



Cisco Catalyst IW9167E Heavy Duty Access Point Cisco Ultra-Reliable Wireless Backhaul Software Configuration Guide, 17.11.1

First Published: 2023-03-30

Last Modified: 2023-03-30

Americas Headquarters

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



CONTENTS

CHAPTER 1	Overview of Cisco URWB Catalyst IW9167E Heavy Duty Access Point 1
	Configuring the Access Point for the First Time 1
	Using the Command-Line Interface 1
	Connecting to the Access Point Console Port 1

CHAPTER 2	Configuring Cisco URWB Operation Mode 3
	Configuring Cisco URWB Operation Mode 3
	Determining from CLI 3
	Cisco URWB LED Pattern 4
	Reset Button Settings 5
	Configuring Image Conversion 5
	Instructions to Access the GUI 6
	Cisco URWB IW9167E Configuration from GUI 6
	Committing CLI Configuration 7
	Configuring and Verifying Regulatory Domain from CLI 8
	Configuring Regulatory Domain from GUI 8
	Configuring IOT-OD and Offline Mode from CLI 12
	Configuring Strong Password (after first login) from CLI 12
	Configuring IOT-OD IW from GUI 14

CHAPTER 3	Configuring Cisco URWB Radio Mode 15
	Configuring Cisco URWB Radio Mode 15
	Configuring Radio-off Mode from CLI 16
	Configuring Fluidity Role from CLI 17
	Configuring Radio Mode for Cisco URWB from CLI 17

Configuring AMPDU from CLI	18
Configuring Frequency from CLI	18
Configuring Maximum MCS Index from CLI	19
Configuring Maximum NSS (Number of Spatial Streams) Index from CLI	19
Configuring Rx-SOP Threshold from CLI	19
Configuring RTS Mode from CLI	19
Configuring WMM Mode from CLI	20
Configuring NTP Enhancement from CLI	20
Configuring NTP Enhancement from GUI	21
Validating Radio Mode for Cisco URWB	22
Configuring Radio-off Mode from GUI	22
Configuring Radio Mode from GUI	23

CHAPTER 4**Configuring Radio Antenna Settings 27**

Configuring Radio Antenna Settings	27
Configuring Antenna Gain	27
Configuring Transmit and Receive Antennas	27
Configuring Transmission Power	28

CHAPTER 5**Configuring and Validating Radio Channel and Bandwidth 29**

Configuring Operating Channel from CLI	29
Configuring Channel Bandwidth from CLI	29
Validating Operating Channel and Bandwidth from CLI	30
Configuring Radio Channel and Bandwidth from GUI	30
Configuring Fluidity from GUI	31

CHAPTER 6**Configuring and Validating of Point-to-Point Relay Topology 37**

Configuring and Validating of Point-to-Point Relay Topology	37
Configuring Point to Point Relay Topology from CLI	37
Validating Point to Point Relay Topology from CLI	38

CHAPTER 7**Configuring and Validating Fluidmax Topology 41**

Configuring and Validating Fluidmax (point to multipoint) Topology	41
Configuring Point to Multipoint Topology from CLI	41

Validating Point to Multipoint Topology from CLI 43

CHAPTER 8 [Configuring and Validating Mixed Mode \(Fixed infrastructure + Fluidity\) Topology](#) 45

[Configuring and Validating Mixed Mode \(Fixed Infrastructure + Fluidity\) Topology](#) 45

[Configuring Mixed Mode Topology from CLI](#) 45

[Validating Mixed Mode Topology from CLI](#) 46

CHAPTER 9 [Configuring and Validating Fluidmax Fast Failover](#) 49

[Configuring and Validating Fluidmax Fast Failover](#) 49

[Configuring Fluidmax Fast Failover from CLI](#) 49

[Validating Fluidmax Fast Failover from CLI](#) 50

CHAPTER 10 [Configuring and Validating High Efficiency \(802.11 ax\)](#) 51

[Configuring and Validating High Efficiency](#) 51

[Configuring Global Gateway from GUI](#) 52

CHAPTER 11 [Configuring Guard Interval for HE \(High Efficiency \)](#) 55

[Configuring Guard Interval for HE](#) 55

CHAPTER 12 [Configuring Indoor Deployment for -E Domain](#) 57

[Configuring Indoor Deployment for -E Domain](#) 57

CHAPTER 13 [Configuring and Validating SNMP](#) 59

[Configuring and Validating SNMP](#) 59

[Configuring SNMP from CLI](#) 59

[Validating SNMP from CLI](#) 61

[Configuring SNMP from GUI](#) 61

CHAPTER 14 [Configuring and Validating Key Controller \(Wireless Security\)](#) 65

[Configuring and Validating Key Controller \(Wireless Security\)](#) 65

[Configuring Key Controller from CLI](#) 65

[Validating Key Controller from CLI](#) 66

CHAPTER 15**Configuring and Validating Smart Licensing 67**Configuring and Validating Smart Licensing from CLI **67**Configuring Smart Licensing from GUI **70**



CHAPTER 1

Overview of Cisco URWB Catalyst IW9167E Heavy Duty Access Point

The Cisco Catalyst IW9167E Heavy Duty Access Point provides reliable wireless connectivity for mission-critical applications in a state-of-the-art platform to deliver a network that is more reliable and secure, with higher throughput, more capacity, and less device interference. The 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 IW9167E can operate in Cisco Catalyst Wi-Fi (CAPWAP) mode or Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) mode and Cisco URWB software on IW9167E designed to support the Cisco style parser. This document covers configuration of Cisco URWB mode specific to the IW9167EH Access Point.

- [Configuring the Access Point for the First Time, on page 1](#)
- [Using the Command-Line Interface, on page 1](#)
- [Connecting to the Access Point Console Port, on page 1](#)

Configuring the Access Point for the First Time

This section describes how to configure basic settings on the wireless device for the first time. You can configure all the settings described in this section using the CLI, but it might be simplest to browse to the wireless device web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

Using the Command-Line Interface

Use Secure Shell (SSH) to access the CLI. SSH provides a secure, remote connection to networking devices. The SSH software package provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection.

Connecting to the Access Point Console Port

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

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

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

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

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

Use these default credentials to log in:

- Username: Cisco
- Password: Cisco



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



CHAPTER 2

Configuring Cisco URWB Operation Mode

- [Configuring Cisco URWB Operation Mode, on page 3](#)
- [Determining from CLI, on page 3](#)
- [Cisco URWB LED Pattern, on page 4](#)
- [Reset Button Settings, on page 5](#)
- [Configuring Image Conversion, on page 5](#)
- [Instructions to Access the GUI, on page 6](#)
- [Cisco URWB IW9167E Configuration from GUI, on page 6](#)
- [Committing CLI Configuration, on page 7](#)
- [Configuring and Verifying Regulatory Domain from CLI, on page 8](#)
- [Configuring Regulatory Domain from GUI, on page 8](#)
- [Configuring IOT-OD and Offline Mode from CLI, on page 12](#)
- [Configuring Strong Password \(after first login\) from CLI, on page 12](#)
- [Configuring IOT-OD IW from GUI, on page 14](#)

Configuring Cisco URWB Operation Mode

Catalyst IW9167E Access Point supports three wireless technologies on a single hardware platform, such as Cisco Catalyst Wi-Fi, Cisco URWB, and Cisco Workgroup Bridge (WGB). These access point have the flexibility to change their operating mode from Wi-Fi mode to Cisco URWB mode and vice versa.

To identify the image mode (AP mode or Cisco URWB mode) on IW9167E, the following method is used:

- [Determining from CLI](#)

Determining from CLI

IW9167E supports two different OS (Cisco URWB and CAPWAP Stack) for different feature sets and data plane logic. To determine Cisco URWB mode on IW9167E use the following show command.

```
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 Cisco AP Software (**ap1g6j**), it means that the image supports Cisco URWB mode.

Cisco URWB LED Pattern

The IW9167E Cisco URWB mode follow the below LED pattern during booting process (Blinking Green during a normal booting process).

Table 1: 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 GREEN

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

Table 2: Definition of Cisco URWB OS LED Pattern

AP State	LED State
General warning: Insufficient inline power	Cycling through RED, GREEN, and AMBER
Limbo (Provisioning) mode: Fallback	Chirping AMBER
Limbo (Provisioning) mode: DHCP(Dynamic Host Configuration Protocol)	AMBER

AP State	LED State
SNR(Signal to Noise Ratio) Excellent (≥ 25 dB)	Blinking GREEN
SNR Good ($15 \leq X < 25$ dB)	Fade-in GREEN
SNR Bad ($10 \leq X < 15$ dB)	Fade-in AMBER
SNR Unbearable (< 10 dB)	Fade-in RED

Reset Button Settings

The following reset actions are performed in the Cisco URWB when the LED turns to blinking RED (after the boot loader gets the reset signal):

- If reset button pressed for less than 20 seconds, configuration gets cleared.
- If reset button pressed for more than 20 seconds and less than 60 seconds, factory reset triggered.
- If reset button pressed for more than 60 seconds, nothing will be cleared.

Configuring Image Conversion

To convert an IW9167E Access Point from Wi-Fi mode (CAPWAP AP) to Cisco URWB mode and vice versa follow below procedures:

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

```
configure boot mode urwb
```

2. To convert from Cisco URWB to CAPWAP 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 enter the following CLI command.

```
configure boot mode wgb
```

4. To convert from URWB to WGB/uWGB enter the following CLI command.

```
configure boot mode wgb
```

5. To convert from WGB/uWGB to CAPWAP enter the following CLI command.

```
configure boot mode capwap
```

6. To convert from WGB/uWGB to URWB enter the following CLI command.

```
configure boot mode urwb
```

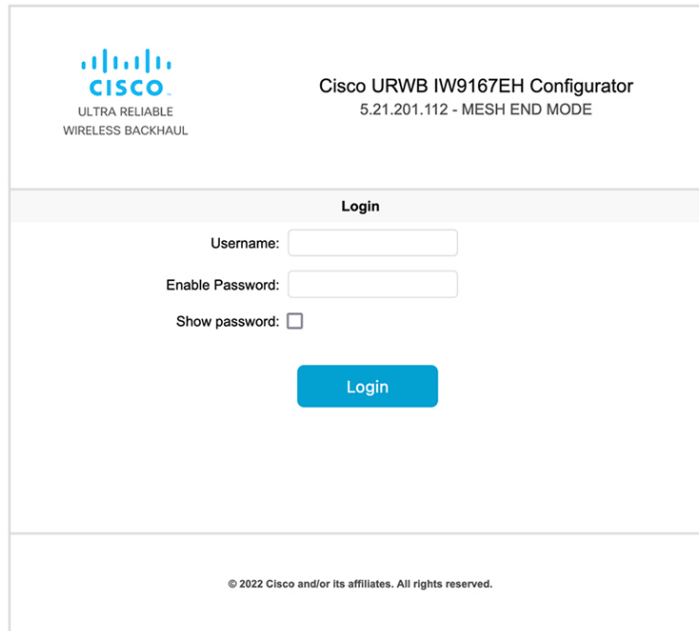


Note Image conversion performs full factory reset (any configuration and data will be removed completely).

Instructions to Access the GUI

To access the Web UI, use the following procedures:

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 Cisco URWB IW9167EH Configurator as below.

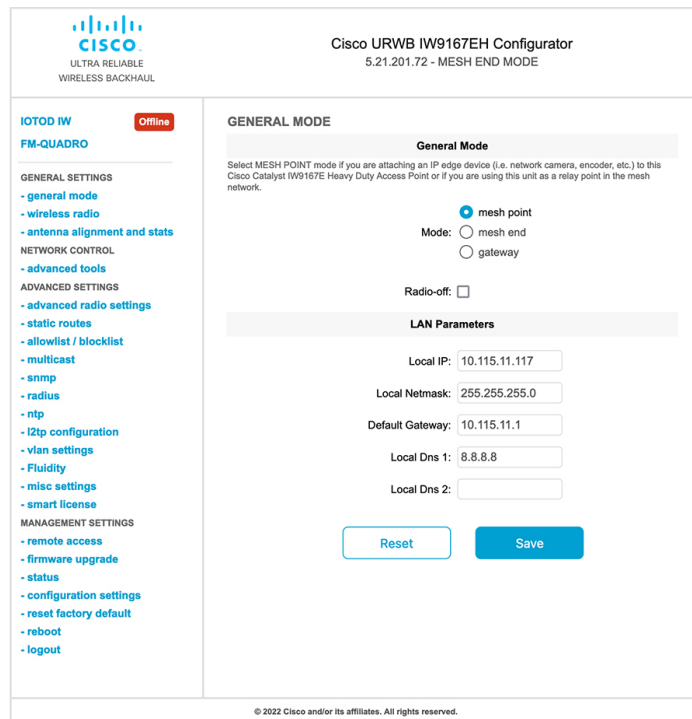


The screenshot shows the login page for the Cisco URWB IW9167EH Configurator. At the top left is the Cisco logo with the tagline "ULTRA RELIABLE WIRELESS BACKHAUL". To the right, the text reads "Cisco URWB IW9167EH Configurator" and "5.21.201.112 - MESH END MODE". Below this is a "Login" section with a header. It contains three input fields: "Username:", "Enable Password:", and "Show password:" with a checkbox. A blue "Login" button is centered below the fields. At the bottom, there is a copyright notice: "© 2022 Cisco and/or its affiliates. All rights reserved."

3. To access the configuration page, user need to use the credentials as follows: username and enable password.

Cisco URWB IW9167E Configuration from GUI

The following image shows the GUI configuration of Cisco URWB IW9167E layout.



Committing CLI Configuration

To save the current or running configuration settings to local storage or memory, user need to type **'write'** CLI command. The modified value is in the cache configuration file so after the **'write'** command is entered, user must 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 and Verifying Regulatory Domain from CLI

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

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

Example:

```
Configure countrycode GB
```

The above CLI will report error if configured country code is not included in ROW and wireless interface does not work properly if the user does not configure the country code.



Note Users need to reboot the device before configuring other wireless parameters (e.g., frequency, channel width), and after configuring country code. The country code is changeable or varying only for IW9167EH-ROW.

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

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

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

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

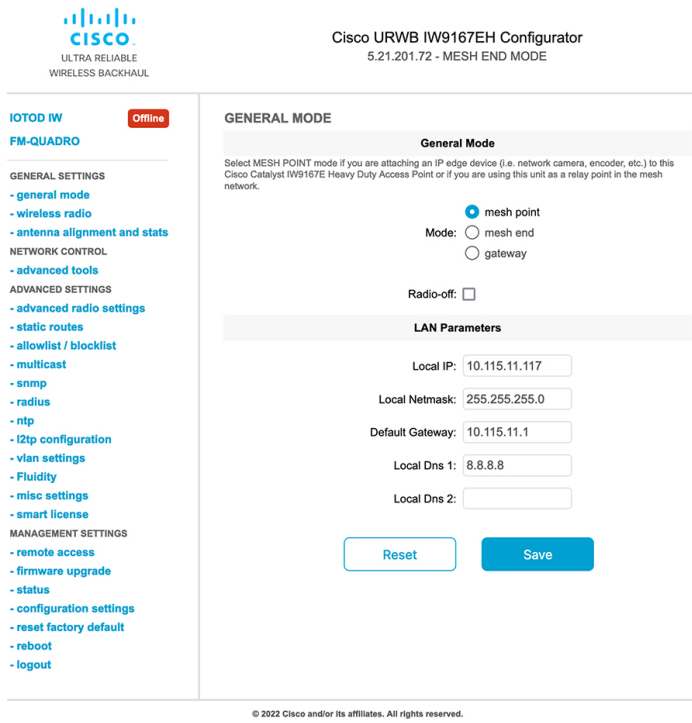
Example:

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

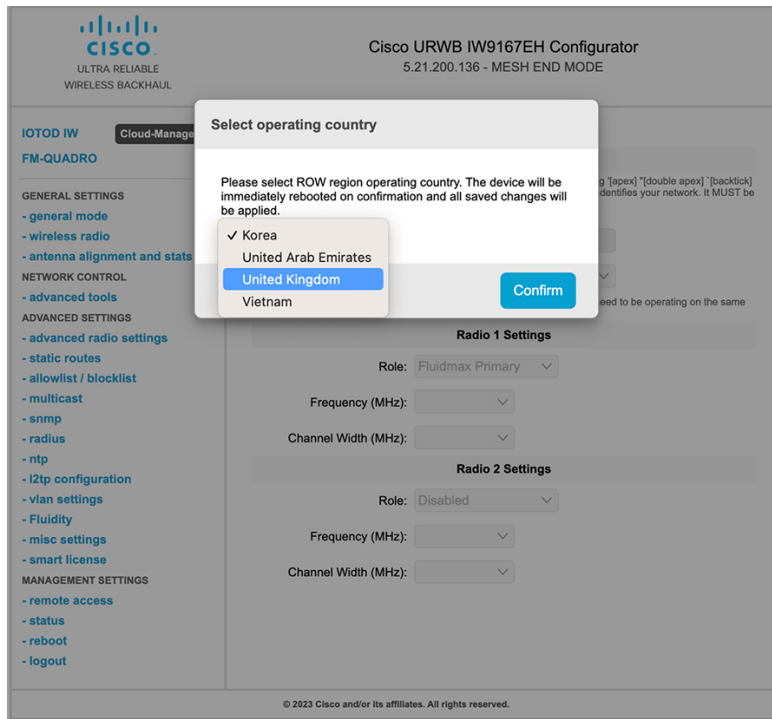
Configuring Regulatory Domain from GUI

Wireless interfaces do not work if user does not configure country code. Use the following procedure to configure a regulatory domain from GUI.

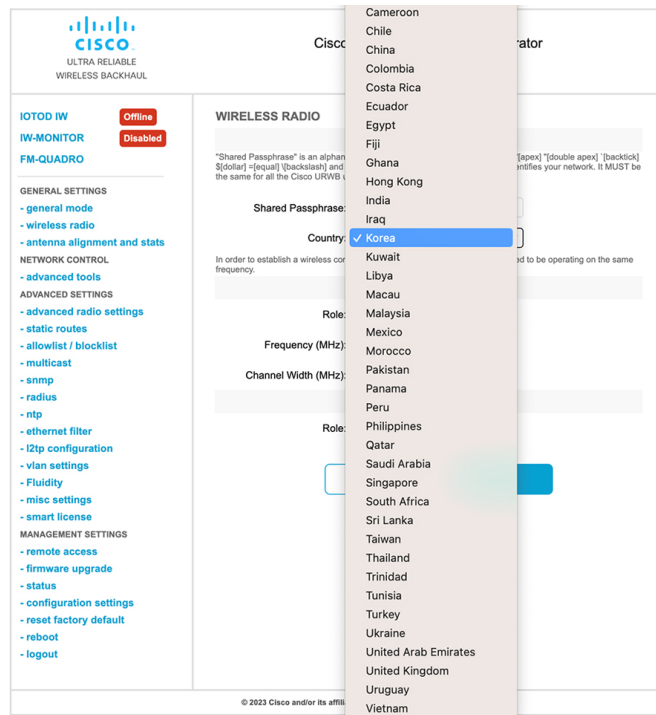
1. Select a Mesh Point mode if you are attaching an IP edge device to Cisco IW9167EH Access Point or if you are using this unit as a relay point in the mesh network.



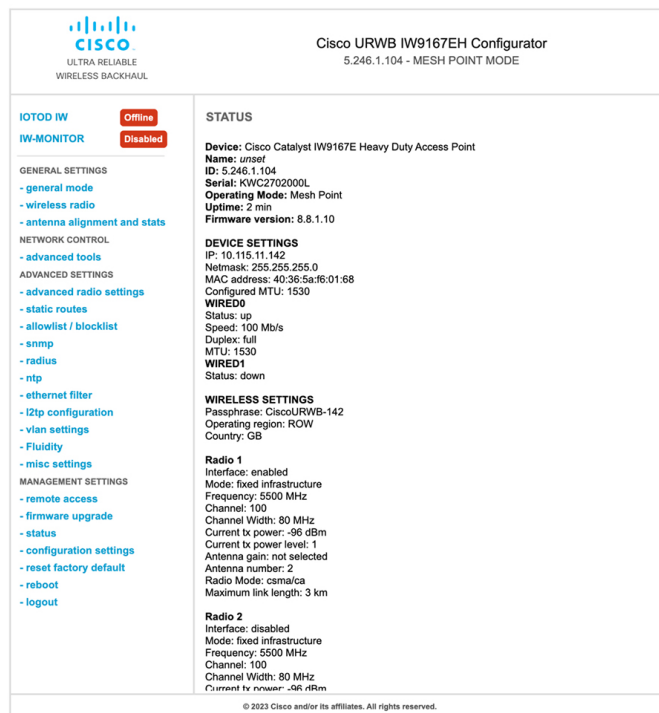
- For ROW domain, if the country code is not selected, the Web UI will display an alert toast as follows.



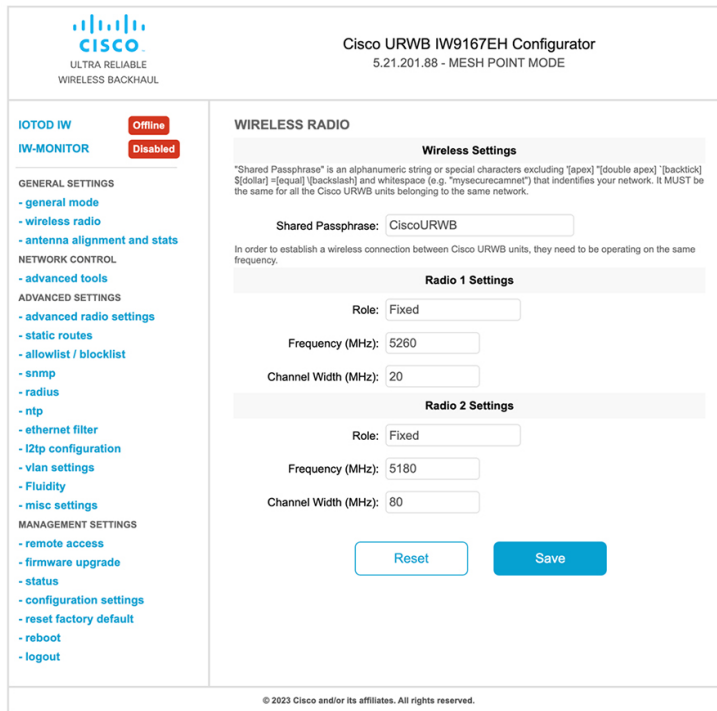
- To select a country code, click the alert toast displays in the below image then the user will be redirected to Web UI wireless section for selecting country code.



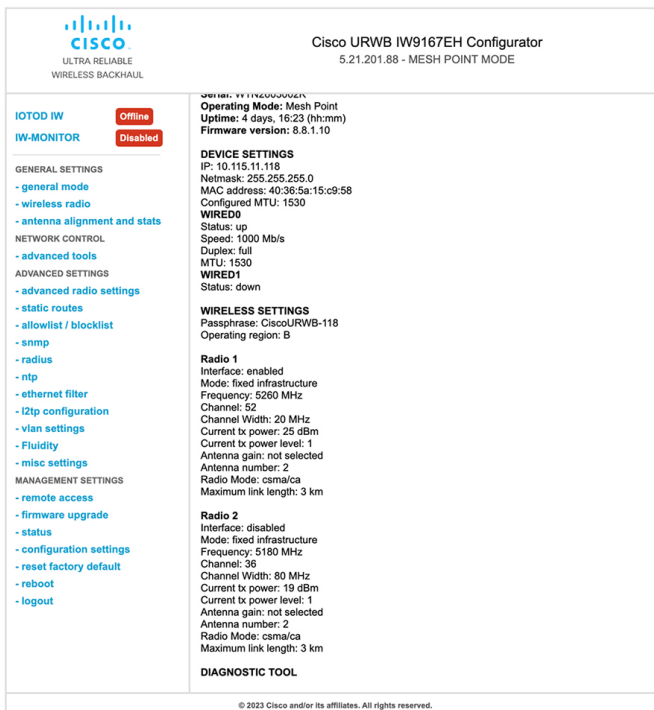
- User must click on "status" link on the left side of menu page and check operating region and country code availability in wireless setting status page.



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



6. The below image shows the configuration of regularity domain from GUI.



Configuring IOT-OD 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 internet. 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, the user can choose following options.

- configure the device manually using CLI and web UI.
- configure the device on IOTOD cloud service and select the configuration file exported from IOD-OD industrial wireless and upload the configuration file by using upload configuration button at the end of IOT-IW management page.

To activate or deactivate IOTOD-IW (IOT Industrial Wireless) configuration capability, use the following CLI command.

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

online - set up IOTOD IW mode to online. The device can be managed from the IOTOD IW cloud server (if it is connected to the Internet).

offline - set up IOTOD IW mode to offline. (The device is disconnected from IOTOD-IW and must be manually configured using the CLI, or its offline Configurator interface.)

Configuring Strong 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 1 and 32 characters.
- The password length should be from 8 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

Upload Configuration



CHAPTER 3

Configuring Cisco URWB Radio Mode

- [Configuring Cisco URWB Radio Mode, on page 15](#)
- [Configuring Radio-off Mode from CLI, on page 16](#)
- [Configuring Fluidity Role from CLI, on page 17](#)
- [Configuring Radio Mode for Cisco URWB from CLI, on page 17](#)
- [Configuring AMPDU from CLI, on page 18](#)
- [Configuring Frequency from CLI, on page 18](#)
- [Configuring Maximum MCS Index from CLI, on page 19](#)
- [Configuring Maximum NSS \(Number of Spatial Streams\) Index from CLI, on page 19](#)
- [Configuring Rx-SOP Threshold from CLI, on page 19](#)
- [Configuring RTS Mode from CLI, on page 19](#)
- [Configuring WMM Mode from CLI, on page 20](#)
- [Configuring NTP Enhancement from CLI, on page 20](#)
- [Configuring NTP Enhancement from GUI, on page 21](#)
- [Validating Radio Mode for Cisco URWB, on page 22](#)
- [Configuring Radio-off Mode from GUI, on page 22](#)
- [Configuring Radio Mode from GUI, on page 23](#)

Configuring Cisco 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 3: Radio Mode Configuration

Radio Role	Mode on Radio*	Description
Fixed Infrastructure	fixed	P2P mode (point to point)
	Fluidmax primary	P2MP (point to multipoint) mode (Fluidmax), P2MP, Master
	Fluidmax secondary	P2MP mode (Fluidmax), P2MP
Mobility AP	Fluidity	Mobility Mode

Radio Role	Mode on Radio*	Description
Mobility Client	Fluidity	Mobility Mode

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

Table 4: 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 5: 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 Fluidity Role from 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 Radio Mode for Cisco URWB from CLI

To configure Radio mode for Cisco 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 vehicle 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 from CLI

To configure an ampdu (Aggregated MAC Protocol Data Unit) 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 all

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 MCS Index from CLI

To configure maximum MCS (modulation coding scheme) 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 - 11.

WORD AUTO.



Note The maximum MCS can be set between 0 to 9 if High Efficiency mode is disabled and maximum MCS can be set as 10 and 11 if High Efficiency mode is enabled.

Configuring Maximum NSS (Number of Spatial Streams) Index from CLI

To configure maximum NSS (Number of Spatial Streams) index, use the following CLI commands:

Set maximum spatial stream number in integer or string “AUTO”.

For “AUTO”, the background process will automatically configure the maxnss.

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

maxnss values:

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

WORD AUTO.

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 Enhancement 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 Enhancement from GUI

The following image shows the Web UI of NTP enhancement.

The screenshot displays the Cisco URWB IW9167EH Configurator interface. The main heading is "Cisco URWB IW9167EH Configurator" with the IP address "5.212.77.232 - MESH END MODE". A status message indicates "NTP time is not synchronized". The left sidebar shows navigation options under "IOTOD IW" and "FM-QUADRO", with "ntp" selected under "ADVANCED SETTINGS". The main content area is titled "NTP - Network Time Protocol" and contains the following configuration fields:

- Enable NTP:**
- NTP server hostname:** 192.168.216.201
- NTP authentication:** MD5 (selected from a dropdown menu)
- NTP password:** [masked with dots] (with a "show" checkbox)
- Select Timezone:** Asia/Shanghai (selected from a dropdown menu)

A warning message states "WARNING: NTP time is not synchronized". At the bottom of the configuration area are "Reset" and "Save" buttons.

Validating Radio Mode for Cisco 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 AP (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 Cisco IOT IW9167E Heavy Duty Access Point at the head end and connecting this unit to a wired network such as LAN.

The screenshot displays the Cisco URWB IW9167EH Configurator interface. The title bar indicates the device model and the current mode: "Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE". The interface is divided into a left sidebar and a main configuration area.

Left Sidebar:

- IOTOD IW (Offline)
- FM-QUADRO
- GENERAL SETTINGS
 - general mode
 - wireless radio
 - antenna alignment and stats
- NETWORK CONTROL
 - advanced tools
- ADVANCED SETTINGS
 - advanced radio settings
 - static routes
 - allowlist / blocklist
 - multicast
 - snmp
 - radius
 - ntp
 - I2tp configuration
 - vlan settings
 - Fluidity
 - misc settings
 - smart license
- MANAGEMENT SETTINGS
 - remote access
 - firmware upgrade
 - status
 - configuration settings
 - reset factory default
 - reboot
 - logout

Main Configuration Area (GENERAL MODE):

General Mode

Select MESH END mode if you are installing this Cisco Catalyst IW9167E Heavy Duty Access Point at the head end and connecting this unit to a wired network (i.e. LAN).

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:

Buttons: Reset, Save

© 2022 Cisco and/or its affiliates. All rights reserved.

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 Cisco URWB units. To configure a Radio mode from GUI, set the operating mode for specified radio (Radio1 and Radio2) interface as below diagram.

The screenshot shows the Cisco URWB IW9167EH Configurator GUI. The main content area is titled "WIRELESS RADIO". It contains the following sections:

- Wireless Settings**: A text box for "Shared Passphrase" containing the text "PASSWORD". Below it, a note states: "In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency."
- Radio 1 Settings**: Three dropdown menus: "Role" set to "Fixed", "Frequency (MHz)" set to "5180", and "Channel Width (MHz)" set to "80".
- Radio 2 Settings**: A dropdown menu for "Role" set to "Disabled".

At the bottom of the configuration area, there are two buttons: "Reset" and "Save".

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 Cisco URWB transmission power control (TPC) will automatically select the optimum transmission power.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

ADVANCED RADIO SETTINGS

Radio 1

FluidMAX Management

Force the FluidMAX operating mode of this unit. If the operating mode is Primary/Secondary a FluidMAX Cluster ID can be set. 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 Secondaries will be disabled.

Radio Mode: PRIMARY

FluidMAX Cluster ID: CLUSTER_ID

Max TX Power

Select the max power level that the radio shall use to transmit (power level 1 sets the highest transmit power). The Cisco URWB TPC (Transmit Power Control) will automatically select the optimum transmission power according to the channel condition while not exceeding the MAX TX Power parameter. Note: in Europe TPC is automatically enabled.

Select TX Max Power: 1

Antenna Configuration

Select radio 1 antenna gain and antenna number.

Select Antenna Gain: UNSELECTED

Antenna number: ab-antenna

Data Packet Encryption

Enable AES to cypher all wireless traffic. This setting must be the same on all the Cisco URWB units.

Enable AES: Disabled

Maximum link length

Insert the length of the longest link in the net, or let the system select an optimal value.

© 2022 Cisco and/or its affiliates. All rights reserved.



Note In Europe TPC is automatically enabled.

- 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 Cisco URWB transmission power control (TPC) will automatically select the optimum transmission power.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

ADVANCED RADIO SETTINGS

Radio 1

FluidMAX Management

Force the FluidMAX operating mode of this unit. If the operating mode is Primary/Secondary a FluidMAX Cluster ID can be set. 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 Secondaries will be disabled.

Radio Mode: SECONDARY

FluidMAX Cluster ID: CiscoURWB

FluidMAX Autoscan:

Max TX Power

Select the max power level that the radio shall use to transmit (power level 1 sets the highest transmit power). The Cisco URWB TPC (Transmit Power Control) will automatically select the optimum transmission power according to the channel condition while not exceeding the MAX TX Power parameter. Note: in Europe TPC is automatically enabled.

Select TX Max Power: 1

Antenna Configuration

Select radio 1 antenna gain and antenna number.

Select Antenna Gain: UNSELECTED

Antenna number: ab-antenna

Data Packet Encryption

Enable AES to cypher all wireless traffic. This setting must be the same on all the Cisco URWB units.

Enable AES: Disabled

Maximum link length

Insert the length of the longest link in the net, or let the system select an optimal value.

© 2022 Cisco and/or its affiliates. All rights reserved.



Note In Europe TPC is automatically enabled.

- 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.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

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. "mys@ccarmer") that identifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase:

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

Radio 1 Settings

Role:

Frequency (MHz):

Channel Width (MHz):

Radio 2 Settings

Role:

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

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 from 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:

Network Type:

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:

© 2022 Cisco and/or its affiliates. All rights reserved.



CHAPTER 4

Configuring Radio Antenna Settings

- [Configuring Radio Antenna Settings, on page 27](#)

Configuring Radio Antenna Settings

The IW9167EH supports eight external antennas with eight type-N female connectors to support multiple antenna options. Three ports numbered 1, 4, and 5 can read the information stored within self-identifying antennas (SIA). Radio 1 connects to ports 1 to 4, and Radio 2 connects to ports 5 to 8. For more information on antennas, refer to the Hardware Installation Guide https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw9167/hardware/installation/b-iw9167eh-hig/m-about-iw9167e.html#Cisco_Concept.dita_ccda37ff-d976-420f-a87d-9d9683017ab3

The following CLI commands used 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 user 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.

```
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 to power level 1.

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



CHAPTER 5

Configuring and Validating Radio Channel and Bandwidth

- [Configuring Operating Channel from CLI, on page 29](#)
- [Configuring Channel Bandwidth from CLI, on page 29](#)
- [Validating Operating Channel and Bandwidth from CLI, on page 30](#)
- [Configuring Radio Channel and Bandwidth from GUI, on page 30](#)
- [Configuring Fluidity from GUI, on page 31](#)

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
```

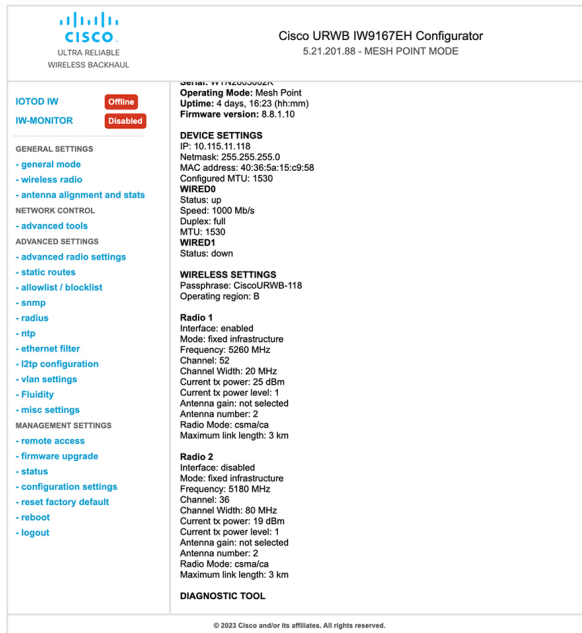
Configuring Radio Channel and Bandwidth from GUI

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.



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



Configuring Fluidity from GUI

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

Set the radio role to Fluidity, as shown in the diagram below.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

WIRELESS RADIO

Wireless Settings

"Shared Passphrase" is an alphanumeric string or special characters excluding "[apex]" "[double apex]" "[backtick]" "[colon]" "[equal]" "[backslash]" and whitespace (e.g. "my@conncam.net") that identifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase:

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

Radio 1 Settings

Role:

Frequency (MHz):

Channel Width (MHz):

Radio 2 Settings

Role:

© 2022 Cisco and/or its affiliates. All rights reserved.

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

IOTUD IW Offline

FM-QUADRO

GENERAL SETTINGS

- general mode
- wireless radio
- antenna alignment and stats

NETWORK CONTROL

- advanced tools

ADVANCED SETTINGS

- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license

MANAGEMENT SETTINGS

- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout

FLUIDITY

Fluidity Settings

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 from 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:

Automatic Vehicle ID: Enable

Vehicle ID:

Network Type:

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:

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

IOTUD IW Offline

FM-QUADRO

GENERAL SETTINGS

- general mode
- wireless radio
- antenna alignment and stats

NETWORK CONTROL

- advanced tools

ADVANCED SETTINGS

- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license

MANAGEMENT SETTINGS

- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout

FLUIDITY

Fluidity Settings

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 from 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:

Automatic Vehicle ID: Enable

Network Type:

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:

© 2022 Cisco and/or its affiliates. All rights reserved.

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

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

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., "mys@creamnet") that identifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase:

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

Radio 1 Settings

Role:

Frequency (MHz):

Channel Width (MHz):

Radio 2 Settings

Role:

© 2022 Cisco and/or its affiliates. All rights reserved.

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

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 from 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:

Network Type:

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:

© 2022 Cisco and/or its affiliates. All rights reserved.

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.



CHAPTER 6

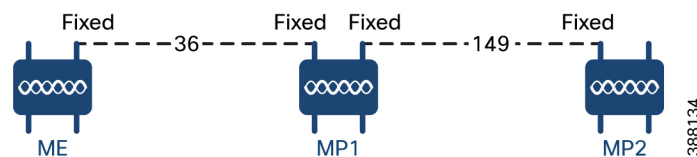
Configuring and Validating of Point-to-Point Relay Topology

- [Configuring and Validating of Point-to-Point Relay Topology, on page 37](#)
- [Configuring Point to Point Relay Topology from CLI, on page 37](#)
- [Validating Point to Point Relay Topology from CLI, on page 38](#)

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 1: point to point relay topology



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

1. Configure ME (Mesh End) 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 MP2 (Mesh Point) and wait for 30 seconds then point-to-point relay topology implemented by two radio interfaces on a single device.

Configuring Point to Point Relay Topology from CLI

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

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

```
Device# configure dot11Radio <interface>
```
2. Set wireless interface admin state to enable or disable mode.

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

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

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

4. Set the operating channel for the specified interface and the operating channel id 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.

ME (Mesh End) Configuration

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

MP1 (Mesh Point) 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
```

ME (Mesh End) 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
```

MP1 (Mesh Point) 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 7

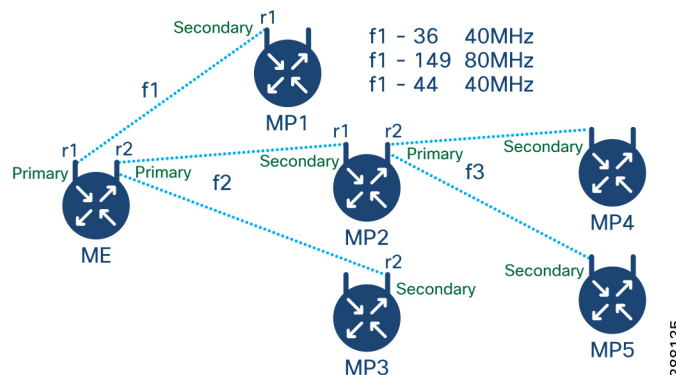
Configuring and Validating Fluidmax Topology

- [Configuring and Validating Fluidmax \(point to multipoint\) Topology, on page 41](#)

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 2: Two cascaded Fluidmax Topology



Configuring Point to Multipoint Topology from CLI

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

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

```
Interface - <0-3> Dot11Radio interface number.
```

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

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

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

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

Primary | secondary - 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 8

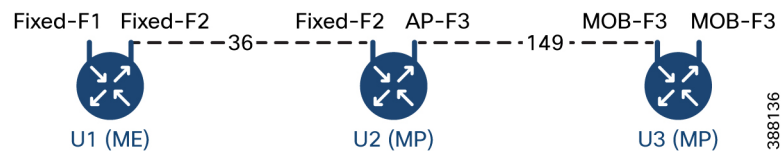
Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology

- [Configuring and Validating Mixed Mode \(Fixed Infrastructure + Fluidity\) Topology, on page 45](#)
- [Configuring Mixed Mode Topology from CLI, on page 45](#)

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 below diagram, U2 is configured with one radio in fixed infrastructure and the second radio as a Fluidity AP 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 3: 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 9

Configuring and Validating Fluidmax Fast Failover

- [Configuring and Validating Fluidmax Fast Failover, on page 49](#)
- [Configuring Fluidmax Fast Failover from CLI, on page 49](#)
- [Validating Fluidmax Fast Failover from CLI, on page 50](#)

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 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-fllood
```

```
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 10

Configuring and Validating High Efficiency (802.11 ax)

- [Configuring and Validating High Efficiency, on page 51](#)
- [Configuring Global Gateway from GUI, on page 52](#)

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.

- Cisco URWB HE supports 20/40/80 MHz bandwidth for slot 1.
- Cisco URWB HE supports 20/40/80/160 MHz bandwidth for slot 2.
- Cisco 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.



ULTRA RELIABLE
WIRELESS BACKHAUL

Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE

IOTOD IW Offline

FM-QUADRO

GENERAL SETTINGS

- general mode
- wireless radio
- antenna alignment and stats

NETWORK CONTROL

- advanced tools

ADVANCED SETTINGS

- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license

MANAGEMENT SETTINGS

- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout

GENERAL MODE

General Mode

Global Gateway mode automatically enforces MPLS layer 3 and radio-off. Radio status cannot be changed in Global Gateway mode.

mesh point
 mesh end
 gateway

Radio-off: Fluidity v

LAN Parameters

Local IP:

Local Netmask:

Default Gateway:

Local Dns 1:

Local Dns 2:

Reset
Save

© 2022 Cisco and/or its affiliates. All rights reserved.

WIRELESS RADIO

Wireless Settings

"Shared Passphrase" is an alphanumeric string or special characters excluding "[apex]" "[double apex]" "[backtick]" "\$[dollar]" "[equal]" "[backslash]" and whitespace (e.g. "mysecurecarnet") that identifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase:

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

Radio 1 Settings

Role:

Radio 2 Settings

Role:

Reset
Save

FLUIDITY

Fluidity Settings

The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming from 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 ▾

Reset

Save



CHAPTER 11

Configuring Guard Interval for HE (High Efficiency)

- [Configuring Guard Interval for HE, on page 55](#)

Configuring Guard Interval for HE

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 12

Configuring Indoor Deployment for -E Domain

- [Configuring Indoor Deployment for -E Domain, on page 57](#)

Configuring Indoor Deployment for -E Domain

The IW9167E supports enabling indoor deployment for -E domain and user can turn on and off indoor deployment by configuration on URWB CLI.



Note It is the responsibility of the user to ensure that the IW9167EH 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-only in -E countries..

Outdoor mode is always the default.

To enable indoor deployment (5 GHz reg domain changes from -E to -Ei) use the following CLI command.

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

To disable indoor deployment (5 GHz reg domain changes from -Ei to -E) 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 13

Configuring and Validating SNMP

- [Configuring and Validating SNMP, on page 59](#)

Configuring and Validating SNMP

SNMP (simple network monitoring protocol) applications used in Cisco 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 4: 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 from GUI

The following images shows the configuration of SNMP from GUI

GUI for SNMP v2:

The screenshot shows the Cisco URWB IW9167EH Configurator interface. The main title is "Cisco URWB IW9167EH Configurator" with the version "5.21.200.136 - MESH END MODE". The left sidebar contains a navigation menu with categories like "IOTOD IW", "GENERAL SETTINGS", "NETWORK CONTROL", "ADVANCED SETTINGS", and "MANAGEMENT SETTINGS". The "SNMP" configuration page is active, showing the following settings:

- SNMP mode: v2c
- Community ID: test
- Enable SNMP periodic trap:
- Enable SNMP event trap:
- NMS hostname: 192.168.0.100
- Notification period (minutes): 1

Buttons for "Reset" and "Save" are visible at the bottom of the configuration area.

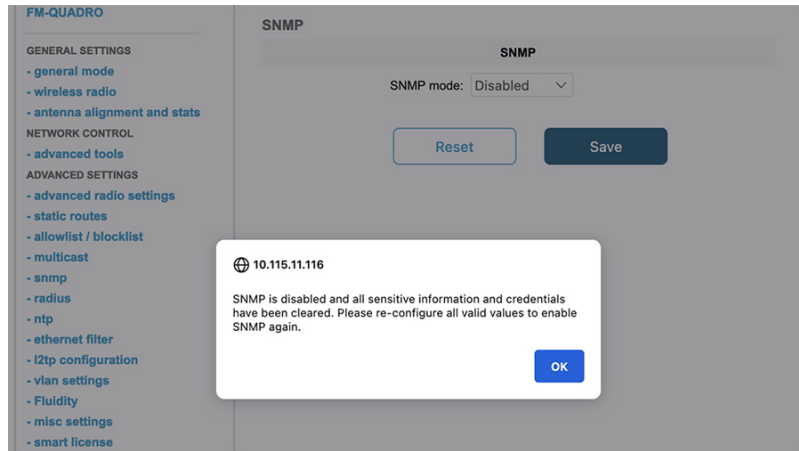
GUI for SNMP v3:

The screenshot shows the Cisco URWB IW9167EH Configurator interface for SNMP v3 configuration. The main title is "Cisco URWB IW9167EH Configurator" with the version "5.21.200.136 - MESH END MODE". The left sidebar is the same as in the previous screenshot. The "SNMP" configuration page is active, showing the following settings:

- SNMP mode: v3
- SNMP v3 username: user
- SNMP v3 password: *****
- Show SNMP v3 password:
- SNMP v3 authentication proto: SHA
- SNMP v3 encryption: AES
- SNMP v3 encryption passphrase: *****
- Show SNMP v3 encryption passphrase:
- Enable SNMP periodic trap:
- Enable SNMP event trap:
- Engine ID: *Currently Unavailable*
- NMS hostname: 192.168.0.100
- Notification period (minutes): 1

Buttons for "Reset" and "Save" are visible at the bottom of the configuration area.

Disable SNMP via GUI





CHAPTER 14

Configuring and Validating Key Controller (Wireless Security)

- [Configuring and Validating Key Controller \(Wireless Security\)](#), on page 65

Configuring and Validating Key Controller (Wireless Security)

To support wireless security to standard WPA protocols, a key rotation strategy has been implemented on 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 15

Configuring and Validating Smart Licensing

- [Configuring and Validating Smart Licensing from CLI, on page 67](#)
- [Configuring Smart Licensing from GUI, on page 70](#)

Configuring and Validating Smart Licensing from CLI

Smart licensing for Cisco Catalyst IW9167E Heavy Duty Access Point support the following scenarios:

- Smart license management provides a seamless experience with the various aspects of licensing.
- License level can control the feature list 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 could connect to CSSM (Cisco Smart Software Manager) directly to sync license usage.
- Airgap mode could use the downloaded file to sync with CSSM manually.
- User should configure same license level on both primary and secondary layer2 ME (Mesh End) or layer3 GW (Global Gateway).



Note Make sure device syncs up right time from NTP (Network Time Protocol) server to establish connection with CSSM successfully.

Smart license level can control the feature list by using the following table:

License Type	Features
Essentials	Unlimited fixed infra throughput (Fluidity and pure fixed infra). 0.5 Mbps Mobility client throughput.
Advantage	50 Mbps mobility client throughput. Cisco URWB Essentials.

License Type	Features
Premier	Unlimited mobility client throughput. Cisco URWB Advantage. Cisco URWB Essentials .

To configure smart license, use the following CLI command.

```
Device# configure license iw-level advantage
```

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_CSSM> 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 2 days.

When active devices > configured license seats, ME will try to send license usage report to CSSM every 8 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 CSSM 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 procedures.

1. Select the network license level for Cisco URWB stack.
2. The license level is bound to software features and monitored by CSSM.
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 CSSM Acknowledge and sync license usage, import the ACK (Acknowledge) that downloaded from CSSM 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
5.21.201.88 - MESH END MODE

SMART LICENSE

Smart License Settings

Select the network license level for Cisco URWB stack.
The license level is bound to software features and monitored by the CSSM.
Set the network seats to consume usage for particular license level.

License Level: Network Essentials for Radios

Platform IW9165 License Seats: 0

Platform IW9167 License Seats: 0

Reset Save

Smart Agent is set to Online Mode

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

Cisco URWB IW9167EH Configurator
5.21.201.88 - MESH END MODE

SMART LICENSE

Smart License Settings

Select the network license level for Cisco URWB stack.
The license level is bound to software features.
Set the network seats to consume usage for particular license level.

License Level: Network Advantage for Radios


Platform IW9165 License Seats: 0

Platform IW9167 License Seats: 0

Reset Save

Smart Agent is set to Online Mode

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



CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL

Cisco URWB IW9167EH Configurator
5.21.201.88 - MESH END MODE

IOTOD IW Offline

IW-MONITOR Disabled

FM-QUADRO

GENERAL SETTINGS

- general mode
- wireless radio
- antenna alignment and stats

NETWORK CONTROL

- advanced tools

ADVANCED SETTINGS

- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license

MANAGEMENT SETTINGS

- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout

SMART LICENSE

Smart License Settings

Select the network license level for Cisco URWB stack.
The license level is bound to software features and monitored by the CSSM.
Set the network seats to consume usage for particular license level.

License Level: Network Essentials for Radios

Platform IW9165 License Seats:

Platform IW9167 License Seats:

Reset
Save

1
Smart Agent is set to Airgap(Offline) Mode

Download Usage

Save RUM reports (license usage information). Save all RUM reports using All options. Save RUM report for the last n number of days (excluding the current day) using Days option. Save all unreported RUM reports using Unreported option.

Usage range: All

Days:

Download

Upload CSSM ACK

Import the ACK that downloaded from CSSM on the production instance.

Browse
No file selected

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

© 2023 Cisco Systems, Inc. All rights reserved.

