable

Network Type: Flat

Handoff Logic: Standard

Configuring Fluidity Using CLI

To enable fluidity, at least one radio interface should be in fluidity mode. Following are the available modes that can be selected:

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

Example of enabling 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 Fluidity CLI commands and procedure:

1. Configure the Fluidity role (infrastructure or mobile)

   ```
   Device# configure fluidity id
   ```

2. Configure Fluidity id mode

   ```
   Device# configure fluidity id {mode}
   Mode will be 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. End of configuration.

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

   ```
   Device# wr
   ```

   Example:

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

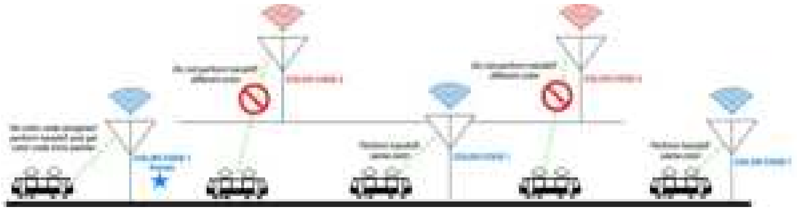
Configuring Fluidity Coloring

Fluidity Colouring is introduced from release 17.12.1. It 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 4: 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
```

CHAPTER 8

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 20/40/80 MHz bandwidth for slot 1.
- URWB HE supports 20/40/80/160 MHz bandwidth for slot 2.
- URWB HE defaults setting is disabled.
- HE negotiation is only supported between devices with HE enabled.

To enable High Efficiency mode, use the following CLI commands:

```
Device# configure dot11Radio [1|2] high-efficiency enable
Device# configure dot11Radio [1|2] mcs maxmcs <mcs index in integer or string>
```

Note Need to configure maxmcs as 11 by CLI configure dot11Radio 1/2 mcs maxmcs 11 since default maxmcs is 9.

To disable High Efficiency mode, use the following CLI commands:

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

To validate High Efficiency 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:

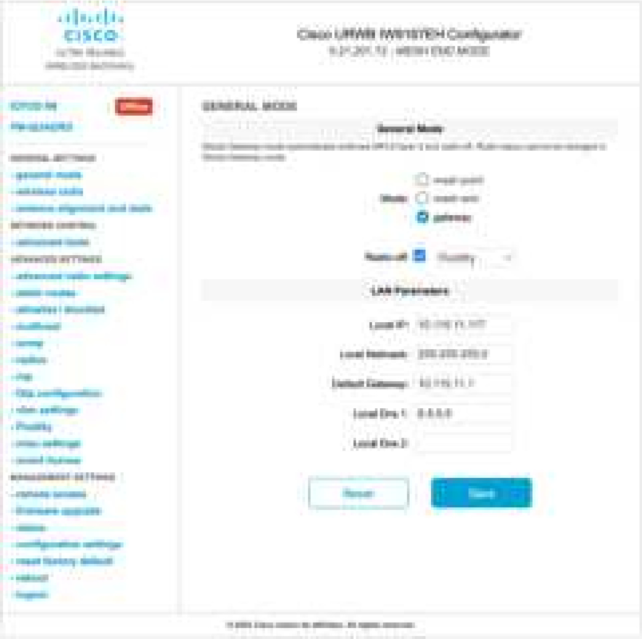
```
FC:58:9A:16F8:13 rate 1201 MCS 11/2 HE80/G1(800ns) ssn 50 rssi-46 received
```

WLAN2 Tx:

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

Configuring Global Gateway from GUI

Global gateway mode automatically enforces MPLS (Multi-Protocol Label Switching) layer 3 and radio-off and radio status cannot be changed in global gateway mode. The below images show the GUI configuration of global gateway mode.



Cisco URWB IW9167EH Configurator

[illegible] | MESH END MODE

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

Mode: ○ mesh point ○ mesh end ● gateway

Fluidity: ☑

LAN Parameters

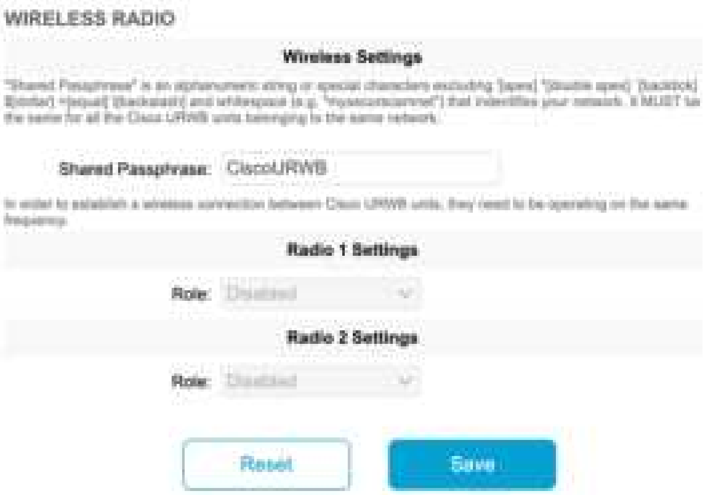
Local IP: [illegible]

Local Netmask: 255.255.255.0

Default Gateway: [illegible]

Local Dns 1: 8.8.8.8

Local Dns 2:



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. "mysecurecommet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase: CiscoURWB

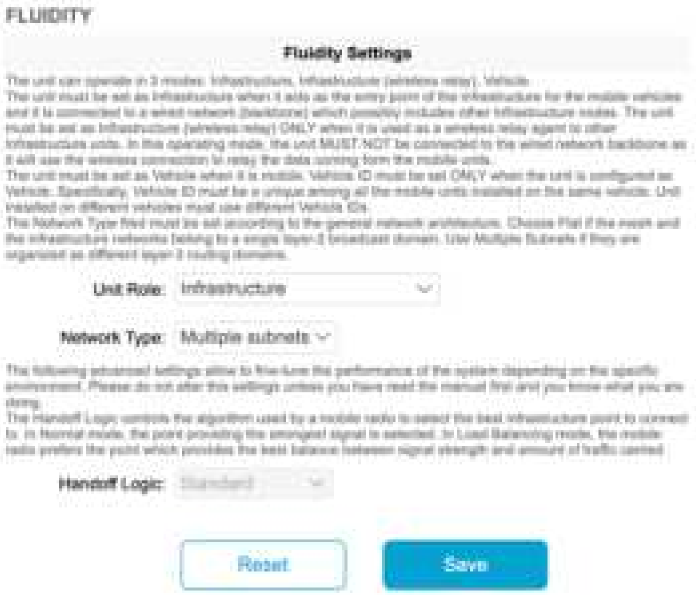
In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.

Radio 1 Settings

Role: Disabled

Radio 2 Settings

Role: Disabled



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 field 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

CHAPTER 9

Configuring Guard Interval for HE (High Efficiency)

Configuring Guard Interval for HE (High Efficiency)

Longer guard intervals improve link reliability for longer range outdoor deployments and this features like guard interval supports URWB stacks.

To configure a guard interval, use the following CLI commands.

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

gi will be one of the following values

1600 - Configure 1600 ns guard interval (only in HE mode)

3200 - Configure 3200 ns guard interval (only in HE mode)

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

800 - Configure 800 ns guard interval (default guard interval mode and disabled mode in HT, VHT, 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 CLI 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
Maximum tx nss : 2
```

```
RTS protection : disabled
guard-interval : 3200 ns
```

CHAPTER 10

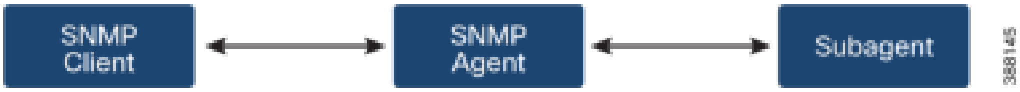
Configuring and Validating SNMP

Configuring and Validating SNMP

SNMP (simple network monitoring protocol) applications used in URWB software for network management functionalities.

The following illustration shows the SNMP process. SNMP agent receives a request from SNMP client, and it passes the request to the subagent. The subagent then returns a response to the SNMP agent and the agent creates an SNMP response packet and sends the response to the remote network management station that initiated the request.

Figure 1: SNMP Process



Configuring SNMP from CLI

The following CLI commands are used for SNMP (Simple Network Monitoring Protocol) configuration.

Note

- SNMP CLI logic modified for SNMP configuration, all parameters of SNMP are required to be configured before enable SNMP feature by CLI: configure snmp enabled.
- All the related configurations of SNMP will be removed automatically when disable SNMP feature.

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
```

SNMP is disabled and all sensitive information and credentials have been cleared. Please respecify all valid values to enable SNMP again.

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 a SNMP, use the following show commands.

Show SNMP info:

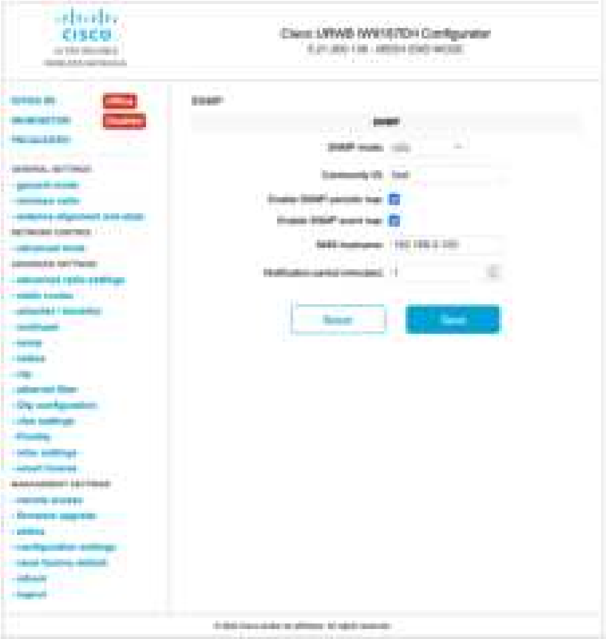
```
Device# show snmp
SNMP: enabled
Version: v3
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
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 Version v2c using GUI

By default, the access points are shipped from the factory with SNMP in disabled mode.

To change the access point's SNMP mode to version **v2c** and configure the access point, follow these steps:

Step 1 Choose the version **v2c** from the **SNMP mode** drop-down list.
The **SNMP** window appears.



SNMP mode:
Community ID:
Enable SNMP periodic trap: ☑
Enable SNMP event trap: ☑
NMS hostname:
Notification period (minutes): 1

Step 2 Enter the community identity value in the **Community ID** field.

Important The same community identity value must be set for all the access points in the network.

Step 3 Check the **Enable SNMP event trap** check box to enable SNMP event traps for significant system-related events, and then enter the network management station (NMS) host name in the **NMS hostname** field.

Important The NMS host to which traps are sent must have an SNMP agent that is configured to collect SNMP v2c traps.

Step 4 Check the **Enable SNMP periodic trap** check box to enable periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.

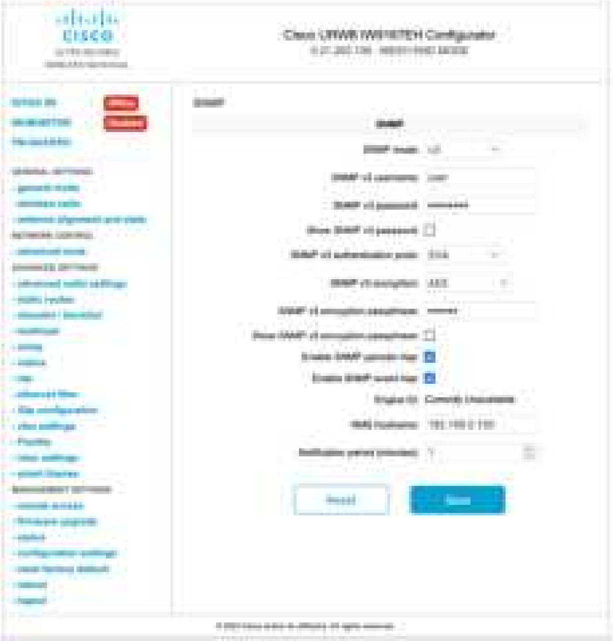
Step 5 Click **Save**.

Configuring SNMP Version v3 using GUI

By default, the access points are shipped from the factory with SNMP in disabled mode.

To change the access point's SNMP mode to version **v3** and then configure the access point, follow these steps:

Step 1 Choose the version **v3** from the **SNMP mode** drop-down list.
The **SNMP** window appears.



Step 2 Enter the SNMP v3 username in the **SNMP v3 username** field.

Note The same SNMP v3 username must be set for all the access points in the network.

Step 3 To change the current SNMP v3 password, enter the new password in the **SNMP v3 password** field.

Step 4 Choose the authentication type from the **SNMP v3 authentication proto** drop-down list. The available options are:

- **MD5**
- **SHA**

Important The same SNMP authentication protocol must be set for all the access points in the network.

Step 5 Choose the appropriate encryption protocol from the **SNMP v3 encryption** drop-down list. The available options are:

- **No Encryption**
- **DES** (Data Encryption Standard)
- **AES** (Advanced Encryption Standard)

Note The same encryption protocol must be set for all the access points in the network.

Step 6 To change the encryption passphrase, enter a new passphrase in the **SNMP v3 encryption passphrase** field.

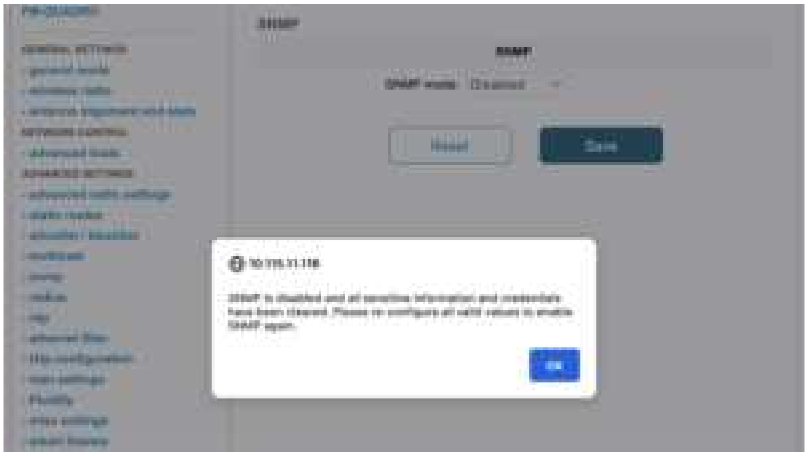
Step 7 Check the **Enable SNMP periodic trap** check box to enable the periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.

Step 8 Check the **Enable SNMP event trap** check box to enable the SNMP event traps for significant system-related events and then enter the host name of NMS in the **NMS hostname** field.

Note The NMS host to which traps are sent must have an SNMP agent configured to collect v3 traps.

Step 9 Click **Save**.

Note If you disable the SNMP, the following pop-up appears:



SNMP mode: Disabled

SNMP is disabled and all sensitive information and credentials have been cleared. Please re-configure all valid values to enable SNMP again.

CHAPTER 11

Configuring and Validating Key Controller (Wireless Security)

Configuring and Validating Key Controller (Wireless Security)

To support wireless security to standard WPA protocols, a key rotation strategy has been implemented on Catalyst IW9167E.

The key controller protocol can be described as a packet exchange between two devices, in which different stages of the process correspond to different states of each device, and the algorithm flow is controlled by a set of timers scheduled periodically to generate new PTK/GTK (Pairwise Transient Key/Group Transient Key) for packet encryption. The more often keys are updated, the less information is leaked in case of attack.

Configuring Key Controller from CLI

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

1. To enable AES (Advanced Encryption Standard) 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 AES disabled by default. Config should be the same on all devices.

Validating Key Controller from CLI

To validate a key controller, use the following show commands.

show key controller config:

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

CHAPTER 12

Configuring, Supporting the Fixed Domains and Country Codes (ROW)

Configuring and Verifying Country Code using 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 country code, 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
```

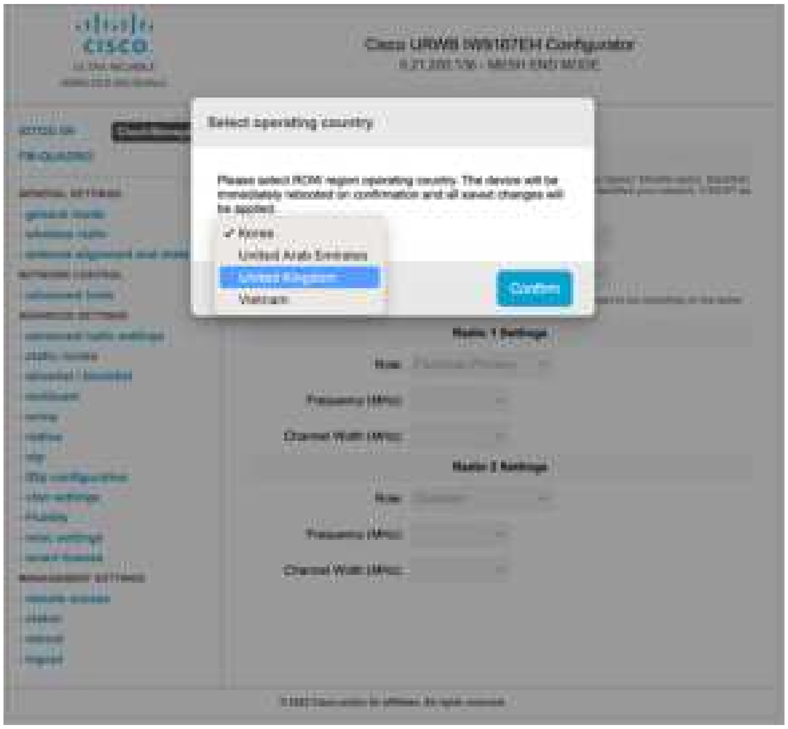
Example:

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

Configuring Country Code using GUI

Wireless interfaces fails to work if country code is not configured. To configure the country code:

1. In the **GENERAL SETTINGS**, click **wireless radio**.
2. For ROW domain, if the country code is not selected, the following pop-up appears:



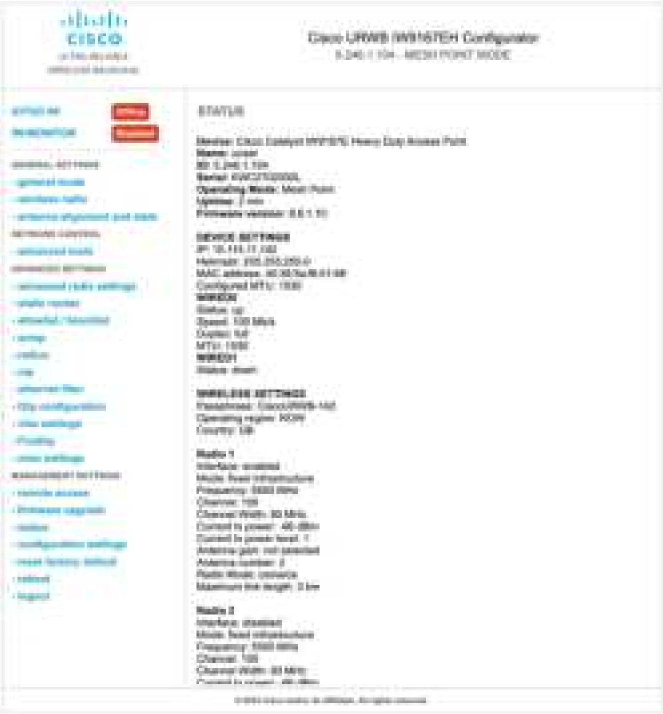
Please select ROW region operating country. The device will be immediately rebooted on confirmation and all saved changes will be applied.

3. To select a country code, click the pop-up in the above image then it redirects to the **Wireless Settings** section. In the **Wireless Settings** section, choose country from the 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.



Cisco URWB IW9167EH Configurator

STATUS

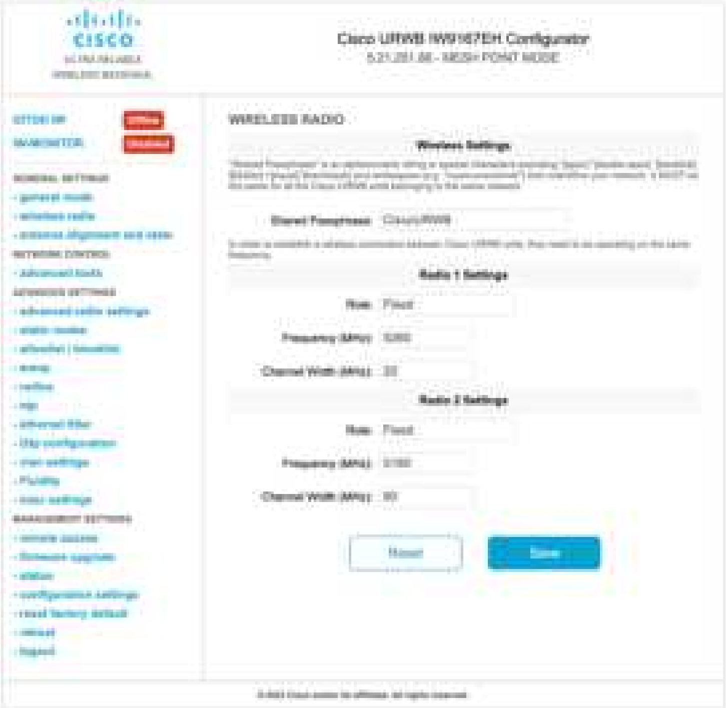
DEVICE SETTINGS

WIRELESS SETTINGS

Radio 1

Radio 2

7. To establish a wireless connection between devices, set a same operating frequency in radio units. Shared Passphrase must be the same for all the devices belonging to the same network.



Cisco URWB IW9167EH Configurator

WIRELESS RADIO

Wireless Settings

Shared Passphrase: CiscoURWB

Radio 1 Settings

Role: Fixed

Frequency (MHz): 5260

Channel Width (MHz): 20

Radio 2 Settings

Role: Fixed

Frequency (MHz): 5180

Channel Width (MHz): 80

The below image shows the configuration of country code from GUI:

Cisco URWB IW9167EH Configurator
[illegible] - MESH POINT MODE

Operating Mode: Mesh Point
Uptime: [illegible]
Firmware version: [illegible]

DEVICE SETTINGS
IP: [illegible]
Netmask: 255.255.255.0
MAC address: [illegible]
Configured MTU: [illegible]
WIRED0
Status: up
Speed: 1000 Mbs
Duplex: full
MTU: [illegible]
WIRED1
Status: down

WIRELESS SETTINGS
Passphrase: [illegible]
Operating region: B

Radio 1
Interface: enabled
Mode: fixed infrastructure
Frequency: [illegible] MHz
Channel: [illegible]
Channel Width: 20 MHz
Current tx-power: [illegible] dBm
Current tx-power level: 1
Antenna gain: not selected
Antenna number: [illegible]
Radio Mode: [illegible]
Maximum link length: [illegible]

Radio 2
Interface: disabled
Mode: fixed infrastructure
Frequency: [illegible] MHz
Channel: [illegible]
Channel Width: 40 MHz
Current tx-power: [illegible] dBm
Current tx-power level: 1
Antenna gain: not selected
Antenna number: [illegible]
Radio Mode: [illegible]
Maximum link length: [illegible]

DIAGNOSTIC TOOL

Supporting Fixed Domains and Country Codes (ROW)

The ROW reg domain simplifies the domain management of the manufacturing process for all the country codes 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	N/A
E	Yes
F	No
Q	No
Z	No

Note Outdoor and indoor frequencies are the same for the B domain.

Catalyst IW9167E Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
KR (Korea)	No
VN (Vietnam)	N/A
GB (Great Britain)	Yes
IN (India)	No
PE (Peru)	No
PH (Philippines)	No
ZA (South Africa)	No
AR (Argentina)	No
HK (Hong Kong)	No
PK (Pakistan)	No
UY (Uruguay)	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.

IS (Iceland) and MC (Monaco) are supported using EU domain.

Catalyst IW9165E Supported Fixed Domains

Domain	Indoor Deployment Support
A	Yes
B	N/A
E	Yes
Z	Yes
Q	Yes
F	Yes

Note Outdoor and indoor frequencies are the same for B domain.

Catalyst IW9165E Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
GB (Great Britain)	Yes
ZA (South Africa)	Yes
IN (India)	Yes
KR (Korea)	Yes
PE (Peru)	Yes
AE (UAE)	Yes
MX (Mexico)	Yes
BR (Brazil)	Yes
CL (Chile)	Yes
SA (Saudi Arabia)	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.

Catalyst IW9165D Supported Fixed Domains

Domain	Indoor Deployment Support
A	No
B	N/A
E	Yes
Z	No
Q	Yes
F	Yes

Note Outdoor and indoor frequencies are same for the B domain.

Catalyst IW9165DH Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
GB (Great Britain)	Yes
ZA (South Africa)	No
IN (India)	No
KR (Korea)	No
PE (Peru)	No
AE (UAE)	No
MX (Mexico)	No
BR (Brazil)	No
CL (Chile)	No
SA (Saudi Arabia)	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.

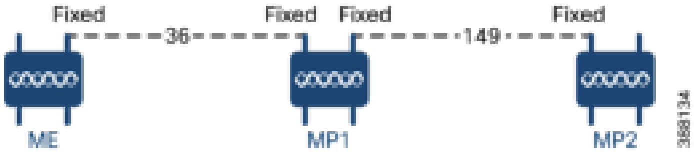
CHAPTER 13

Configuring and Validating of Point-to-Point Relay Topology

Configuring and Validating of Point-to-Point Relay Topology

Two radio interfaces on a single device (MP1) to implement a point-to-point relay topology as depicted in the picture below.

Figure 2: point to point relay topology



To configure point to point relay topology, follow the scenarios listed below:

1. Configure Mesh End (ME) on channel 36, MP1 on channel 36 and MP2 on the default channel 149.

2. Continue from step 1 configuration.

3. Re-enable the second slot interface on Mesh Point (MP2) and wait for 30 seconds then point-to-point relay topology implemented by two radio interfaces on a single devicet.

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 between 1 to 256

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

5. End of configuration mode.

   ```
   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
```

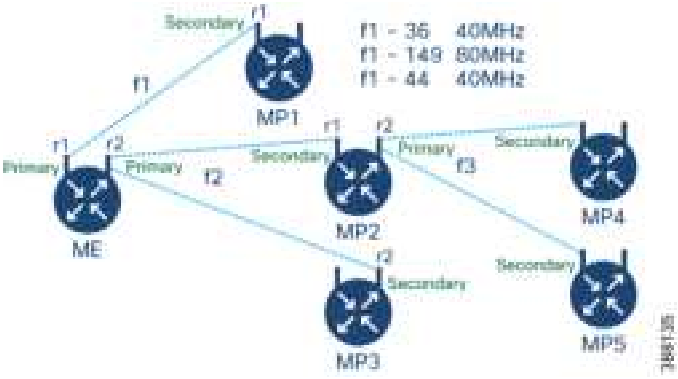
CHAPTER 14

Configuring and Validating Fluidmax Topology

Configuring and Validating Fluidmax (point to multipoint) Topology

Concerning 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 picture below illustrated 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. Concerning 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 3: 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
```

Validating Point to Multipoint Topology from CLI

To validate the point to multipoint (Fluidmax) topology configuration use the following show command.

```
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
```

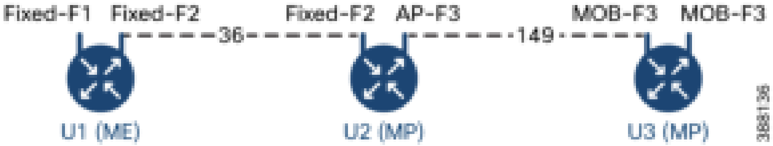
CHAPTER 15

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 in fixed infrastructure and the second radio as a Fluidity access point to accept vehicle connections simultaneously. Both radio interfaces on U1 configured as fixed infra 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 4: Mixed Mode Topologies



Configuring Mixed Mode Topology from CLI

To configure a mixed mode topology, use a following CLI commands.

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

Fluidity id – configure Fluidity role for device.

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.

```
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 a 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 16

Configuring and Validating Fluidmax Fast Failover

Configuring and Validating Fluidmax Fast Failover

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

1. Primary and backup primary node should have same configuration, it includes the same channel's parameters (frequency, channel width, etc.) as well as the Fluidmax parameters like role, cluster ID.
2. Fluidmax redundancy provides resilience for node-failure type of faults (eg. power loss or catastrophic hardware fault on the primary node).
3. Enable Fluidmax fast failover using Fluidmax CLI commands on all devices except vehicle devices.

Note Catalyst IW9167E supports both Gateway + MP (Mesh Point) – MP (with same tower ID) and ME (Mesh End) – ME fast failover.

Configuring Fluidmax Fast Failover from CLI

To configure Fluidmax fast failover, use the following CLI commands.

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

Modeconfig – configure current operating mode of device. Mode could mesh end, mesh point 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.

```
Device# configure dot11Radio [1|2] mode fluidmax [primary|secondary]
```

Fluidmax - Set the interface in Fluidmax mode.

Primary | Secondary - Fluidmax role for the unit, either primary or secondary.

```
Device# configure dot11Radio [1|2] mode fluidmax cluster id fluidmesh
```

cluster id - Set Fluidmax Cluster ID assigned to the interface.

```
Device# configure dot11Radio [1|2] mode fluidmax tower [enable|disable]
```

Tower – Enable or disable Fluidmax Tower ID for specified interface.

Note Radio interface setting must be the same on both ME (Mesh End) point to multi point primaries.

Validating Fluidmax Fast Failover from CLI

To validate Fluidmax fast failover, use the following show commands.

```
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 17

Configuring Indoor Deployment

Configuring Indoor Deployment

The Catalysts IW9167E or IW9165 support enabling indoor deployment and can turn on and off indoor deployment by configuration on URWB CLI.

> **Note** It is the responsibility of you to ensure that the Catalyst IW9167E or IW9165 is indeed located indoors before toggling the indoor deployment setting. Outdoor mode can be used indoors, but indoor mode cannot be used outdoors because 5150–5350 MHz channels are indoor related countries.
>
> Outdoor mode is always the default.

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 commands.

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 18

Configuring and Validating Smart Licensing

Overview of Smart Licensing Support

Smart licensing for Catalyst Access Point running in URWB mode support the following scenarios:

- Smart license management provides a seamless experience with the various aspects of licensing.
- License level controls the features by essential, advantage and premier mode.
- IoT specific seats will cache a device list in the mobility scenario and seats will reserve some license usage which is the expected maximum number of devices in the managed network.
- Smart transport mode connects to smart software manager (SSM) (formerly it was CSSM) directly to sync license usage.
- Airgap mode uses the downloaded file to sync with SSM manually.
- You should configure same license level on both primary and secondary layer2 ME (Mesh End) or layer3 GGW (Global Gateway).

Note Ensure the device syncs up right time from network time protocol (NTP) server to establish connection with SSM successfully.

From release 17.12.1, the smart licensing supports the following enhancements:

- Seats and license level management for both Catalyst IW9165 and IW9167.
- CLI command to check configured and current seats values.
- CLI command to check running license level.

License level and seats configuration are available for the following device roles:

- ME (Mesh End) fixed infrastructure network.
- ME (Mesh End) fluidity Layer 2 network.
- GGW (Global Gateways) fluidity Layer 3 network.

A RUM (Resource Utilisation Measurement) report counts the number of devices using license seats for a specific feature that is used to configure seats for each entitlement tag.

Smart license level for Catalysts IW9167 and IW9165 controls the feature list by using the following tables:

Table 5: Smart license level for Catalyst IW9167

License Type	Features
Essentials	• Unlimited fixed throughput • Unlimited AP mobility throughput • 0.5 Mbps Mobility client throughput
Advantage	• Unlimited fixed throughput • Unlimited AP mobility throughput • 50 Mbps vehicle mobility throughput • Multipath Operation (MPO)
Premier	• Unlimited fixed throughput • Unlimited AP mobility throughput • Unlimited vehicle mobility throughput • Multipath Operation (MPO)

Table 6: Smart license level for Catalyst IW9165

License Type	Features
Essentials	• Unlimited fixed throughput • 15 Mbps AP mobility throughput • 5 Mbps vehicle mobility throughput
Advantage	• Unlimited fixed throughput • 50 Mbps AP mobility throughput • 50 Mbps vehicle mobility throughput • Multipath Operation (MPO)

License Type	Features
Premier	• Unlimited fixed throughput • Unlimited AP mobility throughput • Unlimited vehicle mobility throughput • Multipath Operation (MPO)

Configuring and Validating Smart Licensing from CLI

To configure smart license, use the following CLI command:

```
Device# configure license iw-level [advantage | essentials | premier]

                 advantage:  Network Advantage for Radios
                 essentials: Network Essentials for Radios
                 premier:    Network Premier for Radios
```

To configure smart license device number, use the following CLI command:

```
Device# configure license iw-network seats 6
```

To configure smart license online deployment, use the following CLI command:

```
Device# configure license smart transport smart
Device# configure license
Device# configure license smart proxy address 192.168.1.1 (Optional)
Device# configure license smart proxy port 3128 (Optional)
Device# license smart trust idtoken <id_token_generate_from_SSM> local
Device# configure license smart usage interval 50 (Optional)
```

To configure smart license offline deployment, use the following CLI command:

```
Device# configure license smart transport off
Device# license smart save usage all tftp://192.168.216.201/rum_report_all.xml
Device# license smart import tftp://192.168.216.201/rum_report_ack.xml
```

To configure reset license configuration as default, use the following CLI command:

```
Device# license smart factory reset
```

(do not type write just reload to clear all license configuration)

To validate smart license type, use the following show command:

```
Device# show license usage
License Authorization Status: Not Applicable
IW9167_URWB_NW_A(IW9167_URWB_NW_A);
Description: Network Advantage for Catalyst Industrial Wireless CURWB Radios
Count: 1
Version: 0.1
Status: IN USE
Export Status: NOT RESTRICTED
Feature Name: IW9167_URWB_NW_A
```

To validate smart license device number, use the following show command:

```
Device# show license iw seats

 6
```

To validate smart license usage count, use the following show command:

```
Device# show license summary
Account information:
Smart account <none>
Virtual account <none>
License Usage:
License : IW9167_URWB_NW_A
Entitlement Tag : (IW9167_URWB_NW_A)
Count Status : 6 IN USE
```

Note License usage count = max (configured license seats, active devices)

When device offline, device record paging time is two days.

When active devices > configured license seats, ME will try to send license usage report to SSM every eight days.

To validate smart license HA (High Availability) role, use the following show command:

```
Primary_ME# show license tech support
License Usage
===============
Handle 1
……..
Measurements:
ENTITLEMENT:
Interval: 00: 15: 00
Current value: 0
Application Name: UrwbSLP
Application id: UrwbHA
Application Role: Active
Peer info:
Application Name: UrwbSLP
Application id: UrwbHA
Application Role: Standby
PID: ‘nullPtr’
UDI: P: IW9167EH-B, S: KWC26330HMR
Smart Account Name: ‘nullPtr’
Virtual Account Name: ‘nullPtr’
```

```
Standy_ME# show license tech support
License Usage
===============
Handle 1
……..
Measurements:
ENTITLEMENT:
Interval: 00: 15: 00
Current value: 0
Application Name: UrwbSLP
Application id: UrwbHA
Application Role: Standby
Peer info:
Application Name: UrwbSLP
Application id: UrwbHA
Application Role: Active
PID: ‘nullPtr’
UDI: P: IW9167EH-B, S: KWC26330HLF
Smart Account Name: ‘nullPtr’
Virtual Account Name: ‘nullPtr’
```

To validate smart license SSM connection, use the following show command:

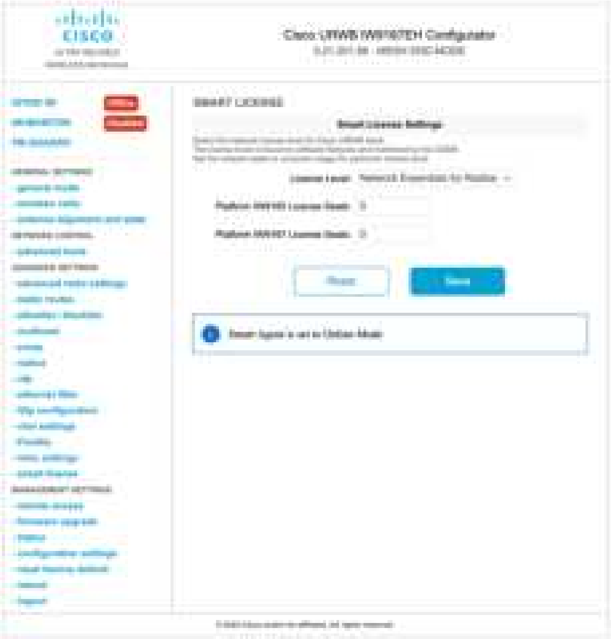
```
Device# show license status
…..
Account information
Smart Account SA-IOT-Polaris As of Sep 28 2022 11: 04:03 CST
Virtual Account: CURWB
Transport:
Type: Smart
Proxy:
Address: 192.168.216.201
Port: 3128
…….
Policy
Policy in use: Installed on Sep 28 2022 11: 04:03 CST
Policy name: Test policy
Reporting ACK required: no (Customer Policy)
First report requirement (days): 94 (Customer Policy)
Report on change (days): 100 (Customer Policy)
```

Configuring Smart Licensing from GUI

To configure smart licensing from the GUI, follow the below procedure:

1. Select the network license level for the URWB network.
2. Verify that the licence level is controlled by SSM and is connected to software features.
3. Set the network seats to consume usage for particular license level (example : Network Essentials for Radios).
4. To download a usage, Save RUM (Resource Utilization Measurement) reports (license usage information) and save all RUM reports using All options. Save RUM report for the last n number of days (excluding the current day) using Days option.
5. To upload SSM Acknowledge and sync license usage, import the ACK (Acknowledge) that downloaded from SSM on the production instance when Smart agent is in Airgap (Offline) Mode.

Following images are example for GUI configuration of smart licensing (online mode and offline mode):



Cisco URWB IW9167EH Configurator

SMART LICENSE

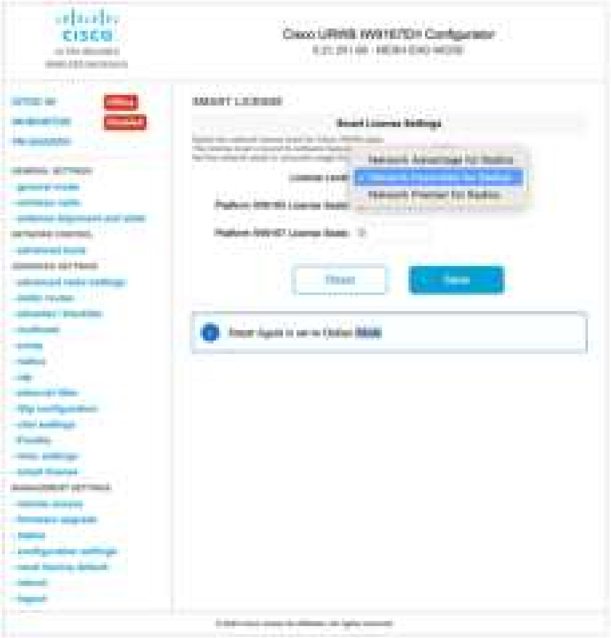
Smart License Settings

License Level: Network Essentials for Radios

Platform IW9165 License Seats: 0

Platform IW9167 License Seats: 0

Smart Agent is set in Online Mode



Cisco URWB IW9167EH Configurator

SMART LICENSE

Smart License Settings

Network Advantage for Radios
Network Essentials for Radios
Network Premier for Radios

Platform IW9167 License Seats: 0

Smart Agent is set in Online Mode

Configuring Smart License Seats Management using CLI

To configure a smart license seats, use the following CLI commands:

```
Device# configure license iw-network seats platform
         iw9165 iw9167
         WORD Select one above platform (case sensitive) to configure seats.
```

Example:

```
Device# configure license iw-network seats platform iw9165 12
Device# configure license iw-network seats platform iw9167 15
```

Verifying license iw-seats using CLI

```
Device# show license iw seats
                 Platform Configured Current
                 IW9167      0         15
                 IW9165      0         12
         Device# write
         Device# reload

         Device# show license iw seats
                 Platform Configured Current
                 IW9167       15       15
                 IW9165       12       12
```

Configuring Smart License Seats Management using GUI

To select the network license level for URWB stack, follow these steps:

1. In the **Advanced Settings**, click **smart license**.

2. In the **Smart License Settings**, set **License level** as **Network Essentials for Radios**.
3. Enter **Platform IW9165 License Seats** value.
4. Enter **Platform IW9167 License Seats** value.
5. Click **Save**.

Configuring Running License Level using CLI

The license level is configured by the primary ME or GGW device (based on network configuration) then the license level is distributed and applied to all the devices connected to the network.

To configure a license level for ME (Mesh End) and GGW (license distributor), use the following CLI command:

```
Device# configure license iw-level
                 Advantage: Network Advantage for Radios
                 essentials: Network Essentials for Radios
                 premier: Network Premier for Radios
```

Example:

```
Device# configure license iw-level [ premier | essentials | Advantage ]
```

To verify the license level for ME and GGW (license distributor), use the following CLI command:

```
Device# show license iw level
                 Configured IW Network License: ESSENTIALS
                 Running IW Network License: PREMIER
         Device# write
         Device# reload

         Device# show license iw level
                 Configured IW Network License: PREMIER
                 Running IW Network License: PREMIER
```

To verify the license level for MP (license receiver), use the following CLI command:

```
Device# show license iw level
                 Running IW Network License: PREMIER
```

Note License level configuration is not allowed.

CHAPTER 19

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 a CLI command or Web UI interface to enable or disable the network. The following list of reserved ether types cannot be configured:

Table 7: 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 by the URWB data plane mesh network when used in MPLS Layer-2 mode.

- The Layer-2 mesh transparency feature allows forwarding 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 allow-list.

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

Configuring and Verifying Layer-2 Protocols Forwarding Using CLI

The following CLI commands are used to configure a Layer-2 protocol forwarding.

To add an ethernet type to allow-list, 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# write
Device# reload

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

To delete an ethernet type to allow-list, 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# write
Device# reload

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

To clear all ethernet type to allow-list, 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 type to allow-list, 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# write
         Device# reload

        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 allow-list 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
         Device# write
         Device# reload

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#write
         Device# reboot

         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:

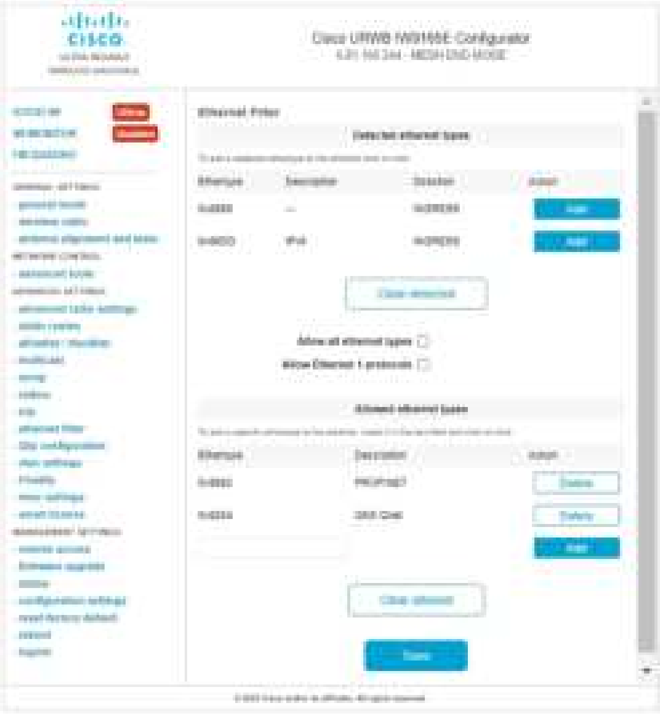
```
Device# show mpls ether-filter table
                Ether-type   Direction   Description
                0x8899        INGRESS       ---
                0x86DD        INGRESS       IPv6
```

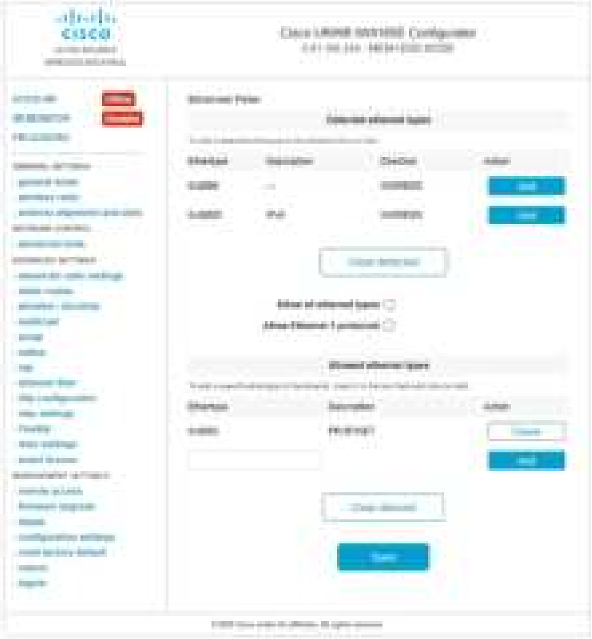
Configuring Layer-2 Protocol Forwarding using GUI

To add a specific and detected ether types to allow-list, follow these steps:

1. Choose **ethernet filter** in the **ADVANCED SETTINGS** section on the left side of the **Cisco URWB IW9165E or IW9167E Configurator** window.
2. In **Detected ethernet types** tab, click **Add** to add a ether types to the allow-list.
3. After click **Add** in **Detected ethernet types** tab, you can see the added ether types reflected in **Allowed Ethernet type** tab.
4. In **Allowed ethernet types** tab, to add a specific ether type to the allow-list, enter a ether type name in the text box and click **Add**.

Following images shows the specific and detected ethert ypes added to the allow-list:

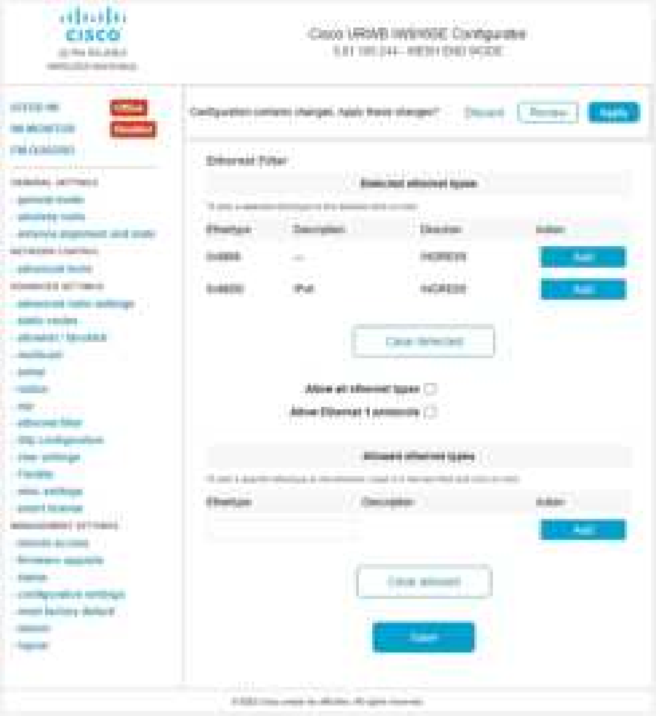




To clear all allowed ethernet types from allow-list, follow these steps:

1. Choose **ethernet filter** in the **ADVANCED SETTINGS** section on the left side of the **Cisco URWB IW9165E or IW9167E Configurator** window.
2. To clear all ethernet types from the allow-list, Click **Clear allowed** in the **Allowed ethernet types** tab.
3. After you click **Clear allowed**, you can see all ethernet types cleared from allow-list.

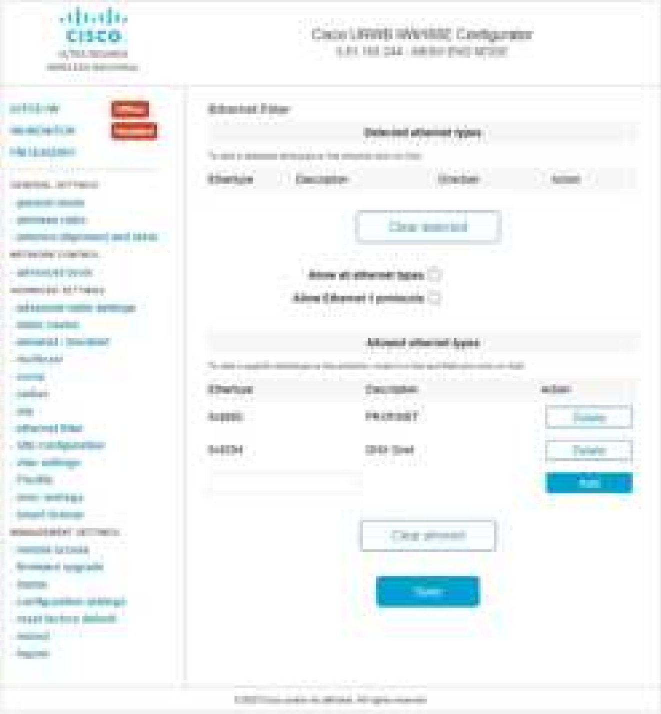
Following image shows all allowed ethernet types cleared from allow-list:



To clear all detected ethernet types from allow-list, follow these steps:

1. Choose **ethernet filter** in the **ADVANCED SETTINGS** section on the left side of the **Cisco URWB IW9165E or IW9167E Configurator** window.
2. To clear detected ethernet types from allow-list, Click **Clear detected** in **Detected ethernet types** tab.
3. After you click **Clear detected**, you can see ethernet types cleared in **Detected ethernet types** tab.

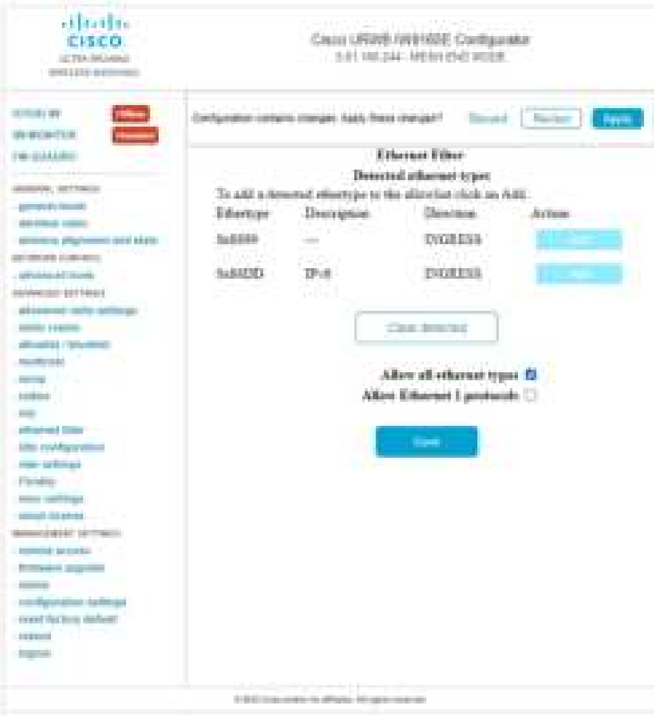
Following image shows the all detected ethernet types cleared from allow-list:



To add or allow all ethernet types to allow-list, follow these steps:

1. Choose **ethernet filter** in the **ADVANCED SETTINGS** section on the left side of the **Cisco URWB IW9165E or IW9167E Configurator** window.
2. To allow all ethernet type to allow-list, check or click the **Allow all ethernet types** check box in the **Ethernet Filter** section.
3. Click **Save** and **Apply** to change the configuration.

Following image shows the adding all ethernet types to allow-list:



Cisco URWB IW9165E Configurator

Ethernet Filter

Detected ethernet types

To add a detected ethertype to the allowlist click on Add.

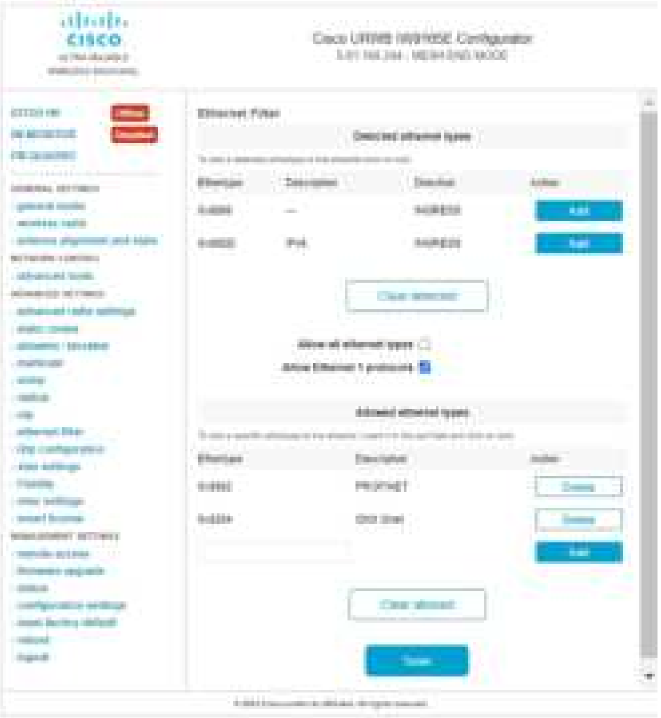
Ethertype	Description	Direction	Action
0x8899	—	INGRESS	
0x86DD	IPv6	INGRESS	

Allow all ethernet types ☑
Allow Ethernet I protocols ☐

To configure an ethernet I protocol, follow these steps:

1. Choose **ethernet filter** in the **ADVANCED SETTINGS** section on the left side of the **Cisco URWB IW9165E or IW9167E Configurator** window.
2. To enable ethernet I protocol mode, check or click the **Allow Ethernet I protocols** check box in the **Ethernet Filter** section.
3. Click **Save** and **Apply** to change the configuration.

Following image shows the configuration of allowing ethernet-I protocol:



Ethernet Filter

Detected ethernet types

Ethertype	Description	Direction	Action
0x8899	—	INGRESS	Add
0x0800	IPv4	INGRESS	Add

Allow all ethernet types ☐

Allow Ethernet 1 protocols ☑

Allowed ethernet types

Ethertype	Description	Action
0x8892	PROFINET	Delete
0x88A4	[illegible]	Delete
		Add

CHAPTER 20

Configuring Multipath Operation

Overview of MPO

Fast moving mobile systems expect on board, high speed connectivity, which implies a reliable wireless ground to vehicle communication without any interruptions. However, the dynamic nature of the network, as well as the environmental radio frequency conditions and roaming under the various Wi-Fi standards lead to packet losses. MPO (Multipath Operation) enhances reliability by sending duplicate copies of packets across multiple wireless paths. This patented technology duplicates your high priority traffic up to 8x and work with hardware failures to increase availability, reduce latency, and lower the effects of interference and hardware failures.

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 via redundant paths, reducing packet loss and seamless handoffs can also be supported.

Working Functionality of MPO

MPLS (Multi-Protocol Label Switching) has a single tunnel that connecting the home network with infrastructure and using 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 4 different tunnels simultaneously that will use different radio links. Multiple MPLS tunnels protect the specific traffic and improve system reliability.

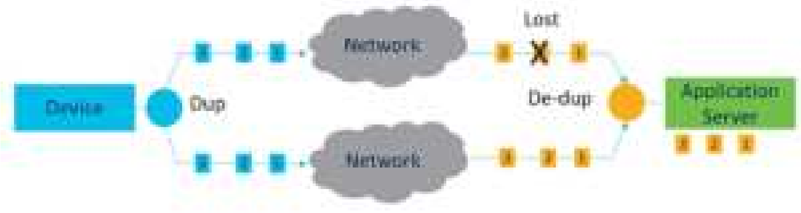
To protect the system from interference on wireless links, the control traffic is replicated over many MPLS tunnels, and copies of each packet are made and sent to various pathways. The receiver from the infrastructure side, receives more than one copy of the same packet after multiple copies of the traffic are produced and sent to parallel tunnels. However, without MPO functionality, if the wireless link fails, there is traffic loss. Multiple MPLS tunnels provides 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 multipath operations, 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 that is used 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 is shown below:



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

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

```
Device# configure fluidity mpo
```

cos - configure CoS of traffic to protect with MPO redundancy (only one CS at a time) and cos value is 0-7 (default 6)

path - configure max number of simultaneous redundant path established by mobile units (mobile units only). Maximum path link in 1 to 4 (default 1).

rssi - configure min RSSI threshold for a wireless link to be eligible as a redundant path(dB) (mobile units only). Minimum rssi value 0-96 (default 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, do not duplicate outgoing traffic

enabled: enable MPO. Duplicate outgoing traffic, 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 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 MPO configuration parameter, use the following show commands:

```
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: These counters represent, respectively, the number of packets transmitted on the primary path and secondary paths (cumulative sum for all available secondary paths, that is path IDs 1-3).

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 21

Configuring URWB Telemetry Protocol

Configuring URWB Telemetry Protocol

The URWB Telemetry Protocol is introduced from release 17.12.1 and it 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.

Configuration of GNSS Telemetry Protocol using CLI

To enable GNSS telemetry, use the following CLI command:

```
Device# configure gnss telemetry enable
```

To disable GNSS telemetry, use the following CLI command:

```
Device# configure gnss telemetry disable
```

To show GNSS telemetry, use the following CLI command:

```
Device# show gnss telemetry
```

CHAPTER 22

Configuring IW Monitor Management

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 8: IW Monitor features support from release 17.12.1 onwards.

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:

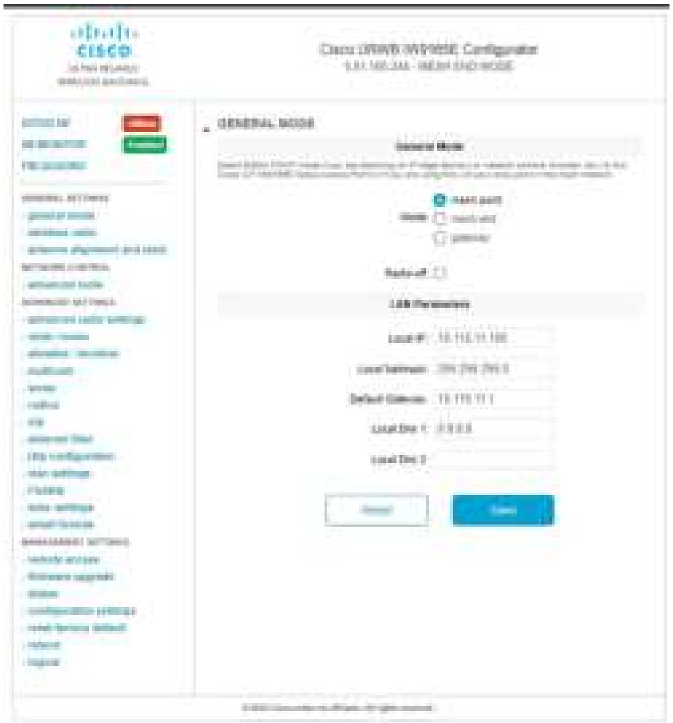
```
Device# show monitor
```

Example:

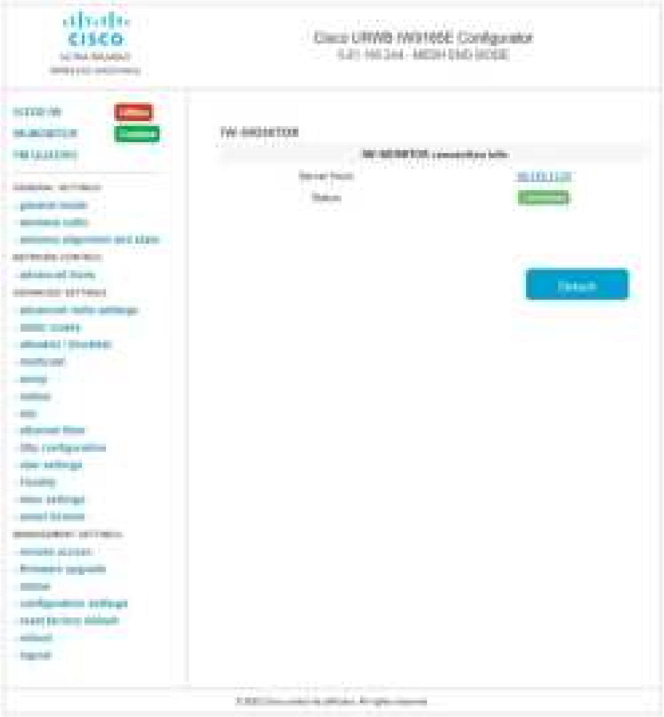
```
Device# show monitor
IW MONITOR: enabled
Status: Connected
```

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:


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
IW-MONITOR
IW-MONITOR connection info
Server host
Status
Connected

CHAPTER 23

Upgrading the Device using TFTP

To upgrade the device using trivial file transfer protocol (TFTP), follow these conditions:

- The device must be connected to the network.
- The device must be configured to communicate with the local TFTP server.
- The target device image must be uploaded to the root directory of the local TFTP server.

Device Upgrade using TFTP

The TFTP device upgrade feature enables you to perform an automatic device upgrade or a direct device upgrade. In an automatic device upgrade, the device periodically checks for the availability of new device using the manifest file and initiates the upgrading process. In a direct device upgrade, the device retrieves the specified device image from the TFTP server and initiates the upgrading process. You can choose either of the following methods:

- Automatic Device Upgrade using TFTP
- Direct Device Upgrade using TFTP

Automatic Device Upgrade using TFTP

Before you begin

This method enables the device to connect to the local TFTP server at user-determined intervals to check for the availability of new device image. The device detects the device image file and performs the upgrade.

Step 1 Create *device.manifest* file and upload to the same TFTP server root directory where the device image is stored.

Step 2 Before enabling the TFTP automatic upgrade, configure the TFTP server and time interval.

Note The time interval must be specified in the hours format.

Caution Do not disconnect or reboot the device until the device download completes. Based on the image file size, the device upgrade may take some time.

Configuring Manifest File on the TFTP Server

At first, the device retrieves the manifest file from the TFTP server. Based on the information in the manifest file, the device then retrieves the device image from the TFTP server. Once the conditions are satisfied, the device initiates the device upgrade process.

Manifest File Format

The manifest file must be hosted on the TFTP server. It contains information related to the device image intended for the device upgrade. The manifest file holds the following information:

- Device image filename
- MD5 checksum of the device image file
- Device image version

The manifest file name must be specified based on the IW device model:

Device Type	Manifest File Name
IW9167EH	IW9167EH.manifest
IW9165E	IW9165E.manifest
IW9165DH	IW9165DH.manifest

Example format of manifest file:
`image_name=ap1g6m-k9c1-tar.202307110910`
`image_md5=376e15acd4e82a49a81d42add904f5b0`
`image_version=8.8.1.101`

Direct Device Upgrade using TFTP

The device obtains the specified device image from the TFTP server. To start the direct device upgrade process, use the following CLI commands:

Purpose	Command or Action
To configure the TFTP server with IP address	`Device#configure tftp server A.B.C.D` A.B.C.D: IP address of the TFTP server

Purpose	Command or Action
To configure the TFTP upgrade image	Device#configure tftp upgrade <image file> Device#write Device#reload Configure TFTP upgrade image <image file bin>

The device immediately starts the upgrade process.

Caution Do not disconnect or reboot the device until the device download completes. Based on the image file size, the device upgrade may take some time.

TFTP Device Upgrade using CLI

Purpose	Command or Action
To perform a device upgrade using the TFTP server	Device#configure tftp server A.B.C.D A.B.C.D: IP address of the tftp server
To disable automatic TFTP device upgrade	Device#configure tftp upgrade automatic disable
To enable automatic TFTP device upgrade	Device#configure tftp upgrade automatic enable Device#write Device#reload
To check immediately for the manifest file without waiting for the check period	Device#configure tftp upgrade check now
To check TFTP device upgrade periodically	Device#configure tftp upgrade check period 3 Device#write **Note** The check period must be specified in the hours format.
To check TFTP configuration	Device#show tftp config

Example of show TFTP configuration:

```
Device#show tftp config
Automatic TFTP Upgrade settings:
Status: enabled
Server: A.B.C.D
Check period (hours): 3
```

Example of automatic TFTP upgrade:

```
Device#configure tftp server A.B.C.D
Device#configure tftp upgrade check period 3
Device#write
Device#configure tftp upgrade automatic enable
Device#write
Device#reload
```

The device upgrade procedure fails to start:

- If the MD5 checksum reported in the manifest file does not match the MD5 checksum calculated on the device image file (*image_name*).
- If the device image version reported in the manifest file matches the current device version running on the device.

CHAPTER 24

LED Pattern for Catalysts IW9167 and IW9165

LED Pattern for Catalyst IW9167

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

Table 9: 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
To press Reset button less than 20 s	Blinking red
To press Reset button more than 20 s	Solid red
When Reset button is released Or Reset button is pressed more than 60 sec	Blinking geen

After the access point boots up, the Catalyst IW9167E URWB mode follows the below LED pattern.

Table 10: 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 a tri-color red, green, and blue LED and the Catalyst IW9165D has red, green, and amber LED with three brightness levels. The Access Point is flexible with brightness levels. The controller CLI/GUI controls the brightness with eight different settings.

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

Table 11: LED pattern for URWB states

AP State	LED State
Fallback	Blinking amber/blue
DHCP	Amber/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 12: 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 below table shows the URWB LED functionalities for the Catalyst IW9165E:

Table 13: 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 / 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 / port is Off
LAN GE	Green	Port is up with link
	Blinking Green	Link with activity
	Off	No link / port is Off
Digital IO 1-2	Yellow	Active as digital input or output
	Off	Inactive as digital input or output

The below table shows the URWB LED functionalities for the Catalyst IW9165D:

Table 14: 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 / Green	RSSI < - 86 dBm: yellow - 86 dBm =< RSSI =< - 81 dBM: blinking green RSSI > - 81 dBm: green