# cisco.



### Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.15.1

First Published: 2024-08-14

#### **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

| P R E F A C E | Preface ix<br>About this Guide ix<br>Related Documentation ix<br>Communications, Services, and Additional Information x |
|---------------|---|
| CHAPTER 1     | Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1   |
|               | Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1   |
| CHAPTER 2     | Initial Configuration of the Device in Provisioning Mode 3  |
|               | Resetting the Device to Factory Default Using GUI 8   |
|               | Rebooting the Device using GUI 9  |
|               | Saving and Restoring the Device Settings <b>10</b>  |
|               | Configuring General Settings 11   |
|               | Connecting to the Access Point Console Port <b>12</b>   |
| CHAPTER 3     | IPv6 Support 15   |
|               | Overview 15   |
|               | IPv6 Address Types 15   |
|               | IPv6 Limitations on the AP <b>16</b>  |
|               | Enable or Disable IPv6 using CLI 16   |
|               | Enable or Disable IPv6 RA Autoconfig using CLI 16   |
|               | Configure Static IPv6 Address with eui-64, Gateway, and DNS Server Address 17   |
|               | Verify Static IPv6 Address with eui-64, Gateway, and DNS Server Address 17  |
|               | Configure Static IPv6 Address without eui-64, Gateway, and DNS Server Address 17  |
|               | Verify Static IPv6 Address without eui-64, Gateway, and DNS Server Address 17   |

|           | Configure Static IPv6 Address with eui-64 18                           |
|-----------|--|
|           | Verify Static IPv6 Address with eui-64 <b>18</b>                       |
|           | Configure Static IPv6 Address without eui-64 18                        |
|           | Verify Static IPv6 Address without eui-64 18                           |
|           | Clear the IPv6 Gateway and DNS Servers Configuration 18                |
|           | Verify the Cleared IPv6 Gateway and DNS Servers Configuration 19       |
|           | Enable and Configure Static IPv6 using GUI <b>19</b>                   |
|           | Verify Static IPv6 using GUI <b>21</b>                                 |
| CHAPTER 4 | Configuring URWB Operation Mode 23                                     |
|           | Configuring URWB Operation Mode 23                                     |
|           | Determining from CLI <b>23</b>   |
|           | Reset Button Settings 24   |
|           | Configuring Image Conversion 24  |
|           | Instructions to Access the GUI <b>24</b>                               |
|           | URWB Catalyst IW9167E Configuration from GUI 25                        |
|           | Committing CLI Configuration <b>26</b>                                 |
|           | Configuring IoT OD Online and Offline Mode from CLI <b>27</b>          |
|           | Configuring Password (after first login) from CLI <b>27</b>            |
|           | Configuring IoT OD IW from GUI 29                                      |
| CHAPTER 5 | Configuring URWB Radio Mode 31   |
|           | Configuring URWB Radio Mode 31   |
|           | Configuring Radio-off Mode from CLI 32                                 |
|           | Configuring Radio Mode for URWB from CLI <b>33</b>                     |
|           | Configuring AMPDU using CLI <b>33</b>                                  |
|           | Configuring Frequency from CLI 34                                      |
|           | Configuring Maximum Modulation Coding Scheme Index from CLI 34         |
|           | Configuring Maximum Number of Spatial Streams Index from CLI <b>35</b> |
|           | Configuring Rx-SOP Threshold from CLI <b>35</b>                        |
|           | Configuring RTS Mode from CLI <b>35</b>                                |
|           | Configuring WMM Mode from CLI <b>35</b>                                |
|           | Configuring NTP from CLI <b>36</b>                                     |
|           | Configuring NTP from GUI <b>37</b>                                     |
|           |  |

I

|            | <ul><li>Validating Radio Mode for URWB 37</li><li>Configuring Radio-off Mode from GUI 38</li><li>Configuring Radio Mode from GUI 38</li></ul> |
|------------|---|
| CHAPTER 6  | IoT Operations Dashboard Cluster 43   |
|            | Overview 43   |
|            | Configure IoT Operations Dashboard Cluster from CLI <b>43</b>   |
|            | Verify IoT Operations Dashboard Cluster 44  |
| CHAPTER 7  |   |
|            | Configuring Radio Antenna Settings <b>45</b>  |
|            | Configuring Antenna Gain 45   |
|            | Configuring Transmit and Receive Antennas 46  |
|            | Configuring Transmission Power 46   |
|            | Validate URWB Individual Antenna RSSI Values 46   |
| CHAPTER 8  | Configuring Wired Interface 49  |
|            | Enabling and Disabling Wired Interface <b>49</b>  |
|            | Configuring Maximum Transmission Unit Settings <b>50</b>  |
| CHAPTER 9  | Enable or Disable SSH and Web UI Access 51  |
|            | Enable SSH Access 51  |
|            | Disable SSH Access 51   |
|            | Enable Web UI Access 52   |
|            | Disable Web UI Access 52  |
| CHAPTER 10 | — Configuring and Validating Radio Channel and Bandwidth 53   |
|            | Configure Operating Channel from CLI 53   |
|            | Configure Channel Bandwidth from CLI 54   |
|            | Validating Operating Channel and Bandwidth from CLI 54  |
|            | Configuring Radio Channel and Bandwidth from GUI 55   |
|            | Configuring VLAN Settings 56  |
|            | Rules for Packet Management 57  |

I

|            | Configuring Fluidity using GUI <b>57</b>   |
|------------|--|
|            | Configuring Fluidity using CLI 61  |
|            | Configuring Fluidity Role using CLI 62   |
|            | Configuring Fluidity Coloring <b>62</b>  |
| CHAPTER 11 | Configuring and Validating High Efficiency (802.11 ax) 67                                |
|            | Configuring and Validating High Efficiency 67  |
|            | Configuring Global Gateway from GUI <b>68</b>  |
| CHAPTER 12 | Configuring Guard Interval for HE (High Efficiency) 71                                   |
|            | Configuring Guard Interval for HE (High Efficiency) <b>71</b>                            |
| CHAPTER 13 | — Configuring and Validating SNMP 73   |
|            | Configuring and Validating SNMP 73   |
|            | Configuring SNMP from CLI <b>73</b>  |
|            | Validating SNMP from CLI <b>75</b>   |
|            | Configuring SNMP Version v2c using GUI <b>75</b>   |
|            | Configuring SNMP Version v3 using GUI <b>76</b>  |
| CHAPTER 14 | <ul> <li>Configuring and Validating Key Controller (Wireless Security) 79</li> </ul>     |
|            | Configuring and Validating Key Controller (Wireless Security) 79                         |
|            | Configuring Key Controller from CLI <b>79</b>  |
|            | Validating Key Controller from CLI 80  |
| CHAPTER 15 | FIPS Certification 81  |
|            | FIPS Certification 81  |
|            | Enable or Disable FIPS Mode using CLI 81   |
|            | Verify FIPS Mode using CLI 81  |
| CHAPTER 16 | <ul> <li>Configuring, Supporting the Fixed Domains and Country Codes (ROW) 83</li> </ul> |
|            | Configuring and Verifying Country Code using CLI 83                                      |
|            | Configuring Country Code using GUI 84  |
|            | Supporting Fixed Domains and Country Codes (ROW) 87                                      |

I

|            | Catalyst IW9167E Supported Fixed Domains 87  |
|------------|--|
|            | Catalyst IW9167E Supported Country Codes (ROW) 87                                      |
|            | Catalyst IW9165E Supported Fixed Domains 88  |
|            | Catalyst IW9165E Supported Country Codes (ROW) 89                                      |
|            | Catalyst IW9165D Supported Fixed Domains 90  |
|            | Catalyst IW9165DH Supported Country Codes (ROW) 90                                     |
| CHAPTER 17 | — Configuring and Validating of Point-to-Point Relay Topology 93                       |
|            | Configuring and Validating of Point-to-Point Relay Topology 93                         |
|            | Configuring Point to Point Relay Topology from CLI 93                                  |
|            | Validating Point to Point Relay Topology from CLI 94                                   |
| CHAPTER 18 | Configure and Validate Fluidmax Topology 97  |
|            | Configure and Validate Fluidmax (point to multipoint) Topology 97                      |
|            | Configure Point to Multipoint Topology from CLI 97                                     |
|            | Validate Point to Multipoint Topology using CLI 99                                     |
| CHAPTER 19 | — Configuring and Validating Mixed Mode (Fixed infrastructure + Fluidity) Topology 101 |
|            | Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology 101   |
|            | Configuring Mixed Mode Topology from CLI <b>101</b>                                    |
|            | Validating Mixed Mode Topology from CLI <b>102</b>                                     |
| CHAPTER 20 | Configure and Validate Fast Failover 105   |
|            | Overview of Fast Failover 105  |
|            | Configure and Validate Fast Failover <b>105</b>  |
|            | Configure Fast Failover from CLI 106   |
|            | Validate Fast Failover from CLI 106  |
|            |  |
| CHAPTER 21 | –<br>Configuring Indoor Deployment 109   |
| CHAPTER 21 | Configuring Indoor Deployment 109<br>Configuring Indoor Deployment 109                 |
| CHAPTER 21 |  |

I

|            | Configuring and Verifying Layer-2 Protocols Forwarding Using CLI <b>112</b> |
|------------|---|
|            | Configuring Layer-2 Protocol Forwarding using GUI 114                       |
| CHAPTER 23 | Configuring Multipath Operation 121   |
|            | Overview of MPO 121   |
|            | Working Functionality of MPO 121  |
|            | MPO Packet Duplication and Deduplication 121                                |
|            | Configuring MPO Features Using CLI 122                                      |
|            | Verifying MPO Features Using CLI (MPO Monitoring) 123                       |
|            | MPO Limitations 125   |
| CHAPTER 24 | Configuring URWB Telemetry Protocol 127                                     |
|            | Configuring URWB Telemetry Protocol <b>127</b>                              |
| CHAPTER 25 |   |
|            | Configuring IW Monitor Management 131                                       |
| CHAPTER 26 | — Upgrading the Device using TFTP 135                                       |
|            | Device Upgrade using TFTP 135   |
|            | Automatic Device Upgrade using TFTP 135                                     |
|            | Configuring Manifest File on the TFTP Server 136                            |
|            | Manifest File Format 136  |
|            | Direct Device Upgrade using TFTP 137  |
|            | TFTP Device Upgrade using CLI <b>137</b>                                    |
| CHAPTER 27 | LED Pattern for Catalysts IW9167 and IW9165 139                             |
|            | LED Pattern for Catalyst IW9167 139   |
|            | LED Pattern for Catalyst IW9165 140   |
| CHAPTER 28 |   |
|            | Packet Retries Limitation 143   |
|            | Configure Maximum Retry Limit for Packet Retransmissions using CLI 143      |
|            | Verify Maximum Retry Limit for Packet Retransmissions using CLI 143         |

I

#### Contents

I



# **Preface**

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

It includes the following sections:

- About this Guide, on page ix
- Related Documentation, on page ix
- Communications, Services, and Additional Information, on page x

### **About this Guide**

This guide details the configuration of the URWB mode of operation for the Cisco Catalysts IW9167E, IW9165E, and IW9165D access points. UWRB is supported as part of the Unified Industrial Wireless (UIW) software. UIW Release 17.15.1 introduces these new features:

- IPv6 Support
- FIPS Certification
- Packet Retries Limitation
- Support for 15dBi Antennas
- Enable or Disable SSH and Web UI Access
- Flexibility in URL Cluster Setting for IW Products
- Additional Country Support
- Show Command for Individual Antenna RSSI
- 4.9 GHz Support for Japan (-Q domain)

### **Related Documentation**

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

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

### **Communications, Services, and Additional Information**

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

#### **Cisco Bug Search Tool**

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

#### **Documentation Feedback**

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



CHAPTER

# Overview of Cisco Catalyst IW9167E and IW9165 Access Points

Overview of Cisco Catalyst IW9167E and IW9165 Access Points, on page 1

### **Overview of Cisco Catalyst IW9167E and IW9165 Access Points**

#### **Overview of Cisco Catalyst IW9167E**

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

#### **Overview of Cisco Catalyst IW9165**

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

The Catalyst IW9165 series is available in two models:

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

#### **Cisco Catalyst IW9165E Rugged Access Point and Wireless Client**

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

From UIW Release 17.14.1, the Catalyst IW9165E supports the Dying Gasp functionality. Once the DC-IN power supply stops, the Dying Gasp functionality allows the device to preserve power for at least 100 ms. During this time, the device sends a message to other devices in the network indicating that it is about to shut down, and this avoids abrupt packet transmission failure. Catalyst IW9165E generates the Dying Gasp messages, and the Catalysts IW9165D, IW9165E, and IW9167E devices process these messages.

#### **Cisco Catalyst IW9165D Access Point**

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



# Initial Configuration of the Device in Provisioning Mode

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

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



Note

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

- Username: Cisco
- Password: Cisco

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

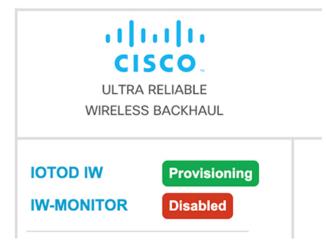
DHCP is only used in provisioning mode. A static IP address must be assigned for normal operation. If DHCP is unavailable and configuration through IoT OD is required, the IP address, subnet, default gateway, and DNS can be manually configured.



Note

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

• To verify if the device is in provisioning mode, go to the device configurator interface and the status of IoT OD IW is shown as **Provisioning**:



• To verify if the device is in provisioning mode, use the following show command:

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

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

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

| IOTOD IW Cloud   | connection info           |
|------------------|---------------------------|
| Server Host:     | IOTOD Industrial Wireless |
| Status:          | Disconnected              |
| Current IP Co    | onfiguration              |
| Current IP:      | 192.168.0.10 (fallback)   |
| Current Netmask: | 255.255.255.0             |

| IOTOD IW Cloud   | connection info                                 |  |  |  |  |  |
|--|---|--|--|--|--|--|
| Server Host:   | IOTOD Industrial Wireless                       |  |  |  |  |  |
| Status:  | Disconnected                                    |  |  |  |  |  |
| Current IP Co  | onfiguration                                    |  |  |  |  |  |
| Current IP: 192.168.10.2   |   |  |  |  |  |  |
| Current Netmask:   | 255.255.255.0                                   |  |  |  |  |  |
|  |   |  |  |  |  |  |
| Configure DHCP to c  | onnect to IOTOD IW                              |  |  |  |  |  |
| Use this section to connect the radio to the Internet via D back IP settings if DHCP is not available. | HCP to use IOTOD IW Cloud Management. Set fall- |  |  |  |  |  |
| DHCP fall-back   | configuration                                   |  |  |  |  |  |
| Local IP:  | 192.168.10.2                                    |  |  |  |  |  |
| Local Netmask:   | 255.255.255.0                                   |  |  |  |  |  |
| Default Gateway:   | 192.168.10.1                                    |  |  |  |  |  |
| Local Dns 1:   | 192.168.10.200                                  |  |  |  |  |  |
| Local Dns 2:   |   |  |  |  |  |  |
| Reset to Prov  | visioning                                       |  |  |  |  |  |

The device's status and LEDs blink continuously and LEDs repeat this cycle until the device either enters a fallback condition, or enters **Online**, or **Offline** mode. To know more about LED status, see LED Pattern for Catalyst IW9165, on page 140 or LED Pattern for Catalyst IW9167, on page 139.



#### Note

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

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

| IOTOD IW Cloud conne | IOTOD IW Cloud connection info |  |  |  |  |  |  |
|----------------------|--------------------------------|--|--|--|--|--|--|
| Server Host:         | IOTOD Industrial Wireless      |  |  |  |  |  |  |
| Status:              | Connected                      |  |  |  |  |  |  |
| Current IP Configu   | ration                         |  |  |  |  |  |  |
| Current IP:          | 10.115.11.152 (dhcp)           |  |  |  |  |  |  |
| Current Netmask:     | 255.255.0.0                    |  |  |  |  |  |  |

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



**Note** In the provisioning mode, the IP, netmask, default gateway, primary DNS, and secondary DNS configuration (IP command) are allowed.

| Device# | configur | е | ip a | lddre | ess | ipv4 | 1 [ | st | cat | cic | 2 1 | ΙP | address | [ | static | netmask | [ | ΙP | address | of |
|---------|----------|---|------|-------|-----|------|-----|----|-----|-----|-----|----|---------|---|--------|---------|---|----|---------|----|
| default | gateway  | [ | dns1 | . ip  | [   | dns2 | ip  | ]  | ]   | ]   | ]   | ]  |         |   |        |         |   |    |         |    |

For example:

Device# configure ip address ipv4 static 192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200 192.168.10.201

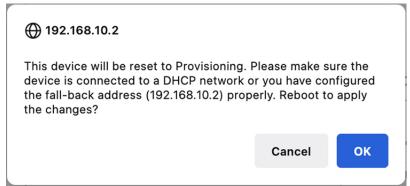
The device sets the fallback address (192.168.0.10 by default) or the configured IP address automatically if it does not receive an address from the DHCP server. If the device fails to connect to IoT OD IW, verify the following to reach IoT OD IW:

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

If the device fails to connect to the network in provisioning mode, follow these steps:

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

A reboot confirmation pop-up appears:



- 2. Click OK or Reset to go back to IoT OD IW and adjust the settings.
  - Once you click **OK**, the device reboots and remains in provisioning mode.
  - The device attempts to connect to the network using the new connection values.
- 3. If the device fails to connect to the network using the DHCP settings, IoT OD IW Cloud connection Status is shows as Disconnected.

| IOTOD IW Cloud   | connection info           |
|------------------|---------------------------|
| Server Host:     | IOTOD Industrial Wireless |
| Status:          | Disconnected              |
| Current IP Co    | onfiguration              |
| Current IP:      | 192.168.0.10 (fallback)   |
| Current Netmask: | 255.255.255.0             |

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

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

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

```
Device#show ip

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers:

DHCP Address (PROVISIONING Mode):

IP: 10.0.0.2

Network: 255.255.0

Gateway: 10.0.0.1

Nameservers: 8.8.8.8

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

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

```
Device#show ip
               192.168.0.10
IP:
Network:
             255.255.255.0
Gateway:
Nameservers:
DHCP Address (PROVISIONING Mode):
IP: 192.168.0.10
Network:
             255.255.255.0
Gateway:
Nameservers: 127.0.0.1
Fallback Address (PROVISIONING Mode):
        169.254.201.72
IP:
             255.255.0.0
Network:
  • Resetting the Device to Factory Default Using GUI, on page 8
```

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

### **Resetting the Device to Factory Default Using GUI**

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



**Note** A hard reset reverts all device configuration settings, including the device IP address and administrator password to factory defaults. Instead if you want to reboot the device, see Rebooting the Device using GUI, on page 9.

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH POINT MODE |
|--|---|
| OTOD IW Offline<br>V-MONITOR Disabled  | Are you sure you want to reset to factory default settings?       |
| ENERAL SETTINGS general mode wrietes racio antenna algament and stats ETWORK CONTROL advanced tools OWANCED SETTINGS advanced racio settings static routes advanced racio settings static routes advanced racio settings atlowist / blocklist allowist / blocklist al | NO YES  |

- 2. Click YES in the confirmation pop-up window. To abort the factory reset, click NO.
- **3.** If you have previously saved a configuration file for the device, you can restore the saved configuration settings to the device, see Saving and Restoring the Device Settings, on page 10.



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

#### **Resetting the Device to Factory Default Using CLI**

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

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

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

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

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

The following files are cleared as part of this process:

```
    Config, Bak config files
    Crashfiles
    syslogs
    Boot variables
    Pktlogs
    Manually created files
    you want to proceed? (y/n)
```

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

### **Rebooting the Device using GUI**

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

1. In the MANAGEMENT SETTINGS, click reboot.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH POINT MODE                   |
|---|---|
| OTOD IW Offline<br>W-MONITOR Disabled   | Are you sure you want to reboot the unit?<br>Any pending changes will be discarded. |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio                                    | No Yes  |
| - antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS |   |
| - advanced radio settings<br>- static routes<br>- allowlist / blocklist                   |   |
| - snmp<br>- radius<br>- ntp<br>- ethernet filter  |   |
| - I2tp configuration<br>- vlan settings<br>- Fluidity                                     |   |
| misc settings<br>MANAGEMENT SETTINGS<br>remote access                                     |   |
| - firmware upgrade<br>- status<br>- configuration settings                                |   |
| reset factory default<br>reboot<br>logout   |   |

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

#### **Rebooting the Device using CLI**

To perform reboot, use the following CLI command:

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

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

### **Saving and Restoring the Device Settings**

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

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



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

 $\mathcal{P}$ 

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

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

1. In the MANAGEMENT SETTINGS, click configuration settings.

The LOAD OR RESTORE SETTINGS window appears.

| COTOD IV CILLING   WAMONTOR Database   WAMONTOR Database   WAMONTOR Database   CENERAL SETTINGS Restore Settings from file:   I and and alignment and stats Restore Settings   WAMONTOR CONTROL Restore Settings from file:   I advanced diod Settings Restore Settings  | ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH POINT MODE |
|--|--|---|
| General. SETTINGS - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced Todio Settings - advanced radio Settings - radius Settings - radius - ethernet filter - 12tp configuration - vina settings - ethernet filter - 12tp configuration - vina settings - result settings - res | IOTOD IW Offline   | LOAD OR RESTORE SETTINGS  |
| General mode<br>• wireless radio<br>• antenna alignment and stats<br>NETWORK CONTROL<br>• advanced Todis<br>• advanced radio settings<br>• factors<br>• ethernet filter<br>• 12tp configuration<br>• vina settings<br>• Fluidity<br>• miss settings<br>• Fluidity<br>• miss settings<br>• remote access<br>• filtiware upgrade<br>• status<br>• configuration settings<br>• reset factory default<br>• resetord<br>• logout  | IW-MONITOR Disabled  | Restore Settings  |
|  | - general mode<br>- wreless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>Advanced setTinkS<br>- advanced radio setTings<br>- static routes<br>- static routes<br>- static routes<br>- allowiist / blocklist<br>- smp<br>- radius<br>- radius<br>- radius<br>- radius<br>- radius<br>- therent filter<br>- 12tp configuration<br>- Vian settings<br>- Vian settings<br>- Nakotess<br>- Filuidity<br>- misc settings<br>MANAGEMENT SETTINGS<br>- remole access<br>- firmware upgrade<br>- status<br>- configuration settings<br>- status<br>- configuration settings<br>- reset factory debutt |   |
| © 2023 Cisco andior its affiliates. All rights reserved.   |  |   |
|  |  | © 2023 Cisco andior its affiliates. All rights reserved.          |

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

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

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

### **Configuring General Settings**

To change the General Mode settings, follow these steps:

1. In the GENERAL SETTINGS, click general mode.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL | Cisco URWB IW91<br>5.81.160.244 - ME   |   |
|-------------------------------------|--|---|
| IOTOD IW Offline                    | GENERAL MODE   |   |
| W-MONITOR Disabled                  | General  | Mode  |
| GENERAL SETTINGS                    | Select MESH POINT mode if you are attaching an IP edg<br>Cisco IOT IW9165E Series Access Point or if you are using | e device (i.e. network camera, encoder, etc.) to this<br>ng this unit as a relay point in the mesh network. |
| - general mode                      |  | mesh point  |
| wireless radio                      | Mode:  | -   |
| - antenna alignment and stats       |  | O gateway   |
| NETWORK CONTROL                     |  | O gateway   |
| - advanced tools                    | Radio-off:   | 0   |
| ADVANCED SETTINGS                   | Radio-oii.   | 0   |
| - advanced radio settings           | LAN Para   | ameters   |
| - static routes                     |  |   |
| - allowlist / blocklist             | Local IP:  | 10.115.11.180   |
| - snmp                              |  |   |
| - radius                            | Local Netmask:   | 255.255.255.0   |
| - ntp                               |  |   |
| - ethernet filter                   | Default Gateway:   | 10.115.11.1   |
| - I2tp configuration                | Local Dns 1:   | 8888  |
| - vlan settings                     | Local Dira 1.  |   |
| - Fluidity                          | Local Dns 2:   |   |
| - misc settings                     |  |   |
| MANAGEMENT SETTINGS                 |  |   |
| - remote access                     | Reset  | Save  |
| - firmware upgrade                  |  |   |
| - status                            |  |   |
| - configuration settings            |  |   |
| - reset factory default<br>- reboot |  |   |
| - logout                            |  |   |
| 109041                              |  |   |
|                                     |  |   |

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



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

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

- Gateway This mode is applicable for advanced Layer 3 mobility deployments, and it is not used in most networks.
- Mesh Point This mode is applicable for the remaining access points in the network. These access points establish links to other access points with the same network passphrase configured as mesh end or mesh point using wireless links or wired links. In this scenario, the access point has Layer 2 visibility of other access points.

• Mesh End - This mode configures the access point to perform control and administrative network functions. There must be at least one mesh end in each network. This access point is typically installed in the most central point where the wireless and wired networks converge.

#### **Configuring General Settings using CLI**

To configure general settings, use the following CLI command:

```
Device#configure modeconfig mode
gateway layer 3 global gateway mode
meshend mesh end mode
meshpoint mesh point mode
Device#configure modeconfig mode meshend
mpls MPLS support
radio-off disable radio interfaces
```

#### **Changing the LAN Parameters**

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

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

#### Configuring LAN Parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

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

### **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:

- 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 |

| Parameter    | Value        |
|--------------|--------------|
| 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

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



# **IPv6 Support**

- Overview, on page 15
- IPv6 Address Types, on page 15
- IPv6 Limitations on the AP, on page 16
- Enable or Disable IPv6 using CLI, on page 16
- Enable or Disable IPv6 RA Autoconfig using CLI, on page 16
- Configure Static IPv6 Address with eui-64, Gateway, and DNS Server Address, on page 17
- Verify Static IPv6 Address with eui-64, Gateway, and DNS Server Address, on page 17
- Configure Static IPv6 Address without eui-64, Gateway, and DNS Server Address, on page 17
- Verify Static IPv6 Address without eui-64, Gateway, and DNS Server Address, on page 17
- Configure Static IPv6 Address with eui-64, on page 18
- Verify Static IPv6 Address with eui-64, on page 18
- Configure Static IPv6 Address without eui-64, on page 18
- Verify Static IPv6 Address without eui-64, on page 18
- Clear the IPv6 Gateway and DNS Servers Configuration, on page 18
- Verify the Cleared IPv6 Gateway and DNS Servers Configuration, on page 19
- Enable and Configure Static IPv6 using GUI, on page 19
- Verify Static IPv6 using GUI, on page 21

### **Overview**

From UIW Release 17.15.1, APs support IPv6 addresses. By default, the IPv6 service is disabled on the AP. You can enable and configure the IPv6 address on the AP using either the CLI or GUI.

### **IPv6 Address Types**

You can configure the AP with the following IPv6 address types:

- Link-Local
- Unique-Local
- Global Unicast

#### Link-Local

Link-local addresses are used within the scope of a single link and cannot be routed. These addresses refer specifically, to a particular physical link and are used for addresses on a single link for purposes such as automatic address configuration and the neighbor discovery protocol. Link-local addresses can be used to reach the neighboring nodes attached to the same link.

#### **Unique-Local**

Unique local addresses can be routed within a private organization, but not through the public internet. It is not expected to be routable on the global Internet. However, it is routable inside a limited area, such as a site, and it may route between a limited set of sites.

#### **Global Unicast**

A global unicast address is a routable address in the IPv6 Internet, similar to the public IPv4 address space.

# **IPv6 Limitations on the AP**

- The IPv6 support is limited only to host functionality.
- The Fluidity Layer 3 network does not support IPv6.

### **Enable or Disable IPv6 using CLI**

By default, IPv6 support is disabled on the AP. When IPv6 is enabled, a link-local address is automatically assigned to the AP.

Use this command to enable or disable the IPv6 address on the AP.

```
Device#configure ipv6 {enable | disable}
```

### Enable or Disable IPv6 RA Autoconfig using CLI

Use this command to enable or disable the IPv6 RA Autoconfig on the AP.

Device#configure ipv6 enable autoconfig-ra {enable | disable}

• Enable: Enables the autoconfiguration from router advertisement.

• Disable: Disables the autoconfiguration from router advertisement.

# Configure Static IPv6 Address with eui-64, Gateway, and DNS Server Address

Use this command to configure the static IPv6 address with eui-64, gateway, and DNS server address on the AP.

Device#configure ap address ipv6 static fc00::4236:5aff:xxxx:168/64 eui-64 fc00::1
2001:4860:4860::xxxx 2001:4860::xxxx

# Verify Static IPv6 Address with eui-64, Gateway, and DNS Server Address

To verify the static IPv6 address with eui-64, gateway, and DNS server address on the AP, use the following **show** command:

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::4236:5aff:xxxx:168/64
Gateway: fc00::1
DNS1: 2001:4860:4860::xxxx
DNS2: 2001:4860:4860::xxxx
Currently assigned addresses:
fc00::4236:5aff:xxxx:168/64 global
fe80::4236:5aff:xxxx:168/64 link
```

# Configure Static IPv6 Address without eui-64, Gateway, and DNS Server Address

Use this command to configure the static IPv6 address without eui-64, gateway, and DNS server address on the AP.

```
Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def/64 fc00::1
2001:4860:4860::xxxx 2001:4860:4860::xxxx
```

# Verify Static IPv6 Address without eui-64, Gateway, and DNS Server Address

To verify the static IPv6 address without eui-64, gateway, and DNS server address on the AP, use the following **show** command:

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/64
```

```
Gateway: fc00::1
DNS1: 2001:4860:4860::xxxx
DNS2: 2001:4860:4860::xxxx
Currently assigned addresses:
fc00::1234:5678:xxxx:def/64 global
fe80::4236:5aff:xxxx:168/64 link
```

### **Configure Static IPv6 Address with eui-64**

Use this command to configure the static IPv6 address with eui-64 on the AP.

Device#configure ap address ipv6 static fc00::4236:5aff:xxxx:168/64 eui-64

### Verify Static IPv6 Address with eui-64

To verify the static IPv6 address with eui-64 on the AP, use the following **show** command:

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::4236:5aff:xxxx:168/64
Currently assigned addresses:
fc00::4236:5aff:xxxx:168/64 global
fe80::4236:5aff:xxxx:168/64 link
```

### **Configure Static IPv6 Address without eui-64**

Use this command to configure the static IPv6 address without eui-64 on the AP.

Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def

### **Verify Static IPv6 Address without eui-64**

To verify the static IPv6 address without eui-64 on the AP, use the following **show** command:

```
Device#show ipv6
IPv6: Enabled
Router Advertisement auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/128
Currently assigned addresses:
fc00::1234:5678:xxxx:def/128 global
fe80::4236:5aff:xxxx:168/64 link
```

### **Clear the IPv6 Gateway and DNS Servers Configuration**

Use this command to clear the IPv6 gateway and DNS servers addresses configuration on the AP.

Device#configure ap address ipv6 static fc00::1234:5678:xxxx:def/64 :: :: ::

### **Verify the Cleared IPv6 Gateway and DNS Servers Configuration**

To verify the cleared IPv6 gateway and DNS server addresses configuration on the AP, use the following **show** command:

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/64
Currently assigned addresses:
fc00::1234:5678:xxxx:def/64 global
fe80::4236:5aff:xxxx:168/64 link
```

# Note

While adapting services to work with IPv6, such as TFTP, you must consider that link-local IP addresses might require network interface specifications.

### **Enable and Configure Static IPv6 using GUI**

```
Procedure
```

| Step 1 | Launch the computer's web browser and enter the URL to open the configurator login page.        |
|--------|---|
| Step 2 | Enter the username and password in the respective fields.                                       |
| Step 3 | Click <b>Login</b> .<br>Once you successfully log into the GUI, the URWB configurator displays. |
| Step 4 | In the GENERAL SETTINGS, click general mode to open the General Mode window.                    |

| ULTRA RELIABLE<br>WIRELESS BACKHAUL         |  | 167EH Configurator<br>ESH POINT MODE                                  |   |
|---|--|---|---|
| IOTOD IW Offline                            | GENERAL MODE   |   |   |
| W-MONITOR Disabled                          | Genera   | Mode  |   |
| GENERAL SETTINGS                            | Select MESH POINT mode if you are attaching an IP edg<br>Cisco Catalyst IW9167E Heavy Duty Access Point or if yo | e device (i.e. network camera, e<br>ou are using this unit as a relay | encoder, etc.) to this<br>point in the mesh |
| - general mode                              | network.   |   |   |
| - wireless radio                            |  | <ul> <li>mesh point</li> </ul>  |   |
| - antenna alignment and stats               | Mode:  | mesh end  |   |
| NETWORK CONTROL                             |  | 🔘 gateway   |   |
| - advanced tools                            |  |   |   |
| ADVANCED SETTINGS                           | Radio-off:   |   |   |
| <ul> <li>advanced radio settings</li> </ul> |  |   |   |
| - static routes                             | LAN Para   | ameters   |   |
| ADVANCED SETTINGS                           |  |   |   |
| advanced radio settings                     | Local IP:  | 10.115.11.129   |   |
| static routes                               | Local Netmask:   | 255.255.255.0   |   |
| allowlist / blocklist                       | Eodal Notifiasi.   | 200.200.200.0   |   |
| - snmp                                      | Default Gateway:   | 10.115.11.1   |   |
| radius                                      |  |   |   |
| - ntp                                       | Local Dns 1:   | 8.8.8.8   |   |
| - ethernet filter                           | Local Dns 2:   | 4 4 4 4   |   |
| - I2tp configuration                        | Local Dris 2.  | 4.4.4.4   |   |
| - vlan settings                             | Enable IPv6:   |   |   |
| - Fluidity<br>- misc settings               | RA Autoconfig:   |   |   |
| MANAGEMENT SETTINGS                         |  | _   |   |
| - remote access                             | Local IPv6:  |   |   |
| - firmware upgrade                          | Use EUI-64:  |   |   |
| - status                                    |  |   |   |
| - configuration settings                    | Default Gateway IPv6:  |   |   |
| - reset factory default                     | Local Dns 1 IPv6:  |   |   |
| - reboot                                    | Looa Dis FirVo.  |   |   |
| - logout                                    | Local Dns 2 IPv6:  |   |   |
|   |  |   |   |
|   |  |   |   |
|   | Reset  | Save  |   |

**Note** In the GUI, the term "local" refers to the IPv4 or IPv6 addresses that are set up statically. Specifically, the **Local IPv6** accepts all type of IPv6 address, which allows for the static configuration of the device's IPv6 address.

- **Step 5** Check the **Enable IPv6** check box. The system automatically enables the **RA Autoconfig**.
- **Step 6** Enter IPv6 address in the **Local IPv6** field.
- **Step 7** (Optional) Check the **Use EUI-64** check box.

**Note** IPv6 addresses differ with and without the eui-64 option.

- **Step 8** (Optional) Enter the gateway IP address in the **Default Gateway IPv6** field.
- **Step 9** (Optional) Enter the DNS server 1 IP address in the Local Dns 1 IPv6 field.
- **Step 10** (Optional) Enter the DNS server 2 IP address in the Local Dns 2 IPv6 field.
- Step 11 Click Save.

# **Verify Static IPv6 using GUI**

Procedure

I

| Step 1 | In the MANAGEMENT SETTINGS, click status.  |
|--------|--|
| Step 2 | On the <b>STATUS</b> page, in the <b>DEVICE SETTINGS</b> section, you can view the IPv6 details. |

Verify Static IPv6 using GUI

I



# **Configuring URWB Operation Mode**

- Configuring URWB Operation Mode, on page 23
- Determining from CLI, on page 23
- Reset Button Settings, on page 24
- Configuring Image Conversion, on page 24
- Instructions to Access the GUI, on page 24
- URWB Catalyst IW9167E Configuration from GUI, on page 25
- Committing CLI Configuration, on page 26
- Configuring IoT OD Online and Offline Mode from CLI, on page 27
- Configuring Password (after first login) from CLI, on page 27
- Configuring IoT OD IW from GUI, on page 29

### **Configuring URWB Operation Mode**

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

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

### **Determining from CLI**

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

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

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

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

Device# show iotod-iw status

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

### **Reset Button Settings**

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

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

### **Configuring Image Conversion**

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

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

configure boot mode urwb

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

```
configure boot mode capwap
```

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

configure boot mode wgb

```
Note
```

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

### Instructions to Access the GUI

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

 To access a Web UI, open the web browser and enter the following URL: https://<IP address of unit>/ The IW9167E or IW9165 Configurator window appears. 

| ULTRA RELIABLE<br>WIRELESS BACKHAUL             | Cisco URWB IW9167EH Configurator<br>5.21.201.112 - MESH END MODE |
|---|--|
|   | Login  |
| Username:<br>Enable Password:<br>Show password: | ]<br>Login   |
| © 2022 Cisco                                    | and/or its affiliates. All rights reserved.                      |

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL                       | Cisco URWB IW91<br>5.21.201.72 - ME  |   |
|---|--|---|
| IOTOD IW Offline  | GENERAL MODE   |   |
| FM-QUADRO   | Genera   | I Mode  |
| GENERAL SETTINGS<br>- general mode                        | Select MESH POINT mode if you are attaching an IP edg<br>Cisco Catalyst IW9167E Heavy Duty Access Point or if yo<br>network. | ou are using this unit as a relay point in the mesh |
| - wireless radio  |  | <ul> <li>mesh point</li> </ul>                      |
| <ul> <li>antenna alignment and stats</li> </ul>           | Mode:  | mesh end  |
| NETWORK CONTROL   |  | ⊖ gateway   |
| - advanced tools  |  |   |
| ADVANCED SETTINGS   | Radio-off:   |   |
| <ul> <li>advanced radio settings</li> </ul>               |  | _   |
| - static routes   | LAN Para   | ameters   |
| - allowlist / blocklist                                   |  |   |
| - multicast   | Local IP:  | 10.115.11.117                                       |
| - snmp  |  |   |
| - radius  | Local Netmask:   | 255.255.255.0                                       |
| - ntp   | Default Gateway:   | 10.115.11.1   |
| - I2tp configuration                                      | bolaik balonay.  | 10.110.11.1   |
| - vlan settings   | Local Dns 1:   | 8.8.8.8   |
| - Fluidity  |  |   |
| - misc settings   | Local Dns 2:   |   |
| - smart license   |  |   |
| MANAGEMENT SETTINGS                                       |  |   |
| - remote access   | Reset  | Save  |
| - firmware upgrade  |  |   |
| - status  |  |   |
| - configuration settings                                  |  |   |
| <ul> <li>reset factory default</li> <li>reboot</li> </ul> |  |   |
| - reboot<br>- logout                                      |  |   |
| - 109041  |  |   |
|   | © 2022 Cisco and/or its affiliates. All rights reserved  | L   |

## **URWB Catalyst IW9167E Configuration from GUI**

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

| FM-QUADRO<br>GENERAL SETTINGS<br>general mode<br>- wireless radio<br>- antenna alignment and stats<br>network courrool<br>- advanced tools<br>Advanced tools<br>Advanced tools<br>- advanced tools<br>- advanced tools<br>- advanced tools<br>- adiowilist / blocklist<br>- allowilist / blocklist<br>- multicast<br>- annp<br>- radius | Radio-off:<br>LAN Par  | e device (i.e. network camera, encoder, etc.) to this<br>ou are using this unit as a relay point in the mesh<br>mesh point<br>mesh end<br>gateway |
|---|--|---|
| General settings<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings<br>- static routes<br>- allowlist / blocklist<br>- multicast<br>- simp<br>- radius   | Select MESH POINT mode if you are attaching an IP edg<br>Cicco Catalyst W9167E Heavy Duty Access Point or if y<br>network.<br>Mode:<br>Radio-off:<br>LAN Par | e device (i.e. network camera, encoder, etc.) to this<br>ou are using this unit as a relay point in the mesh<br>mesh point<br>mesh end<br>gateway |
| GENERAL SETTINGS - general mode - general mode - wrieless radio - antenna alignment and stats NETWORK CONTROL - advanced tools ADVANCED SETTINGS - advanced radio settings - static routes - allowilst / blocklist - multicast - simmp - radius   | Cleoc Gatalyst W9167E Heavy Duty Access Point or if y<br>network.<br>Mode:<br>Radio-off:<br>LAN Par  | ourreusing this unit as a relay point in the mesh mesh point mesh end gateway   |
| - antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings<br>- static routes<br>- aliowilat / blockilat<br>- multicast<br>- snmp<br>- radius   | Radio-off:<br>LAN Par  | <ul> <li>mesh end</li> <li>gateway</li> </ul>   |
| NETWORK CONTROL<br>advanced tools<br>ADVANCED SETTINGS<br>- static routes<br>- allowlist / blocklist<br>- multicast<br>- simp<br>- radius   | Radio-off:<br>LAN Par  | gateway   |
| - advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings<br>- static routes<br>- allowlist / blocklist<br>- multicast<br>- samp<br>- radius   | LAN Par  |   |
| ADVANCED SETTINGS<br>advanced radio settings<br>- static routes<br>- allowlist / blocklist<br>- multicast<br>- samp<br>- radius   | LAN Par  | _   |
| - advanced radio settings<br>- static routes<br>- allowilist / blocklist<br>- multicast<br>- samp<br>- radius   | LAN Par  | _   |
| - static routes<br>- allowlist / blocklist<br>- multicast<br>- snmp<br>- radius   | LAN Par  | _   |
| - allowlist / blocklist<br>- multicast<br>- snmp<br>- radius  |  | ameters   |
| - multicast<br>- snmp<br>- radius   | l ocal IP <sup>.</sup>   |   |
| - snmp<br>- radius  | Local IP:  |   |
| - radius  |  | 10.115.11.117   |
|   |  |   |
|   | Local Netmask:   | 255.255.255.0   |
| - ntp   |  | (   |
| - I2tp configuration  | Default Gateway:   | 10.115.11.1   |
| - vlan settings   | Local Dns 1:   | 8888  |
| - Fluidity  | Edda Brid H  |   |
| - misc settings   | Local Dns 2:   |   |
| - smart license   |  |   |
| MANAGEMENT SETTINGS   |  |   |
| - remote access   | Reset  | Save  |
| - firmware upgrade  |  |   |
| - status  |  |   |
| - configuration settings  |  |   |
| - reset factory default   |  |   |
| - reboot  |  |   |
| - logout  |  |   |

## **Committing CLI Configuration**

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

```
Device# write

or

Device# wr

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

Device# reload

reload: reload the device.

Example:

Device# write

!!! Please reboot to take effect

Device# reload
```

Proceed with reload? [confirm]

(enter to confirm)

### Configuring IoT OD Online and Offline Mode from CLI

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

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

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

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

Device# configure iotod-iw {offline | online}

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

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

### Configuring Password (after first login) from CLI

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

- The username length must be from 1 to 32 characters.
- The password length must be from 8 to 120 characters.
- The password must include the following:
  - At least one uppercase letter
  - · At least one lowercase character,
  - At least one digit
  - · At least one special character
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not allowed:
  - " [double quote]
- ' [single quote]
- ? [question mark]
- The password must not contain:
  - Three sequential characters or digits (ABC/CBA)

- The same three characters or digits consecutively (AAA) or (666)
- · Same as the current or existing password
- Same as or the reverse of the username

#### Example:

#### Default credentials:

username: Cisco password: Cisco enable password: Cisco

#### To reset the credentials, use the following sample credentials:

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

#### Example of configuring password using CLI:

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

#### After first login, reset the credentials:

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

#### Once the credentials are changed, re-login:

User access verification Username: demouser Password: DemoP@ssw0rd Device> enable

| Password:DemoE^aP@ssw0rd |  |
|--------------------------|--|
| Device#                  |  |



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

# **Configuring IoT OD IW from GUI**

The following image shows the configuration of IoT OD IW:

| eradio MUST be configured using the<br>ass US, (OTOD Industrial Wireless EU) If<br>Iguration is selected.<br>changes through the radio Web UI / CLI or<br>section in IOTOD Industrial Wireless ( <u>IOTOD</u><br>U).<br>can be configured from the Centralized Web<br>reless US or IOTOD Industrial Wireless EU) if it<br>V Cloud Server, Radio Web U and CLI are read- |
|---|
| section in IOTOD Industrial Wireless ( <u>IOTOD</u><br><u>U</u> ).<br>can be configured from the Centralized Web<br>reless US or IOTOD Industrial Wireless EU) if it  |
| reless US or IOTOD Industrial Wireless EU) if it  |
| v Cloud Server, kadio web of and CLI are read-  |
| ged Offline   |
| FILE  |
| guration File   |
| Browse No file selected   |
| 34  |
| I   |

l



# **Configuring URWB Radio Mode**

- Configuring URWB Radio Mode, on page 31
- Configuring Radio-off Mode from CLI, on page 32
- Configuring Radio Mode for URWB from CLI, on page 33
- Configuring AMPDU using CLI, on page 33
- Configuring Frequency from CLI, on page 34
- Configuring Maximum Modulation Coding Scheme Index from CLI, on page 34
- Configuring Maximum Number of Spatial Streams Index from CLI, on page 35
- Configuring Rx-SOP Threshold from CLI, on page 35
- Configuring RTS Mode from CLI, on page 35
- Configuring WMM Mode from CLI, on page 35
- Configuring NTP from CLI, on page 36
- Configuring NTP from GUI, on page 37
- Validating Radio Mode for URWB, on page 37
- Configuring Radio-off Mode from GUI, on page 38
- Configuring Radio Mode from GUI, on page 38

### **Configuring URWB Radio Mode**

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

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

#### Table 1: Radio Mode Configuration

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

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

Table 2: Operating Mode of Radio Interface

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

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

Table 3: Configuration of Multiple Radio interfaces

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

### **Configuring Radio-off Mode from CLI**

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



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

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

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

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

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

3. To set the radio-off mode.

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

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

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

Device# wr Example: Configure modeconfig mode meshend radio-off fluidity Configure modeconfig mode meshend radio-off fixed

### Configuring Radio Mode for URWB from CLI

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

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

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

Device# configure dot11Radio <interface>

2. Configure an operating mode for the specified interface.

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

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

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

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

3. Set Fluidmax role for Fluidmax interface mode.

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

Primary - set Fluidmax role to primary

Secondary - set Fluidmax role to secondary

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

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



Note

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

### **Configuring AMPDU using CLI**

To configure an Aggregated MAC Protocol Data Unit's (AMPDU) length and priority, use the following CLI commands:

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

length: <0-255> integer number – microseconds
Device# configure dotllradio <interface> ampdu priority {enable | disable}
enable: enable ampdu tx priority
disable: disble ampdu tx priority
Device# configure dotllradio <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 all indexes (index 0 to 7)

### **Configuring Frequency from CLI**

To configure an operating frequency, use the following CLI command: Device# configure dot11radio <interface> frequency <frequency> frequency: <0-7125> operating frequency in MHz

### Configuring Maximum Modulation Coding Scheme Index from CLI

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

Device# configure dot11radio <interface> mcs <maxmcs>

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

Maxmcs values:

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

Word AUTO



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

# Configuring Maximum Number of Spatial Streams Index from CLI

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

Device# configure dotl1radio <interface> spatial-stream <maxnss>

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

Maxnss values:

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

Word AUTO



Note

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

### **Configuring Rx-SOP Threshold from CLI**

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

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

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

### **Configuring RTS Mode from CLI**

To disable ready to send (RTS) mode, use the following CLI command: Device# configure dotl1radio <interface> rts <disable> Disable: Disables the RTS protection. To enable RTS with threshold value, use the following CLI command: Device# configure dotl1radio <interface> rts enable <threshold> Threshold: Threshold range <0 - 2346>.

### **Configuring WMM Mode from CLI**

To configure wireless multimedia (WMM) mode, use the following CLI command: Device# configure dotllradio <interface> wmm [bk|be|vi|vo] [bk|be|vi|vo]: Represents the class-of-service (CoS) parameters. be: Best-effort traffic queue (CS0 and CS3). bk: Background traffic queue (CS1 and CS2).

vi: Video traffic queue (CS4 and CS5).

vo: Voice traffic queue (CS6 and CS7).

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

Device# configure dot11Radio <interface> wifistats <clear>

Clear: Clear wireless stats counters.

### **Configuring NTP from CLI**

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

Device# configure ntp server <string>

String - IP address or domain name.

Example:

Device# configure ntp server 192.168.216.201

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

Device# configure ntp authentication none Device# configure ntp authentication md5 <password> <keyid> Device# configure ntp authentication shal <password> <keyid>

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

#### Example:

Device# configure ntp authentication md5 test1234 65535



Note

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

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

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

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

Device# configure ntp { enable|disable }

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

Device# configure ntp timezone <string>

Example:

Device# configure ntp timezone Asia/Shanghai

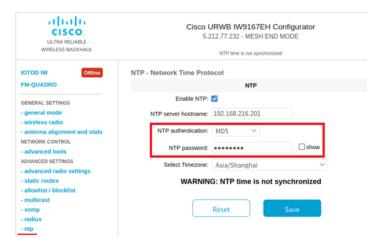
To validate the NTP configuration and status, use the following show commands:

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

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

### **Configuring NTP from GUI**

The following image shows the GUI of NTP:



### Validating Radio Mode for URWB

To validate Radio mode, use the following show commands:

Device# show dot11Radio <interface> config

Example:

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

```
Channel : 157
Channel width : 40 MHz
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
```

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

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

### **Configuring Radio-off Mode from GUI**

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |  |  |
|---------------------------------------|---|--|--|
| IOTOD IW Offline                      | GENERAL MODE  |  |  |
| FM-QUADRO                             | General Mode  |  |  |
| GENERAL SETTINGS                      | Select MESH END mode if you are installing this Cisco Catalyst IW9167E Heavy Duty Access Point at the head<br>end and connecting this unit to a wired network (i.e. LAN). |  |  |
| - general mode                        | () mesh point   |  |  |
| - wireless radio                      | Mode: O mesh end  |  |  |
| - antenna alignment and stats         | Qateway   |  |  |
| NETWORK CONTROL                       | 0.1   |  |  |
| - advanced tools<br>ADVANCED SETTINGS | Radio-off: V Fixed V  |  |  |
| - advanced radio settings             |   |  |  |
| - static routes                       | LAN Parameters  |  |  |
| - allowlist / blocklist               |   |  |  |
| - multicast                           | Local IP: 10.115.11.117   |  |  |
| - snmp                                | Local Netmask: 255.255.255.0  |  |  |
| - radius                              |   |  |  |
| - ntp<br>- I2tp configuration         | Default Gateway: 10.115.11.1  |  |  |
| - vlan settings                       | Local Dns 1: 8.8.8.8  |  |  |
| - Fluidity                            | Local Dris 1. 0.0.0   |  |  |
| - misc settings                       | Local Dns 2:  |  |  |
| - smart license                       |   |  |  |
| MANAGEMENT SETTINGS                   |   |  |  |
| - remote access<br>- firmware upgrade | Reset   |  |  |
| - status                              |   |  |  |
| - configuration settings              |   |  |  |
| - reset factory default               |   |  |  |
| - reboot                              |   |  |  |
| - logout                              |   |  |  |
|                                       |   |  |  |
|                                       | © 2022 Cisco and/or its affiliates. All rights reserved.  |  |  |

### **Configuring Radio Mode from GUI**

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

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

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL              | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |                       |  |  |
|--|---|-----------------------|--|--|
| IOTOD IW Offline                                 | WIRELESS RADIO  |                       |  |  |
| FM-QUADRO  | Wireless Settings   |                       |  |  |
| GENERAL SETTINGS<br>- general mode               | "Shared Passphrase" is an alphanumeric string or special characters excluding "geoxi "[double apex] ['backtick]<br>§joliar] =[equal] [backslash] and whitespace (e.g. "myscorecamnet") that identifies your network. It MUST be<br>the same for all the Class UMPN suits biologing) to be same network. |                       |  |  |
| - wireless radio                                 | Shared Passphrase: PASSWORD   |                       |  |  |
| - antenna alignment and stats<br>NETWORK CONTROL | In order to establish a wireless connection between Cisco URWB units, they need to be   | operating on the same |  |  |
| - advanced tools                                 | frequency.  |                       |  |  |
| ADVANCED SETTINGS                                | Radio 1 Settings  |                       |  |  |
| - advanced radio settings                        | Role: Fixed V   |                       |  |  |
| - static routes                                  |   |                       |  |  |
| - allowlist / blocklist                          | Frequency (MHz): 5180 V   |                       |  |  |
| - multicast                                      | Channel Width (MHz): 80 V   |                       |  |  |
| - snmp   |   |                       |  |  |
| - radius   | Radio 2 Settings  |                       |  |  |
| - ntp  | Role: Disabled V  |                       |  |  |
| - I2tp configuration<br>- vlan settings          |   |                       |  |  |
| - Fluidity                                       |   |                       |  |  |
| - misc settings                                  | Reset Save  |                       |  |  |
| - smart license                                  |   |                       |  |  |
| MANAGEMENT SETTINGS                              |   |                       |  |  |
| - remote access                                  |   |                       |  |  |
| - firmware upgrade                               |   |                       |  |  |
| - status   |   |                       |  |  |
| <ul> <li>configuration settings</li> </ul>       |   |                       |  |  |
| - reset factory default                          |   |                       |  |  |
| - reboot   |   |                       |  |  |
| - logout   |   |                       |  |  |

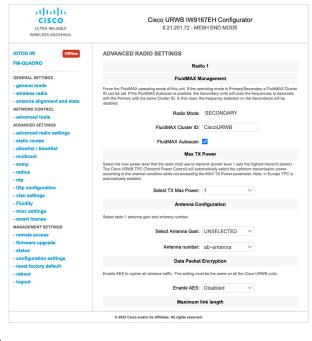
2. In the WIRELESS RADIO section, choose Radio 1 Role as Fluidmax Primary with FluidMAX Cluster ID. In this scenario, the frequency selection for the Primary is enabled and Secondary is disabled. In the ADVANCED RADIO SETTINGS window, go to Max TX Power section, and choose power level as 1 from the Select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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL                                 | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |  |  |  |
|---|---|--|--|--|
| IOTOD IW Offline  | ADVANCED RADIO SETTINGS   |  |  |  |
| FM-QUADRO   | Radio 1   |  |  |  |
| GENERAL SETTINGS  | FluidMAX Management   |  |  |  |
| - general mode<br>- wireless radio<br>- antenna alignment and stats | Force the FluidMAX operating mode of this unit. If the operating mode is Primary/Secondary a FluidMAX (<br>ID can be set. If the FluidMAX Autoscan is enabled, the Secondary units will scan the frequencies to asso<br>with the Primary with the same Cluster ID. In this case, the frequency selection on the Secondarys will be<br>disabled.   |  |  |  |
| NETWORK CONTROL<br>- advanced tools                                 | Radio Mode: PRIMARY   |  |  |  |
| ADVANCED SETTINGS<br>- advanced radio settings                      | FluidMAX Cluster ID: CLUSTER_ID   |  |  |  |
| - static routes   | Max TX Power  |  |  |  |
| - allowlist / blocklist<br>- multicast<br>- snmp                    | Select the max power level that the radio shall use to transmit (power level 1 sets the highest transmit pow<br>The Cisco URWB TPC (transmit Power Control) will automatically select the optimum transmission power<br>according to the channel condition while not exceeding the MAX TX Power parameter. Note: In Europe TP<br>automatically enabled.   |  |  |  |
| - radius<br>- ntp   | Select TX Max Power: 1 V  |  |  |  |
| - I2tp configuration  | Antenna Configuration   |  |  |  |
| - vlan settings<br>- Fluidity<br>- misc settings                    | Select radio 1 antenna gain and antenna number.   |  |  |  |
| - smart license<br>MANAGEMENT SETTINGS                              | Select Antenna Gain: UNSELECTED   |  |  |  |
| - remote access   | Antenna number: ab-antenna  |  |  |  |
| - firmware upgrade<br>- status                                      | Data Packet Encryption  |  |  |  |
| - configuration settings<br>- reset factory default                 | Enable AES to cypher all wireless traffic. This setting must be the same on all the Cisco URWB units.   |  |  |  |
| - reboot  | Enable AES: Disabled  |  |  |  |
| - logout  | Maximum link length   |  |  |  |
|   | Insert the length of the longest link in the net, or let the system select an optimal value.  |  |  |  |
|   | © 2022 Clsco and/or its affiliates. All rights reserved.  |  |  |  |
|   | <ul> <li>Construction of the second se<br/>Second second sec<br/>second second sec</li></ul> |  |  |  |

Note In Europe TPC is automatically enabled.

⋧

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





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

- 4. In the Fluidity Settings section, choose Unit Role as Infrastructure from the drop-down list, When the device acts as the entry point of the infrastructure for the mobile vehicles or choose unit role as Infrastructure (wireless relay) only when it used as a wireless relay agent to other infrastructure unit or choose unit role as a Vehicle when it is mobile.
- 5. Choose network type based on the to the general network architecture:
  - **a.** Choose **Flat** mode from **Network Type** drop-down list, if the network belongs to single layer-2 broadcast domain.
    - or
  - **b.** Choose **Multiple subnets** if the network belongs to single layer-3 broadcast domain.

I

| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE  |  |  |
|---|--|--|--|
| IOTOD IW Offline  | WIRELESS RADIO   |  |  |
| FM-QUADRO   | Wireless Settings  |  |  |
|   | "Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] '[backtick]   |  |  |
| GENERAL SETTINGS  | "Shared Passphrase" is an alphanumeric string or special characters excluding "(apex) "(double apex) "(backtick)<br>S(dolar) =[equal) [backsiash] and whitespace (e.g. "mysecurecannet") that indentifies your network. It MUST be<br>the same for all the Cisco URVB wints belonging to the same network.   |  |  |
| - general mode  |  |  |  |
| - wireless radio  | Shared Passphrase: PASSWORD  |  |  |
| <ul> <li>antenna alignment and stats</li> </ul>   | In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same  |  |  |
| NETWORK CONTROL   | In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same<br>frequency.  |  |  |
| - advanced tools  | Radio 1 Settings   |  |  |
| ADVANCED SETTINGS   | Role: Fluidity   |  |  |
| - advanced radio settings   | Role. Fluidity   |  |  |
| - static routes   | Frequency (MHz): 5180 V  |  |  |
| - allowlist / blocklist   |  |  |  |
| - multicast   | Channel Width (MHz): 80 V  |  |  |
| - snmp  | Radio 2 Settings   |  |  |
| radius  | Radio 2 Settings   |  |  |
| - ntp   | Role: Disabled V   |  |  |
| - I2tp configuration<br>- vlan settings   |  |  |  |
| - vian settings<br>- Fluidity   |  |  |  |
| - Fluidity<br>- misc settings   | Reset Save   |  |  |
| • misc settings<br>• smart license  |  |  |  |
| - SMART LICENSE<br>MANAGEMENT SETTINGS  |  |  |  |
| remote access   |  |  |  |
| - remote access<br>- firmware upgrade   |  |  |  |
| - status  |  |  |  |
| - status<br>- configuration settings  |  |  |  |
| - reset factory default   |  |  |  |
| - reboot  |  |  |  |
| logout  |  |  |  |
|   |  |  |  |
| altalta<br>cisco  | © 2022 Cisco and/or its attiliates. All rights reserved.<br>Cisco URWB IW9167EH Configurator   |  |  |
|   |  |  |  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE  |  |  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE  |  |  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings   |  |  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>NOTOD IW<br>FM-QUADRO   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings   |  |  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE  FLUIDITY  Fuldity Settings  The unit can operate in 3 modes: Infrastructure, finational unity, Vehide. The unit can expense that all end and unity owing it. Additional the infrastructure for the models vehicles   |  |  |
| UTTA RELIABLE<br>WIRELESS BACKHAUL<br>NOTOD IW<br>FM-QUADRO<br>SEENERAL SETTINGS  | Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE  FLUIDTY  Fuldity Settings The unit can operate in 3 modes infrastructure, infrastructure (vietness relay, Veide). The unit can operate in 3 modes infrastructure, infrastructure (vietness relay, Veide). The unit can be also infrastructure (vietness relay) of the final instructure for the mode) within 6 and a the final instructure (vietness relay).   |  |  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>NOTOD IW<br>FM-QUADRO<br>Beneral Settings<br>-general mode  | Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE  FLUIDTY  Fuldity Settings The unit can operate in 3 modes infrastructure, infrastructure (vietness relay, Veide). The unit can operate in 3 modes infrastructure, infrastructure (vietness relay, Veide). The unit can be also infrastructure (vietness relay) of the final instructure for the mode) within 6 and a the final instructure (vietness relay).   |  |  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>VITRO TO DI W<br>FM-QUADRO<br>DENERAL SETTINGS<br>- general mode<br>- wireless radio  | Cisco URWB IW9167EH Configurator<br>5:21.201.72 - MESH END MODE<br>FLUIDITY<br>Fullity Settings<br>The intermediate is a mode simple infrastructure (writes neity). While.<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (writes neity). While.<br>The unit can operate in 3 modes: Infrastructure, for the infrastructure for mode we wickles<br>and it is conserved to a wind neitwork (wicklosted) with the provided to a first neitwork (wicklesse) with the infrastructure noise. The unit<br>Infrastructure unit. In the operating mode, the unit MUST NOT be concreded to the wind induce backbone as<br>It will use the work of which is it models. Which BY must be set all which which is the infrastructure which use the unit is configured as<br>Which is, Secondary, Whiche BY must be a unique among all it models on the same vertice. Unit<br>Which is, Secondary, Whiche BY must be a unique among all the models with site of the same vertice. Unit<br>Which is, Secondary, Whiche BY must be a unique among all the models with site of the unit is configured as<br>the integration of the model with a site of the model with site of the model with site is of the model with site of the unit is not integrated as the model with a site of the model with the integrated on the same vertice. Unit  |  |  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>VIELESS BACKHAUL<br>OTOD IW<br>FM-QUADRO<br>SENERAL SETTINGS<br>-general mode<br>wirfless ratio<br>-antenna alignment and stats<br>KETWORK CONTROL<br>-advanced tools   | Cisco URWB IW9167EH Configurator<br>5:21.201.72 - MESH END MODE<br>FLUIDITY<br>Fullity Settings<br>The intermediate is a mode simple infrastructure (writes neity). While.<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (writes neity). While.<br>The unit can operate in 3 modes: Infrastructure, for the infrastructure for mode we wile less<br>and it is conserved to a wind neitwork (wideological infrastructure) (writes neity). While,<br>The unit must be at all infrastructure when it adds as the entry point of the infrastructure for mode we wile less<br>and it is conserved to a wind neitwork (wideological infrastructure) (writes neitwork) (writes infrastructure wite. In the operating mode, the unit MUST NOT be concreded to the wind induce baselines on the form of the proble unit as the ADN. when the unit is configured as<br>the writes the average and the unique among all in models unit astructure on the unit is configured as the a unique among all in models units induce on the same verteice. Unit<br>Writes, Segreding, Writes OF more than the a unique among all in models units induce on the same verteice. Unit   |  |  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>VIELESS BACKHAUL<br>OTOD IW<br>EM-QLADRO<br>SENERAL SETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>(ETWORK CONTROL<br>advanced tools  | Cisco URWB IW9167EH Configurator LS1210172 - MESH END MODE  FLUDITY  Fuldity Settings Model and  |  |  |
| ULTRA RELABLE<br>WIRELESS BLOCHAUL<br>OTOD IN OFfice<br>M-QUADRO<br>Eseral SetTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>antenna alignment and stats<br>LowArces SetTINGS<br>advanced radio settings   | Cisco URWB IW9167EH Configurator     Catalantian and a second and                                      |  |  |
| CLTRA RELABLE<br>WIRELESS DACOMUL<br>TOTO IN OTHER<br>M-QUADRO<br>ENERAL SETTINOS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>erwork control.<br>Advanced tools<br>DVANCED SETTINOS<br>advanced radio settings<br>static routes   | <section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>  |  |  |
| LITRA RELABLE<br>WIRELESS BLACHAUL<br>VIENERSS BLACHAUL<br>OTOD IW<br>MAQUADRO<br>ENERAL SETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>antenna alignment and stats<br>advanced tools<br>advanced tradio settings<br>advanced radio settings<br>static routes<br>alowsiat / blockilst   | Cisco URWB IW9167EH Configurator     Catalantian and a second and                                      |  |  |
| ULTRA RELABLE<br>WIRELESS BLACHAUL<br>ULTRA RELABLE<br>WIRELESS BLACHAUL<br>OTOD IV<br>M-QUADRO<br>ENERAL SETTINGS<br>eneral mode<br>wireless radio<br>antenna alignment and stats<br>general mode<br>wireless radio<br>antenna alignment and stats<br>advanced radio settings<br>static routes<br>allowits / blocklist<br>multicest  | <section-header>     Critical Current Design France Schwarz S</section-header> |  |  |
| LUTRA RELABLE<br>WRELESS BLACHAUL<br>WRELESS BLACHAUL<br>OTOD IW<br>MAQUADRO<br>EXTRACTION<br>Senteral mode<br>wireloss radio<br>antenna alignment and stats<br>antenna alignment and stats<br>satenna fallo settings<br>static routes<br>advanced radio settings<br>static routes<br>antenna is the settings   | Cisco URWB INPIGETION Configuration     Catalantian     Catalantian     Catalantian     Catalantian     Configuration     Configurati                                      |  |  |
| LUTRA RELABLE<br>WIRELESS BLACHAUL<br>UITRA RELABLE<br>WIRELESS BLACHAUL<br>OTOD IW<br>CHAULESS BLACHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULESS BLACHAULESS<br>CHAULESS BLACHAULESS<br>CHAULESS BLACHAULESS<br>CHAULESS CHAULESS<br>CHAULESS BLACHAULESS<br>CHAULESS BLACHAULESS<br>CHAULESS CHAULESS<br>CHAULESS CHAULESS<br>CHAULE   | <section-header></section-header>  |  |  |
| LITAR RELABLE<br>WIRELESS DEACHAUL<br>WIRELESS DEACHAUL<br>OTOD IW OTHER<br>MAQUADRO<br>DENERAL SETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>antenna alignment and stats<br>satemvork controc.<br>advanced todis settings<br>static routes<br>static routes<br>static routes<br>satempointed and settings<br>static routes<br>multicast<br>somp<br>radius   | <section-header></section-header>  |  |  |
| LUTRA RELABLE<br>WIRELESS BLACHAUL<br>UITRA RELABLE<br>WIRELESS BLACHAUL<br>OTOD IW<br>M-QUADRO<br>SENERAL SETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>advanced tools<br>GUINANCEO SETTINGS<br>advanced tools<br>dater outes<br>advanced radio settings<br>static routes<br>alivnist / blocklist<br>multicast<br>simp<br>radius<br>rtp<br>I2p configuration  | <section-header></section-header>  |  |  |
| LITTA RELABLE<br>WRELESS DEACHAUL<br>WRELESS DEACHAUL<br>COULTA RELABLE<br>WRELESS DEACHAUL<br>COULTA RELABLE<br>COULTA RELABLE<br>C  | <section-header></section-header>  |  |  |
| LUTTAR RELABLE<br>WIRELESS DEACHAUL<br>WIRELESS DEACHAUL<br>OTOD IW<br>MAQUADRO<br>SENERAL SETTINOS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>antenna alignment and stats<br>advanced tools<br>covAnceD setTINOS<br>advanced radio settings<br>static routes<br>advanced radio settings<br>static routes<br>aliowistr./ blocklist<br>multicast<br>simp<br>radius<br>ntp<br>Li2p configuration<br>Vian settings  | <section-header></section-header>  |  |  |
| LUTRA RELABLE<br>WIRELESS BRACHAUL<br>UITRA RELABLE<br>WIRELESS BRACHAUL<br>OTOD IW<br>M-QUADRO<br>SEVERAL SETTINGS<br>Sepenral mode<br>wireless radio<br>antenna alignment and stats<br>advanced tools<br>downoced settings<br>static routes<br>advanced radio settings  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LITAR RELABLE<br>WIRELESS DEACHAUL<br>WIRELESS DEACHAUL<br>COLLESS DEACHAUL<br>COLLESS DEACHAUL<br>MURELESS DEACHAUL  | <section-header></section-header>  |  |  |
| LUTRAR RELABLE<br>WIRELESS BLACHAUL<br>UITRAR RELABLE<br>WIRELESS BLACHAUL<br>OTOD IW<br>MAQUADRO<br>ENERAL SETTINGS<br>General mode<br>wireless radio<br>antenna alignment and stats<br>advanced tools<br>wonACED SETTINGS<br>advanced radio settings<br>static routes<br>alowist / blocklist<br>multicast<br>silowist / blocklist<br>multicast<br>silowist / blocklist<br>multicast<br>silowist / blocklist<br>multicast<br>silowist / blocklist<br>multicast<br>silowist / blocklist<br>multicast<br>simp<br>radius<br>simp<br>radius<br>simp<br>signa filoses<br>smart license<br>MAAGGEMENT SETTINGS   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LUTAN RELABLE<br>WIRELESS BLACHAUL<br>UITAN RELABLE<br>WIRELESS BLACHAUL<br>OTO IW<br>MACUADRO<br>SENERAL SETTINGS<br>Segental mode<br>Wireless radio<br>antenna alignment and stats<br>advanced tools<br>advanced tools<br>advanced tools<br>advanced tools settings<br>static routes<br>advanced tools oettings<br>static routes<br>advanced tools oettings   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| UITRA RELABLE<br>WIRELESS DACIMUL<br>UITRA RELABLE<br>WIRELESS DACIMUL<br>OUTRA RELABLE<br>MURELESS DACIMUL  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LUTRA RELABLE<br>WIRELESS BRACHAUL<br>UITRA RELABLE<br>WIRELESS BRACHAUL<br>OTOD IW O'MIN<br>M-QUADRO<br>SENERAL SETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>advanced tools<br>datenned to   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LITAR RELABLE<br>WIRELESS DEACHAUL<br>UNITAR RELABLE<br>WIRELESS DEACHAUL<br>OTOD IW CITINE<br>MALOUADOO<br>SANTON CONTROL<br>Advanced tools<br>UNITAR ETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>general mode<br>wireless radio<br>advanced tools<br>UNITAR CONTROL<br>advanced tools<br>static routes<br>advanced tools settings<br>static routes<br>samp<br>radius<br>sinto<br>too<br>too figuration<br>vian settings<br>smart licenes<br>Fluidity<br>mice settings<br>smart licenes<br>status<br>configuration settings  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LUTRA RELABLE<br>WIRELESS DACAMAUL<br>UITRA RELABLE<br>WIRELESS DACAMAU<br>OUTRA RELABLE<br>WIRELESS DACAMAU<br>STATUS<br>MINISTRATION<br>CONTON<br>MINISTRATION<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>CONTON<br>C | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |
| LITAR RELABLE<br>WIRELESS DEACHAUL<br>UNITAR RELABLE<br>WIRELESS DEACHAUL<br>OTOD IW CITINE<br>MALOUADOO<br>SANTON CONTROL<br>Advanced tools<br>UNITAR ETTINGS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>general mode<br>wireless radio<br>advanced tools<br>UNITAR CONTROL<br>advanced tools<br>static routes<br>advanced tools settings<br>static routes<br>samp<br>radius<br>sinto<br>too<br>too figuration<br>vian settings<br>smart licenes<br>Fluidity<br>mice settings<br>smart licenes<br>status<br>configuration settings  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |  |  |

l



### **IoT Operations Dashboard Cluster**

- Overview, on page 43
- Configure IoT Operations Dashboard Cluster from CLI, on page 43
- Verify IoT Operations Dashboard Cluster, on page 44

### **Overview**

#### IoT Operations Dashboard Cluster

Cisco IoT Operations Dashboard for Industrial Wireless is a cloud-based IoT services platform designed to monitor and manage IoT devices and networks. For more information about the Industrial Wireless and IoT Operations Dashboard, see Introduction to Industrial Wireless.

#### IoT Operations Dashboard Cluster Before Release 17.15.1

Earlier than Cisco UIW Release 17.15.1, selecting the IoT Operations Dashboard cluster for access was not an option. The default setting was auto, which redirected users to either the US or EU cluster based on the geolocation. For example, devices in the United States are redirected to the US cluster and devices outside the United States are redirected to the EU cluster.

#### IoT Operations Dashboard Cluster in Release 17.15.1

From Cisco UIW Release 17.15.1, you can configure the IoT Operations Dashboard cluster URL to Auto, EU, or US options.

### **Configure IoT Operations Dashboard Cluster from CLI**

Procedure

To configure the IoT Operations Dashboard cluster in an AP, run the following command:

Device#configure iotod-iw cluster { auto | us | eu }

Note

By default, the auto option is enabled.

After you configure the AP with the required cluster, use the following URL to access the IoT Operations Dashboard.

- For auto use: device.ciscoiot.com
- For the US, use: us.ciscoiot.com
- For the EU, use: eu.ciscoiot.com

### **Verify IoT Operations Dashboard Cluster**

To verify the IoT Operations Dashboard cluster configuration, run the following command:

Device#**show iotod-iw cluster configuration** IoT Operations Dashboard **EU Cluster** 



## **Configuring Radio Antenna Settings**

- Configuring Radio Antenna Settings, on page 45
- Validate URWB Individual Antenna RSSI Values, on page 46

### **Configuring Radio Antenna Settings**

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

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

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

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

### **Configuring Antenna Gain**

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

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

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



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

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

### **Configuring Transmit and Receive Antennas**

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

```
Note
```

Catalyst IW9165 does not support abcd-antenna mode.

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

### **Configuring Transmission Power**

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

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



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

```
Device# configure dotl1radio <interface> txpower-level <level>
txpower level:
<1-8> tx power level value
WORD AUTO
Device# write
```

### Validate URWB Individual Antenna RSSI Values

Cisco UIW Release 17.15.1 introduces the URWB Individual Antenna Received Signal Strength Indicator (RSSI) for the Catalyst IW9167E, IW9165E, and IW9165D access points. This feature allows you to view the RSSI value measured for each antenna separately. Multiple RSSI values enable you to monitor the signal strength received separately by each antenna on their radio interface.

For example, with the Catalyst IW9167E's four antennas per radio, you can now check the RSSI for each of the four antennas individually. This detailed information is valuable for troubleshooting and helps identify possible issues with individual antennas or cables. By examining the RSSI for each radio chain, you can determine if a specific antenna is malfunctioning or if its performance varies compared to the others.

| Table | 4: Radio | Chain to A | Antenna | Port I | Mapping |
|-------|----------|------------|---------|--------|---------|
|-------|----------|------------|---------|--------|---------|

| Access Point | Radio Interface | Radio Chain | Antenna Port |
|--------------|-----------------|-------------|--------------|
| IW9167EH     | 1               | [A,B,C,D]   | [4, 3, 2, 1] |
|              | 2               | [A,B,C,D]   | [5,6,7,8]    |

| Access Point | Radio Interface | Radio Chain | Antenna Port |
|--------------|-----------------|-------------|--------------|
| IW9165E      | 1               | [A,B]       | [1,2]        |
|              | 2               | [A,B]       | [3,4]        |
| IW9165D      | 2               | [A,B]       | [1,3]        |

#### Procedure

To validate the RSSI of individual antenna on an AP, use the following command:

Device#**show dot11Radio** <**n**> **wifistats rssi** 

Replace <n> with the appropriate radio number

#### **Example:**

```
Device#show dot11Radio 1 wifistats rssi
FC:58:9A:15:E4:D2
            MeshID 5.21.201.204 via R1
            rssi [-70, -69, -70, -71]
FC:58:9A:15:B9:12
            MeshID 5.21.200.80 via R1
            rssi [-70, -69, -70, -71]
```

l



### **Configuring Wired Interface**

- Enabling and Disabling Wired Interface, on page 49
- Configuring Maximum Transmission Unit Settings, on page 50

### **Enabling and Disabling Wired Interface**

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

#### Enabling or disabling wired interface using CLI

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

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

Example:

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

#### **Error handling configuration**

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

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

#### Verifying enabling and disabling wired interface using CLI

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

Device# #show wired <0-1> config

Example:

```
Device# show wired 0 config
WIRED0 status: enabled
```

Device# show wired 1 config WIRED1 status: disabled

### **Configuring Maximum Transmission Unit Settings**

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

#### **Configuring MTU setting using CLI**

To change the MTU value for wired interfaces, use the following CLI command:

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

#### Example:

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

#### Verifying MTU setting using CLI

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

Device# show wired mtu

#### Example:

Device# show wired mtu Configured MTU: 1600



# **Enable or Disable SSH and Web UI Access**

- Enable SSH Access, on page 51
- Disable SSH Access, on page 51
- Enable Web UI Access, on page 52
- Disable Web UI Access, on page 52

### **Enable SSH Access**

#### Procedure

**Step 1** To enable access to the SSH, use the following command:

Device# configure ssh enable

**Step 2** To verify whether SSH is enabled, use the following command: Device# show ssh

SSH: enabled

### **Disable SSH Access**

#### Procedure

 Step 1
 To disable access to the SSH, use the following command:

 Device# configure ssh disable

**Step 2** To verify whether SSH is disabled, use the following command:

Device# show ssh SSH: disabled

### **Enable Web UI Access**

#### Procedure

| Step 1 | To enable Web UI access, use the following command:                    |
|--------|--|
|        | Device# configure webui enable   |
| Step 2 | To verify whether web UI access is enabled, use the following command: |
|        | Device# show webui config  |
|        | Web-UI: enabled  |

### **Disable Web UI Access**

#### Procedure

 Step 1
 To disable Web UI access, use the following command:

 Device# configure webui disable

 Step 2
 To verify whether web UI access is disabled, use the following command:

 Device# show webui config

 Web-UI: disabled



## **Configuring and Validating Radio Channel and Bandwidth**

- Configure Operating Channel from CLI, on page 53
- Configure Channel Bandwidth from CLI, on page 54
- Validating Operating Channel and Bandwidth from CLI, on page 54
- Configuring Radio Channel and Bandwidth from GUI, on page 55
- Configuring VLAN Settings, on page 56
- Rules for Packet Management, on page 57
- Configuring Fluidity using GUI, on page 57
- Configuring Fluidity using CLI, on page 61
- Configuring Fluidity Coloring, on page 62

### **Configure Operating Channel from CLI**



Note From Cisco UIW Release 17.15.1, the Cisco Catalyst IW9167E, IW9165D, and IW9165E AP supports 4.9 GHz frequency band in URWB mode for -Q domain (Japan).

When operating at 4.9 GHz frequency band, the device supports only 20 MHz channel bandwidth.

The -Q domain supports 802.11ax rates.

#### Table 5: Supported channels and frequencies for the 4.9 GHz band

| Channel | Frequency (MHz) |
|---------|-----------------|
| 184     | 4920            |
| 188     | 4940            |
| 192     | 4960            |
| 196     | 4980            |

To configure the operating channel, use these commands given here:

#### Procedure

```
Step 1 Configure the wireless device with radio interface number < 1 or 2 >.
    Device# configure dot11Radio <interface>
Step 2 Set the operating channel id.
    Device# configure dot11Radio [1|2] channel <1 to 256>
Step 3 Returns to privileged EXEC mode.
    Device (configure dot11Radio [1|2] channel <1 to 256>)# end
```

### **Configure Channel Bandwidth from CLI**

- Configure the wireless device with radio interface number <1 or 2>.
   Device# configure dot11Radio <interface>
- **2.** Set channel bandwidth in MHz.
  - Radio 1 supports 20, 40, and 80 MHz bandwidths.
  - Radio 2 supports 20, 40, 80, and 160 MHz bandwidths.

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

**3.** Returns to privileged EXEC mode.

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

### Validating Operating Channel and Bandwidth from CLI

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

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

Example:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
Device# show dot11Radio 2 config
```

Interface : enabled Mode : fluidity Frequency : 5785 MHz Channel : 157 Channel width : 40 MHz

Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.15.1

### **Configuring Radio Channel and Bandwidth from GUI**

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

Following image shows the configuration of Radio channel and bandwidth:

| ULTRA RELIABLE<br>WIRELESS BACKHAUL              |   | URWB IW9167E<br>21.201.88 - MESH F                       |   |
|--|---|--|---|
| IOTOD IW Offline                                 | WIRELESS RADIO                                      |  |   |
| W-MONITOR Disabled                               |   | Wireless Sett  | tings   |
| GENERAL SETTINGS<br>- general mode               |   | meric string or special cha<br>hitespace (e.g. "mysecure | racters excluding '[apex] "[double apex] `[backtick<br>acamnet") that indentifies your network. It MUST b |
| - wireless radio                                 | Shared Passphrase:                                  | CiscoURWB  |   |
| - antenna alignment and stats<br>NETWORK CONTROL | In order to establish a wireless conn<br>frequency. | ection between Cisco UR                                  | WB units, they need to be operating on the same   |
| - advanced tools                                 |   | Radio 1 Setti  | inas  |
| ADVANCED SETTINGS                                |   |  |   |
| - advanced radio settings                        | Role:   | Fixed  |   |
| - static routes                                  | Frequency (MHz):                                    | 5260   |   |
| - allowlist / blocklist                          |   |  |   |
| - snmp   | Channel Width (MHz):                                | 20   |   |
| - radius   |   | Radio 2 Setti  | in se   |
| - ntp  |   | Radio 2 Setti  | ings  |
| - ethernet filter                                | Role:   | Fixed  |   |
| - I2tp configuration                             |   |  |   |
| - vlan settings                                  | Frequency (MHz):                                    | 5180   |   |
| - Fluidity                                       | Channel Width (MHz):                                | 80   |   |
| - misc settings<br>MANAGEMENT SETTINGS           | Channel Widdi (Wriz).                               | 00   |   |
|  |   |  |   |
| - remote access<br>- firmware upgrade            |   | Reset  | Save  |
| - firmware upgrade<br>- status                   |   | ricoct   | Cure  |
| - status<br>- configuration settings             |   |  |   |
| - reset factory default                          |   |  |   |
| - reboot   |   |  |   |
| - logout   |   |  |   |

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

| CISCO.                      | Cisco URWB IW9167EH Configurator                            |
|-----------------------------|---|
| ULTRA RELIABLE              | 5.21.201.88 - MESH POINT MODE                               |
| WIRELESS BACKHAUL           |   |
|                             | 301101. 11 11120030021V                                     |
| OTOD IW Offline             | Operating Mode: Mesh Point<br>Uptime: 4 days, 16:23 (hh:mm) |
|                             | Firmware version: 8.8.1.10                                  |
| W-MONITOR Disabled          |   |
| SENERAL SETTINGS            | DEVICE SETTINGS<br>IP: 10.115.11.118                        |
|                             | Netmask: 255.255.255.0                                      |
| general mode                | MAC address: 40:36:5a:15:c9:58                              |
| wireless radio              | Configured MTU: 1530  |
| antenna alignment and stats | WIRED0<br>Status: up  |
| ETWORK CONTROL              | Speed: 1000 Mb/s  |
| advanced tools              | Duplex: full  |
| ADVANCED SETTINGS           | MTU: 1530   |
|                             | WIRED1<br>Status: down                                      |
| advanced radio settings     | Visitos, uvim   |
| static routes               | WIRELESS SETTINGS   |
| allowlist / blocklist       | Passphrase: CiscoURWB-118                                   |
| snmp                        | Operating region: B   |
| radius                      | Radio 1   |
| ntp                         | Interface: enabled  |
| ethernet filter             | Mode: fixed infrastructure<br>Frequency: 5260 MHz           |
| 12to configuration          | Channel: 52   |
|                             | Channel Width: 20 MHz                                       |
| vlan settings               | Current tx power: 25 dBm                                    |
| Fluidity                    | Current tx power level: 1<br>Antenna gain: not selected     |
| misc settings               | Antenna gain: not selected<br>Antenna number: 2             |
| ANAGEMENT SETTINGS          | Radio Mode: csma/ca   |
| remote access               | Maximum link length: 3 km                                   |
| firmware upgrade            | Radio 2   |
| status                      | Interface: disabled   |
|                             | Mode: fixed infrastructure                                  |
| configuration settings      | Frequency: 5180 MHz<br>Channel: 36                          |
| reset factory default       | Channel: 36<br>Channel Width: 80 MHz                        |
| reboot                      | Current tx power: 19 dBm                                    |
| logout                      | Current tx power level: 1                                   |
|                             | Antenna gain: not selected                                  |
|                             | Antenna number: 2<br>Radio Mode: csma/ca                    |
|                             | Radio Mode: csma/ca<br>Maximum link length: 3 km            |
|                             |   |
|                             | DIAGNOSTIC TOOL   |
|                             |   |

### **Configuring VLAN Settings**

Default VLAN configuration parameters for the access point are:

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

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

#### Procedure

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

The VLAN SETTINGS window appears.

#### **VLAN SETTINGS**

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

| VLAN                  | l Settings |
|-----------------------|------------|
| Enable VLANs:         |            |
| Management VLAN ID: 1 | \$         |
| Native VLAN ID: 1     | \$         |
| Reset                 | Save       |

- **Step 2** Check the **Enable VLANs** checkbox to connect the access point to a VLAN that is part of the local wireless network.
- **Step 3** Enter the management identification number of the VLAN in the **Management VLAN ID** field. For detailed info about vlan settings and packet management, see **Rules for Packet Management**.

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

- Step 4 Enter the native identification number of the VLAN in the Native VLAN ID field.
- Step 5 Click Save.

L

### **Rules for Packet Management**

#### **Traffic Management**

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

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

#### Access port rules management for outgoing packets with an access point in smart mode

| Packets from the access points (for example: IoT OD IW interface) | Packet tagged with MVID   |
|---|---------------------------|
| Signaling traffic   | Packet tagged with MVID   |
| Tagged with valid VID (1–4094), but not with NVID                 | Packet allowed (tagged)   |
| Tagged with null VID (0) or NVID                                  | Packet allowed (untagged) |



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

### **Configuring Fluidity using GUI**

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

- In the GENERAL SETTINGS, click wireless radio. The WIRELESS RADIO window appears.
- 2. Choose Radio mode as Fluidity from the Role drop-down list.

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

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

1. In the ADVACED SETTINGS, click Fluidity.

The FLUIDITY window appears.

- 2. In the Fluidity Settings, choose Unit Role from the drop-down list. Make device role as any one of following mode:
  - Infrastructure
  - Infrastructure (wireless relay)
  - Vehicle



- Note
- Vehicle ID must be unique among all the mobile devices installed on the same vehicle.
- If the device installed on different vehicles must use different Vehicles IDs'.
- 3. Check the Automatic Vehicle ID check box to automatically set Vehicle ID for mobile units.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |
|---|---|
| Offline Offline   | FLUIDITY  |
| EM-QUADRO<br>DENERAL SETTINGS<br>- general mode<br>wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS  | Fluidity Settings<br>The unit can operate in 3 modes: infrastructure, infrastructure (wrieres relay), Vehicle.<br>The unit must be set as infrastructure, infrastructure (wrieres relay), Vehicle.<br>It is connected to a wrier drawork (backboon) which possibly includes other infrastructure nodes. The unit<br>units which is the infrastructure of the set of the set of the set of the model with the<br>infrastructure which is the infrastructure in the set of the set of the set of the writer infrastructure nodes.<br>The unit use the writers are set of the set of |
| advanced radio settings   | Unit Role: Vehicle V  |
| static routes<br>allowlist / blocklist  | Automatic Vehicle ID: Enable  |
| multicast   | Vehicle ID: 1234  |
| snmp<br>radius  | Network Type: Flat  |
| ntp   | The following advanced settings allow to fine-tune the performance of the system depending on the specific  |
| I2tp configuration<br>vlan settings<br>Fluidity<br>misc settings  | environment. Pease do not alter this settings unless you have read her manual first and you how what you are<br>obig  |
| smart license<br>IANAGEMENT SETTINGS<br>remote access   | Reset   |
| firmware upgrade<br>status<br>configuration settings<br>reset factory default<br>reboot   |   |
|   | © 2022 Cisco and/or its atfiliates. All rights reserved.  |
| Ingout  | 0 2022 Cisco and/or its affiliates. All rights reserved.<br>Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |
|   | Cisco URWB IW9167EH Configurator  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings  |
| IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII   | Chicago URWB IN9167EH Configurator     Catago Configuration     Catago Configuration     Catago Configuration     Configuratin     Configuration     Co                 |
| ILITAR RELABLE     WIRELESS BACHAUL      UITRA RELABLE     WIRELESS BACHAUL      Omine     MAQUADRO      ENERAL SETTINGS     general mode     wireless radio     anterna alignment and stats     ENVORK CONTROL     advanced radio settings   | <section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>   |
| ILTRA RELABLE<br>WIRELESS DACOMUL<br>ULTRA RELABLE<br>WIRELESS DACOMUL<br>OTOD IW<br>MAQUADRO<br>EENERAL SETTINOS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>IETWORK CONTROL<br>advanced tools<br>UWANCED SETTINOS<br>advanced radio settings<br>static routes<br>alowiat / blocklist  | <section-header>         Chicco CURVED INPOINTENE Configuration         Cattarana Configuration         Cattarana Configuration         Cattarana Configuration         Configuration</section-header>  |
| UTRA RELABLE      UITRA RELABLE      WIRELESS BACHAUL      UITRA RELABLE      WIRELESS BACHAUL      OTTIN      WIRELSS BACHAUL      OTTIN      EVERAL SETTINGS      general mode      wireless radio     antenna alignment and stats     EITWORK CONTROL      advanced tools      davanced radio settings     static routes      allowitst / blocklist      multicast   | <section-header>         Chicago URUWB IN99167EH Configurator         Catago 2014         Catago 2014         Chicago URUWB IN9916         Chicago 2014         Chicago 20</section-header>  |
| ILTRA RELABLE     UITRA RELABLE     UITRA RELABLE     WIRELESS BACHAUL  OTOD IW     MAQUADRO  ENERAL SETTINGS     general mode     wireless radio     antenna alignment and stats     EFWORK CONTROL     advanced tools     buvANCED SETTINGS     advanced radio settings     static routes     allowlist / blocklist     multicast     snmp     radius     rip     l2tp configuration     vian settings  | <section-header></section-header>   |
| LITAR RELABLE<br>WRELESS DACOMUL<br>UL TRA RELABLE<br>WRELESS DACOMUL<br>OTOD IW<br>MAQUADRO<br>UENERAL SETTINOS<br>general mode<br>wireless radio<br>antenna alignment and stats<br>sterwork contract<br>advanced tools<br>UWANCED SETTINOS<br>advanced tools<br>UWANCED SETTINOS<br>advanced radio settings<br>static routes<br>allowist / blocklist<br>multicast<br>snmp<br>radius<br>rtip<br>I20 configuration<br>vian settings<br>Fluidity<br>misc settings  | <section-header></section-header>   |
| I I I I I I I I I I I I I I I I I I I   | <section-header></section-header>   |
| LITERA RELABLE<br>WIRELESS BACKHAUL<br>WIRELESS BACKHAUL<br>OTOD IW<br>CM-QUADRO<br>OTOD IW<br>CM-QUADRO<br>OTOD IW<br>CM-QUADRO<br>OTOD IW<br>CM-QUADRO<br>OTOD IW<br>CM-QUADRO<br>SENERAL SETTINGS<br>antenna alignment and stats<br>erwork control.<br>advanced fords<br>antenna alignment and stats<br>setting to the settings<br>advanced fords<br>advanced fords<br>advanced fords<br>advanced fords<br>statis for the settings<br>Fluidity<br>misc settings<br>smart licens<br>Human settings<br>firmare upgrade<br>status<br>configuration settings | <section-header><text><section-header><section-header><section-header><text><text><text><text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL  | <section-header><text><section-header><section-header><section-header><text><text><text><text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |

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

I

| ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE  |
|--|--|
| IOTOD IW Offline   | WIRELESS RADIO   |
| FM-QUADRO  | Wireless Settings  |
|  |  |
| GENERAL SETTINGS   | "Shared Passphrase" is an alphanumeric string or special characters excluding "(apex) "(double apex) '(backtick<br>\$(dollar) =[equal) (backslash) and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST b   |
| - general mode   | the same for all the Cisco URWB units belonging to the same network.   |
| - wireless radio   | Shared Passphrase: PASSWORD  |
| <ul> <li>antenna alignment and stats</li> </ul>  |  |
| NETWORK CONTROL  | In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same<br>frequency.  |
| - advanced tools   | Radio 1 Settings   |
| ADVANCED SETTINGS  | radio rootanga   |
| - advanced radio settings  | Role: Fluidity V   |
| - static routes  |  |
| - allowlist / blocklist  | Frequency (MHz): 5180 V  |
| - multicast  |  |
| - snmp   | Channel Width (MHz): 80 V  |
| - radius   | Radio 2 Settings   |
| - ntp  |  |
| - I2tp configuration   | Role: Disabled V   |
| - vlan settings  |  |
| - Fluidity   |  |
| - misc settings  | Reset Save   |
| - smart license  |  |
| MANAGEMENT SETTINGS  |  |
| - remote access  |  |
| - firmware upgrade   |  |
|  |  |
| - status   |  |
| - configuration settings   |  |
| <ul> <li>reset factory default</li> <li>reboot</li> </ul>  |  |
|  |  |
| - logout   |  |
|  | © 2022 Clisco and/or its atfiliates. All rights reserved.  |
| ULTRA RELIABLE   | © 2022 Clisco and/or its attiliates. All rights reserved.<br>Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE   |
| CISCO.   | Cisco URWB IW9167EH Configurator   |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9167EH Configurator   |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>NOTOD IW OTHine<br>FM-QUADRO   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings   |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL<br>NOTOD IW Offline<br>FM-QUADRO<br>GENERAL SETTINGS   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUIDITY<br>Fluidity Settings   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>IOTOD IW<br>FM-QUADRO<br>GENERAL SETTINGS<br>general mode  | Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE  FLUIDITY  Fluidity Settings The unit can operate in 3 modes: Infrastructure (whereas relay, infrastructure for the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment of the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment of the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment on the and environment of the set of the advector witer interview (bit whereas well). Netwice it is used as a writer and environment on the set of the advector witer interview (bit whereas well). Netwice it is used as a writer and environment of the advector witer interview (bit whereas well). The unit must be set as infrastructure (writer environment).   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>VITRO TO DI W<br>FM-QUADRO<br>GENERALS SETTINGS<br>- general mode<br>- wireless radio  | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE  |
| LISTA RELATE<br>WRELESS BACKHAUL<br>TOTOD IW<br>FM-QUADRO<br>GENERAL SETTINGS<br>- ganeral mode<br>wireless radio<br>- antenna alignment and stats   | Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE  FLUIDITY  Fluidity Settings The unit can operate in 3 modes: Infrastructure (whereas relay, infrastructure for the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment of the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment of the mobile vehicle and it is consected to a writer network (backborn) which possibly includes other infrastructure of whereas welly. Netwice it is used as a writer and environment on the and environment of the set of the advector witer interview (bit whereas well). Netwice it is used as a writer and environment on the set of the advector witer interview (bit whereas well). Netwice it is used as a writer and environment of the advector witer interview (bit whereas well). The unit must be set as infrastructure (writer environment).   |
| ULTAR RELABLE<br>WIRELESS BACKHAUL<br>VICTO IN OMINE<br>FM-QUADRO<br>GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>- antenna statsment  | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUDITY<br>Fullity Setting<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, when it data as the entry point of the infrastructure node. The unit<br>infrastructure with in the operating mode, the unit MUST NOT be concerted to the wired instructions for the model wireless<br>it will use the vehicle when it is mobile. While Dir must be set as Which when the unit is configured as<br>the wind must be set as Which's when it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be used to must be whether.   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>VICTOD IW<br>FM-QUADRO<br>GENERAL SETTINGS<br>- general mode<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUDITY<br>Fullity Setting<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, when it data as the entry point of the infrastructure node. The unit<br>infrastructure with in the operating mode, the unit MUST NOT be concerted to the wired instructions for the model wireless<br>it will use the vehicle when it is mobile. While Dir must be set as Which when the unit is configured as<br>the wind must be set as Which's when it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be used to must be whether.   |
| LUTTA RELABLE<br>WIRELESS BACKHAUL<br>VIRTA SEA CHAUL<br>VIRTA SEA CHAUL<br>VIRTA SEA CHAUL<br>SEA CHAULAR<br>GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>Advanced setTings  | Cisco URWB INVDATE CONTINUES AND   |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>ULTRA RELABLE<br>WIRELESS BACKHAUL<br>FM-QUADRO<br>GENERAL SETTINGS<br>- antenna alignment and stats<br>- wireless radio<br>- antenna alignment and stats<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced taol settings   | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FLUDITY<br>Fullity Setting<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, Infrastructure (wireless relativ), While.<br>The unit must be set as infrastructure, when it data as the entry point of the infrastructure node. The unit<br>infrastructure with in the operating mode, the unit MUST NOT be concerted to the wired instructions for the model wireless<br>it will use the vehicle when it is mobile. While Dir must be set as Which when the unit is configured as<br>the wind must be set as Which's when it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be set as Which's whether it is mobile. Which Dir must be used to must be whether.   |
| LITRA RELABIE<br>WIRELESS BACKHAUL<br>OTOD IW<br>FM-QUADRO<br>CEMERAL SETTINGS<br>- general mode<br>- vireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tods<br>ADVANCED SETTINGS<br>- advanced tods<br>- advanced tods  | <section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>  |
| ULTRA RELABLE<br>WIRELESS BACKHAUL<br>UNTRA RELABLE<br>WIRELESS BACKHAUL<br>UNTRA RELABLE<br>FM-QUADRO<br>GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>- nethen alignment and stats<br>- nethen alignment and stats<br>- advanced tools<br>- advanced tools  | Cisco URWB IW9167EH Configurator<br>5.21.201.72 - MESH END MODE<br>FUDDEY<br>MURICIPAL INFORMATION INFORMATION INFORMATION INFORMATION<br>The standard relative fragment information i |
| ULTRA RELABLE<br>WIRELESS BLACKHAUL<br>ULTRA RELABLE<br>WIRELESS BLACKHAUL<br>COLD IW<br>FM-QUADRO<br>GENERAL SETTINGS<br>- enterias radio<br>- vireless radio<br>- virel  | Cisco URWB IW9167EH Configurator<br>5:12:01:72 - MESH END MODE<br>FULDITS<br>MINING AND  |
| LUTAR RELABLE<br>WIRELESS BACKHAUL<br>UNDERSS BACKHAUL<br>INTO DIW<br>FM-QUADRO<br>OGENERAL SETTINGS<br>- ganeral mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced statio settings<br>- elder outes<br>- elder outes   | <section-header></section-header>  |
| ULTAR RELABLE<br>WIRELESS BACKHAUL<br>UNTAR RELABLE<br>WIRELESS BACKHAUL<br>UNTAR DEVICE<br>UNTAR DEVICE<br>PACHAUSE<br>COMMENDE STAND<br>- advanced tools<br>- advanced tools   | <section-header></section-header>  |
| LITA RELABIE<br>WIRELESS BACKHAUL<br>TOTOD IW<br>MEN-QUADRO<br>COMMENSION<br>SUPPORT<br>MINISTRATE<br>AUXANCED SETTINGS<br>- advanced tool<br>setting coulds<br>- advanced tool<br>setting coulds<br>- advanced tool<br>setting settings<br>- advanced tool<br>setting setting<br>- advanced tool<br>setting<br>- advanced tool<br>setting<br>- advanced tool<br>-  | <section-header></section-header>  |
| LUTRA RELABLE<br>WIRELESS BACOMUL<br>UNTRA RELABLE<br>WIRELESS BACOMUL<br>UNTRA RELABLE<br>MULTRA RELABLE<br>GENERAL SETTINGS<br>-general mode<br>-wireless radio<br>- antenna alignment and stats<br>- antenna figmment and stats<br>- antenna figmment and stats<br>- antenna figmment and stats<br>- advanced tools<br>- advanced radio settings<br>- adva   | <section-header></section-header>  |
| ULTAR RELABLE<br>WIRELESS BRACHAUL<br>ULTAR RELABLE<br>WIRELESS BRACHAUL<br>TOTO IW<br>FM-QUADRO<br>GENERAL SETTINGS<br>- antenna alignment and stats<br>- antenna alignment and stats<br>- antenna alignment and stats<br>- antenna alignment and stats<br>- antenna diools<br>- antenn   | <section-header></section-header>  |
| LUTAR RELABLE<br>WIRELESS BACKHAUL<br>UNTRA RELABLE<br>WIRELESS BACKHAUL<br>OTOD IN<br>MEM-QUADRO<br>OENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>- advanced tools<br>- advanced tools<br>- advanced radio settings<br>- advanced radio settings<br>- atuatic routes<br>- aligneity / blocklist<br>- multicast<br>- simp<br>- radius<br>- itip<br>- 12bp configuration<br>- vian settings  | <section-header></section-header>  |
| ULTAR RELABLE<br>WIRELESS BRACHAUL<br>UUTAR RELABLE<br>WIRELESS BRACHAUL<br>UUTAR RELABLE<br>MILLESS BRACHAUL<br>UUTAR RELABLE<br>MILLESS BRACHAUL<br>OF MALLESS BRACHAUL   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| LITRA RELABRIE<br>WIRELESS BACKMUL<br>INTO IN<br>MALESS BACKMUL<br>OTOD IN<br>MALESS ACCMUL<br>MALESS BACKMUL<br>MALESS BACKMUL<br>MALE  | <section-header></section-header>  |
| LUTRA RELABLE<br>WIRELESS BACKHAUL<br>UNDERS BACKHAUL<br>TOTO IN OTHER<br>FM-QUADRO<br>GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- advanced tools<br>Advanced tools<br>Adv   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| UITAN RELABLE<br>WIRELESS BACAVALU<br>UITAN RELABLE<br>WIRELESS BACAVALU<br>UITAN RELABLE<br>MINISTRATION<br>COMMENDE STINS<br>Segneral mode<br>- sintenna alignment and stats<br>general mode<br>- sintenna alignment and stats<br>- advanced tools<br>- advanced tool  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| LUTA RELABLE<br>WIRELESS BACGHAUL<br>INTO IN<br>MALESS BACGHAUL<br>INTO IN<br>MALESS THOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>- antenna fignment and stats<br>- antenna fignment and stats<br>- antenna fignment and stats<br>- antenna fignment and stats<br>- atvanced to stat<br>- atvanced to stat<br>- statc routes<br>- atvanced to stat<br>- statc routes<br>- static routes<br>- statc ro  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| UITAN RELABLE<br>WIRELESS BACOMUL<br>UITAN RELABLE<br>WIRELESS BACOMUL<br>UITAN RELABLE<br>WIRELESS BACOMUL<br>UITAN RELABLE<br>SUBJECTIONS<br>- COMUL<br>- COMUL | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| LITRARELABUE<br>WIRELESS BACKMAUL<br>INTO INW CMINE<br>FM-QUAORO<br>CEMERAL SETTINGS<br>- general modé<br>- vireless radio<br>- antenna âlgement and stats<br>- general modé<br>- vireless radio<br>- antenna âlgement and stats<br>- advanced todio settings<br>- advanced todio settings<br>- stats routes<br>- singp<br>- Fuidaly<br>- Vain settings<br>- Fuidaly<br>- singt settings<br>- singt less<br>- sin  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| LUTAA RELABLE<br>WIRELESS BACKHAUL<br>UNTRA SEACHAUL<br>TOTO IN OTHER<br>FM-QUADRO<br>OBRERAL SETTINGS<br>- ganeral mode<br>- wireless radio<br>- antenna alignment and stats<br>- advanced tools<br>Advanced tools<br>Advanced radio settings<br>- advanced radio settings<br>- radius<br>- lop<br>102 poonfiguration<br>- Flucitty<br>- Pisce settings<br>- setting settings<br>- radius cocess<br>- remote access<br>- remote access   | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |
| LITRARELABUE<br>WIRELESS BACKMAUL<br>INTO INW CMINE<br>FM-QUAORO<br>CEMERAL SETTINGS<br>- general modé<br>- vireless radio<br>- antenna âlgement and stats<br>- general modé<br>- vireless radio<br>- antenna âlgement and stats<br>- advanced todio settings<br>- advanced todio settings<br>- stats routes<br>- singp<br>- Fuidaly<br>- Vain settings<br>- Fuidaly<br>- singt settings<br>- singt less<br>- sin  | <section-header><text><section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header></text></section-header>   |

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | Cise  | 5.21.201.88 - MESH PC  |  |
|---|---|--|--|
| OTOD IW Offline   | WIRELESS RADIO  |  |  |
| W-MONITOR Disab   | ed  | Wireless Settin  | qs   |
|   | "Shared Passphrase" is an alph  |  |  |
| GENERAL SETTINGS  | \$[dollar] =[equal] \[backslash] ar<br>the same for all the Cisco URW   | d whitespace (e.g. "mysecureca<br>3 units belonging to the same ne   | cters excluding '[apex] "[double apex] '[backtick]<br>imnet") that indentifies your network. It MUST be<br>twork.  |
| - general mode  |   |  |  |
| - wireless radio  | Shared Passphras  | e: CiscoURWB   |  |
| <ul> <li>antenna alignment and st</li> </ul>  | In order to establish a wireless of   | onnection between Cisco URWE   | 3 units, they need to be operating on the same   |
| NETWORK CONTROL   | frequency.  |  |  |
| - advanced tools  |   | Radio 1 Setting  | gs   |
| ADVANCED SETTINGS<br>- advanced radio settings  | Ro  | e: Fixed   | $\sim$   |
| <ul> <li>advanced radio settings</li> <li>static routes</li> </ul>  |   |  |  |
| - allowlist / blocklist   | Frequency (MH:  | z): 5260 V   |  |
| - snmp  |   | 20 ×   |  |
| - radius  | Channel Width (MH   | 20 ~   |  |
| - ntp   |   | Radio 2 Setting  | gs   |
| - ethernet filter   |   | e: Fluidity  | ~  |
| - I2tp configuration  | Ro  | e: Fluidity  | $\checkmark$   |
| - vlan settings   | Frequency (MH   | z); 5500 V   |  |
| - Fluidity  |   |  |  |
| - misc settings   | Channel Width (MH   | z): 80 V   |  |
| MANAGEMENT SETTINGS   |   |  |  |
| - remote access   |   |  |  |
| - firmware upgrade  |   | Reset  | Save   |
| - status  |   |  |  |
| <ul> <li>configuration settings</li> </ul>  |   |  |  |
| <ul> <li>reset factory default</li> </ul>   |   |  |  |
| - reboot  |   |  |  |
| - logout  |   |  |  |
|   | © 2023 Cisco and/or its aff<br>10.115.11.118 says   | lliates. All rights reserved.  |  |
| ahaha<br>cisco.   |   | e with radio configuration   | or   |
| ahahi   | 10.115.11.118 says<br>Error: unit role vehicle is not compatibl   | e with radio configuration<br>dity for role vehicle.   | or   |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | 10.115.11.118 says<br>Error: unit role vehicle is not compatibl   | e with radio configuration   | or   |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | 10.115.11.118 says<br>Error: unit role vehicle is not compatibl   | e with radio configuration<br>dity for role vehicle.   | cor  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL   | 10.115.11.118 says<br>Error: unit role vehicle is not compatibil<br>Both radios must be configured as flui  | e with radio configuration<br>dity for role vehicle.   | cor  |
| LI L  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluir<br>Both radios must be configured as fluir  | e with radio configuration<br>dity for role vehicle.   | cor  |
| ULTRA RELIABLE<br>ULTRA RELIABLE<br>WIRELESS BACKHAUL<br>IOTOD IW<br>IW-MONITOR<br>GENERAL SETTINGS   | 10.115.11.118 says<br>Error: unit role vehicle is not compatibil<br>Both radios must be configured as flui  | e with radio configuration<br>jity for role vehicle.<br>Other section of the section of | cor  |
| CISCO.<br>ULTRA RELIABLE  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY  | e with radio configuration<br>ity for role vehicle.<br>ply these changes? Dis  | card Review Apply  |
| ULTRA RELABLE<br>UNTRESS BACKHUL<br>UNTRESS BACKHUL<br>UNTRESS BACKHUL<br>UNTRO DI W<br>UMMONITOR<br>GENERAL SETTINGS<br>- general mode<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- advanced tools  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY  | e with radio configuration<br>ity for role vehicle.<br>ply these changes? Dis  | card Review Apply  |
| ULTRA RELABLE<br>ULTRA RELABLE<br>WREESS BACKHAUL<br>UNTRO TO THE UNTRA THE<br>UNREESS BACKHAUL<br>UNTRO THE UNTRA THE<br>UNRESS THE UNTRA THE<br>UNTRA THE UNTRA THE UNTRA THE UNTRA THE<br>UNTRA THE UNTRA THE UNTRA THE UNTRA THE UNTRA THE<br>UNTRA THE UNTRA THE U  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY  | e with radio configuration<br>ity for role vehicle.<br>ply these changes? Dis  | card Review Apply  |
| ULTON RELABLE<br>WIRELESS BACKHUL<br>WIRELESS BACKHUL<br>UNTON DIM<br>WHONITOR<br>GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stat<br>network control.<br>- advanced tools<br>Apdwaced tools<br>Apdwaced sols settings  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY  | e with radio configuration<br>ity for role vehicle.<br>ply these changes? Dis  | card Review Apply  |
| ULTRA RELABLE<br>URTELESS BACKAUL<br>URTELESS   | 10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluit Configuration contains changes. Ap FLUIDITY The unit can operate in 3 modes: Infin The unit must be set a Infinite/Configured The unit can operate in 3 modes: Infin The unit can operate in 3 modes: Infin The unit must be set a Infinite/Configured The unit can operate in 3 modes: Infin The unit must be set a Infinite/Configured The unit can operate in 3 modes: Infin The unit must be set a Infinite/Configured The unit can operate in 3 modes: Infin The unit must be set a Infinite/Configured The unit can operate in 3 modes: Infin The unit  | e with radio configuration<br>ity for role vehicle.  | card Review Apply  |
| ULTRA RELADLE<br>ULTRA RELADLE<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>AUTORNON<br>CENERAL SETTINGS<br>- advanced tools<br>Advanced tools<br>Advanced soft SetTings<br>- advanced tools<br>- advanced tools<br>- advanced tools<br>- advanced tools<br>- advanced tools<br>- advanced tools   | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY<br>The unit can centre in 3 modes: Infin   | e with radio configuration<br>ity for role vehicle.  | card Review Apply  |
| ULTRA RELABLE<br>UUTRA RELABLE<br>UUTRA RELABLE<br>UUTRA RELABLE<br>UWAMONITOR<br>DEMEAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna aligament and stat<br>NETWORK CONTROL<br>- advanced tools<br>Advanced radio settings<br>- atlatic routes<br>- alicular statis<br>- alicular statis<br>- alicular statis  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluid<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can persite in 3 modes: Infin<br>The unit can operate in 3 modes: Infin<br>The unit must be set a Infinito-Unit<br>(Separation) and the set as a Infinito-Unit<br>the Infinito-Unit Set as a Infinito-Unit<br>the Infinito-Unit Set as a Infinito-Unit<br>The Unit must be set as Infinito-Unit<br>The Unit Set as Infinito-Unit<br>The Infinito-Unit Set as a Infinito-Unit<br>The Infinito-Unit Set as Infinito | e with radio configuration<br>ity for role vehicle.  | or<br>eard Review Apply<br>why block<br>of the mobile vehicles<br>of the interfactorian codes. The unit<br>interfactorian codes are unit<br>of the interfactorian codes. The unit<br>review of the mobile vehicles<br>of the interfactorian codes. The unit<br>of the interfactorian codes. The unit of the unit<br>of the interfactorian codes. The unit of the unit of the unit<br>of the unit of the unit  |
| ULTRA RELABLE<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>SHORE STITUS<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- advanced ratio settings<br>- atiatic noutes<br>- alowiest blocklist<br>- align status<br>- align status   | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluid<br>Configuration contains changes. Ap<br>FLUIDITY<br>The unit can operate in 3 modes: Infin<br>and the set as infrastructure (onter<br>the base of the set as infrastructure)<br>onter and the set as infrastructure<br>onter and the set as infrastructure on the<br>the base of the set as infrastructure on the<br>set as infrastructure on the<br>set as infrastructure on the<br>set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infrastructure on the set as infrastructure on the<br>set as infrastructure on the set as infras  | e with radio configuration<br>sity for role vehicle.   | or<br>eard Review Apply<br>why block<br>of the mobile vehicles<br>of the interfactorian codes. The unit<br>interfactorian codes are unit<br>of the interfactorian codes. The unit<br>review of the mobile vehicles<br>of the interfactorian codes. The unit<br>of the interfactorian codes. The unit of the unit<br>of the interfactorian codes. The unit of the unit of the unit<br>of the unit of the unit  |
| ULTRA RELADLE<br>UNTRELESS BACKAUL<br>UNTRELESS BACKAUL<br>UNTRELESS BACKAUL<br>IDTOD IW<br>WWMONITO<br>OBNERAL SETTINOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- advanced todis settings<br>- static routes<br>- advanced radio settings  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluid<br>Configuration contains changes: Ap<br>FLUIDITY<br>The unit can openet in 3 modes: Info<br>FLUIDITY<br>The unit can openet in 3 modes: Info<br>September 2005<br>The second of the second of the second<br>of the second of the second of the second of the second<br>of the second of the second of the second of the second<br>of the second of the second of the second of the second<br>of the second of the second of the second of the second<br>of the second of the second of the second of the second of the second<br>of the second of t  | e with radio configuration<br>dity for role vehicle.   | error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>error<br>er |
| ULTAN RELABLE<br>WIRELESS BACOMUL<br>UNTAN RELABLE<br>WIRELESS BACOMUL<br>UNTAN RELABLE<br>WIRELESS BACOMUL<br>UNTAN RELABLE<br>WIRELESS BACOMUL<br>OUTDO IW<br>OUTDO   | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluid<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can operate in 3 modes: Infin<br>The unit can operat  | e with radio configuration<br>sity for role vehicle.   | Apply where the standard stand   |
| ULTRA RELADLE<br>UUTRA RELADLE<br>UUTRA RELADLE<br>UUTRA RELADLE<br>UUTRA STATA<br>INVAMONITO<br>CENERAL SETINOS<br>- general mode<br>- wireless radio<br>- antenna aligament and stat<br>NETWORK CONTROL<br>- advanced tools<br>Advanced tools<br>- advanced tools<br>- adva   | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can operate in 3 modes: Infin<br>The unit can operate  | e with radio configuration<br>sity for role vehicle.   | Apply where the standard stand   |
| LUTTA RELABLE<br>WIRELESS BACGIOUU<br>ULTA RELABLE<br>WIRELESS BACGIOUU<br>ULTA RELABLE<br>WIRELESS BACGIOUU<br>OTOD IW<br>ULTA RELABLE<br>SACGIOUU<br>OTOD IW<br>OTOD IW<br>OT | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can operate in 3 modes: Infin<br>The unit can operate  | e with radio configuration<br>sity for role vehicle.   | Apply where the standard stand   |
| ULTRA RELABLE<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>UNTREESS BACKHUL<br>SHOWENS CONTROL<br>- antenna alignment and stat<br>sevenees and<br>- avdanced radio settings<br>- atalic noutes<br>- aliowitest / blocklist<br>- anten<br>- radius<br>- htp<br>- ethernet filter<br>- Jitp configuration<br>- vian settings  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can operate in 3 modes: Infin<br>The unit must be set in Infin and the unit can<br>be set in Infin and the unit of the unit of the unit<br>the behavior, Type Infin<br>Configuration Configured to the unit of the unit<br>the behavior, Type Infin<br>Configured to the unit of the unit of the unit of the unit<br>the behavior of the unit of the   | e with radio configuration<br>dity for role vehicle.   | Apply where the standard stand   |
| ULTRA RELADLE<br>UNTRELESS BACKHUL<br>UNTRELESS BACKHU   | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as fluid<br>Configuration contains changes: Ap<br>FLUIDITY<br>The unit can openet in 3 modes: Info<br>FLUIDITY<br>The unit can openet in 3 modes: Info<br>September 2005<br>The second of the second of the second<br>openet of the second of the second of the second<br>openet of the second of the second of the second<br>openet of the second of the second of the second<br>openet of the second of the second of the second<br>openet of the second of the second of the second<br>openet of the second of the second of the second of the second<br>openet of the second of t  | e with radio configuration<br>dity for role vehicle.   | Apply where the standard stand   |
| ULTRA RELADLE<br>UUTRA RELADLE<br>UUTRA RELADLE<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>URELESS BACHAUL<br>INFORMATION<br>Second<br>URELASS BACHAUL<br>SUMMONITOR<br>CENERAL SETTINGS<br>- advanced radio settings<br>- advanced radi  | 10.115.11.118 says<br>Error: unit role vehicle is not compatible<br>Both radios must be configured as flui<br>Configuration contains changes. Ap<br>FLUIDITY<br>Hund can operate in 3 modes: Infin<br>The unit must be set in Infin and the unit can<br>be set in Infin and the unit of the unit of the unit<br>the behavior, Type Infin<br>Configuration Configured to the unit of the unit<br>the behavior, Type Infin<br>Configured to the unit of the unit of the unit of the unit<br>the behavior of the unit of the   | e with radio configuration<br>dity for role vehicle.   | Apply where the standard stand   |
| ULTON RELABLE<br>WIRELESS DACHAUL<br>ULTON RELABLE<br>WIRELESS DACHAUL<br>UNITON DIM<br>DEMEMAL SETTINGS<br>- general mode<br>- vireless radio<br>- antenna alignment and stat<br>NerWORK CONTROS<br>- advanced tools<br>- advance  | 10.115.11.118 says<br>Torr: unit role vehicle is not compatibility<br>both radios must be configured as fluid<br><b>Configuration contains changes: AP</b><br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br>to set as offendation and the set as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit met and set as a fluid as a   | e with radio configuration<br>dity for role vehicle.   | or<br>exercise Apply and a second secon   |
| ULTRA RELABLE<br>UURTRA RELABLE<br>UURTRA RELABLE<br>UURTRA SELABLE<br>UURTRA SETINOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>Advanced radio settings<br>- static routes<br>- route access<br>- firmware upgrade<br>- statis<br>- configuration settings   | 10.115.11.118 says<br>Torr: unit role vehicle is not compatibility<br>both radios must be configured as fluid<br><b>Configuration contains changes: AP</b><br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br>to set as offendation and the set as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit met and set as a fluid as a   | e with radio configuration<br>dity for role vehicle.   | Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr   |
| ULTAN RELABLE<br>WIRELESS BACGIOUX<br>WIRELESS BACGIOUX<br>ULTAN RELABLE<br>WIRELESS BACGIOUX<br>OTOD IW<br>WHONITOR<br>CENERAL SETTINGS<br>- general mode<br>- vireless radio<br>- antenna alignment and stat<br>NEWTORK CONTRO STATUS<br>- advanced tools<br>- advanced   | 10.115.11.118 says<br>Torr: unit role vehicle is not compatibility<br>both radios must be configured as fluid<br><b>Configuration contains changes: AP</b><br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br>to set as offendation and the set as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit met and set as a fluid as a   | e with radio configuration<br>dity for role vehicle.   | Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr   |
| ULTRA RELABLE<br>UURTRA RELABLE<br>UURTRA RELABLE<br>UURTRA SELABLE<br>UURTRA SETINOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>NETWORK CONTROL<br>- antenna alignment and stat<br>Advanced radio settings<br>- static routes<br>- route access<br>- firmware upgrade<br>- statis<br>- configuration settings   | 10.115.11.118 says<br>Torr: unit role vehicle is not compatibility<br>both radios must be configured as fluid<br><b>Configuration contains changes: AP</b><br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit and set as a fluid as a fluid as a fluid<br>to set as offendation and the set as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid<br>to set as a fluid as a fluid as a fluid as a fluid as a fluid<br><b>FLUDITY</b><br>The unit met and set as a fluid as a   | e with radio configuration<br>dity for role vehicle.   | Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr<br>Cr   |

### **Configuring Fluidity using CLI**

To enable Fluidity, use the following CLI commands:



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

Device# configure dot11Radio <interface> mode fluidity

Example to enable Fluidity for radio 1:

configure dot11Radio 1 mode fluidity

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

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

### **Configuring Fluidity Role using CLI**

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

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

Device# configure fluidity id

2. Configure Fluidity id mode.

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

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

Device (configure fluidity id {mode}) # end

Device# wr

Example:

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

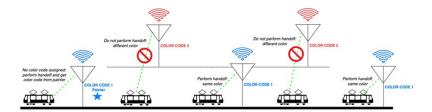
### **Configuring Fluidity Coloring**

Fluidity Coloring is introduced from UIW Release 17.12.1. It enables wayside or outside devices (Fluidity infrastructure devices) to be given specific color codes to enhance or drive the handoff process, and with the standard configuration handoff decision is made based on received signal strength indication (RSSI).

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

#### **Fluidity Coloring Logic**

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



The process of Fluidity coloring as follows:

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

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

#### Table 6: Fluidity Coloring Role

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

### **Configuring Fluidity Coloring using CLI**

To configure a Fluidity color mode, use the following CLI commands:

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

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

#### Example (painter):

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

#### Example (non-painter):

Device# configure fluidity color mode enabled Device# configure fluidity color value "3 4 5" Device# write Devie# reload

#### Example (clear):

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

#### Verifying Fluidity Coloring using CLI

To verify a Fluidity color mode, use the following show commands:

Device# #show fluidity config

Example (painter):

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

## Example (non-painter):

Device# show fluidity config

Color: enabled, current: 3 4 5

### Example (clear):

Device# show fluidity config

Color: enabled, current: 0 ...

#### **Configuring Fluidity Coloring RSSI Threshold**

. . .

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

#### Configuring Fluidity Coloring RSSI Threshold using CLI

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

Example:

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

### Verifying Fluidity Coloring RSSI Threshold using CLI

Device# show fluidity config

### Example:

Device# show fluidity config ...

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

l



# **Configuring and Validating High Efficiency** (802.11 ax)

- Configuring and Validating High Efficiency, on page 67
- Configuring Global Gateway from GUI, on page 68

# **Configuring and Validating High Efficiency**

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

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

To enable HE mode, use the following CLI command:

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

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

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



Note The default maxmcs is Nine.

To disable HE mode, use the following CLI command:

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

To validate HE mode, use the following show command:

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

```
Device# show dotllRadio 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 the MPLS Layer 3. In this mode, Radio-off and Radio status cannot be changed.

1. In the GENERAL SETTINGS, click general mode.

The GENERAL MODE window appears.

2. Click gateway from Mode.

Following images shows the GUI configuration of global gateway mode:

| ULTRA RELIABLE<br>WIRELESS BACKHAUL | Cisco URWB IW916<br>5.21.201.72 - ME  |  |
|-------------------------------------|---|--|
| Offline Offline                     | GENERAL MODE  |  |
| FM-QUADRO                           | General   | Mode   |
| GENERAL SETTINGS                    | Global Gateway mode automatically enforces MPLS layer<br>Global Gateway mode. | r 3 and radio-off. Radio status cannot be changed in |
| - general mode                      |   | O mesh point   |
| - wireless radio                    | Mode:   |  |
| - antenna alignment and stats       |   | • gateway  |
| NETWORK CONTROL                     |   | gatoway  |
| - advanced tools                    |   | -  |
| ADVANCED SETTINGS                   | Radio-off:  | Fluidity V   |
| advanced radio settings             |   |  |
| static routes                       | LAN Para  | ameters  |
| - allowlist / blocklist             |   |  |
| multicast                           | Local IP:   | 10.115.11.117  |
| snmp                                | Least Nationalu   | 255.255.255.0  |
| radius                              | Eocal Neuriask.   | 233.233.233.0  |
| - ntp                               | Default Gateway:  | 10.115.11.1  |
| · I2tp configuration                | • • • • • • • • • • • • •   |  |
| vlan settings                       | Local Dns 1:  | 8.8.8.8  |
| Fluidity                            |   |  |
| misc settings                       | Local Dns 2:  |  |
| smart license                       |   |  |
| MANAGEMENT SETTINGS                 |   |  |
| remote access                       | Reset   | Save   |
| firmware upgrade                    |   |  |
| status                              |   |  |
| configuration settings              |   |  |
| reset factory default               |   |  |
| reboot                              |   |  |
| logout                              |   |  |

#### WIRELESS RADIO

#### Wireless Settings

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

Shared Passphrase: CiscoURWB

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

|       | Radio 1 S | Settings     |  |
|-------|-----------|--------------|--|
| Role: | Disabled  | $\checkmark$ |  |
|       | Radio 2 S | Settings     |  |
| Role: | Disabled  | $\sim$       |  |
|       | Reset     | Save         |  |

#### FLUIDITY

#### Fluidity Settings

Thuidity 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 gent to other
Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as
it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle HD must be a unique among all the mobile units installed on the same vehicle. Unit
installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set ascirling layer-2 broadcast domain. Use Multiple Subnets if they are
organized as different layer-3 routing domains.

| Unit Role: | Infrastructure | $\sim$ |
|------------|----------------|--------|
|            |                |        |

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

environment. Prese so not and this social so the second social so

Handoff Logic: Standard V

| Reset | Save |
|-------|------|



# **Configuring Guard Interval for HE (High Efficiency)**

• Configuring Guard Interval for HE (High Efficiency), on page 71

# **Configuring Guard Interval for HE (High Efficiency)**

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

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

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

gi - Guard interval values are:

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

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

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

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

Example:

Device# configure dot11Radio 1 high-efficiency enable Device# configure dot11Radio 1 guard-interval 1600 Device# configure dot11Radio 1 guard-interval 3200 Device# wr

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

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

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



# **Configuring and Validating SNMP**

• Configuring and Validating SNMP, on page 73

# **Configuring and Validating SNMP**

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

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

### Figure 1: SNMP Process



# **Configuring SNMP from CLI**

To configure SNMP, use the following CLI commands:



Note

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

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

Device#configure snmp [enable | disable]

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

Device#configure snmp version {v2c | v3}

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

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

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

Device#configure snmp v3 username <length 32>

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

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

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

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

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

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

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

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

Device#configure snmp secret <length 8-64>

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

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

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

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

Notification value trap period measured in minutes.

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

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

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

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

To disable SNMP configuration, use the following CLI command:

Device#configure snmp disabled

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

Example of SNMP configuration:

CLI for SNMP v2:

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

#### CLI for SNMP v3:

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

# Validating SNMP from CLI

To validate the SNMP, use the following show command:

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

# Configuring SNMP Version v2c using GUI

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

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

### Procedure

Step 1Choose the version v2c from the SNMP mode drop-down list.<br/>The SNMP window appears.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL            | Cisco URWB IW91<br>5.21.200.136 - MI                    |               |
|--|---|---------------|
| IOTOD IW Offline                               | SNMP  |               |
| IW-MONITOR Disabled                            | SN  | MP            |
| FM-QUADRO                                      | SNMP mode:  | v2c ×         |
|  | SIMIP HIDLE.  | VZC V         |
| GENERAL SETTINGS - general mode                | Community ID:   | test          |
| - general mode                                 | Enable SNMP periodic trap:                              |               |
| - antenna alignment and stats                  | Enable SNMP event trap:                                 |               |
| NETWORK CONTROL                                |   |               |
| - advanced tools                               | NMS hostname:   | 192.168.0.100 |
| ADVANCED SETTINGS<br>- advanced radio settings | Notification period (minutes):                          | 1 0           |
| - static routes                                |   |               |
| - allowlist / blocklist                        |   |               |
| - multicast                                    | Reset   | Save          |
| - snmp   |   |               |
| - radius                                       |   |               |
| - ntp  |   |               |
| - ethernet filter                              |   |               |
| - I2tp configuration                           |   |               |
| - vlan settings<br>- Fluidity                  |   |               |
| - misc settings                                |   |               |
| - smart license                                |   |               |
| MANAGEMENT SETTINGS                            |   |               |
| - remote access                                |   |               |
| - firmware upgrade                             |   |               |
| - status                                       |   |               |
| - configuration settings                       |   |               |
| - reset factory default                        |   |               |
| - reboot                                       |   |               |
| - logout                                       |   |               |
|  | © 2023 Cisco and/or its affiliates. All rights reserved | d.            |

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

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

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

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

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

Step 5 Click Save.

# **Configuring SNMP Version v3 using GUI**

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

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

## Procedure

Step 1Choose the version v3 from the SNMP mode drop-down list.<br/>The SNMP window appears.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL | Cisco URWB IW9167EH<br>5.21.200.136 - MESH EP |                       |
|-------------------------------------|---|-----------------------|
| TOD IW Offline                      | SNMP  |                       |
| -MONITOR Disabled                   | SNMP  |                       |
| M-QUADRO                            | SNMP mode:                                    | v3 ~                  |
| ENERAL SETTINGS                     |   |                       |
| eneral mode                         | SNMP v3 username:                             | user                  |
| wireless radio                      | SNMP v3 password:                             |                       |
| intenna alignment and stats         | · · · · · · · · · · · · · · · · · · ·         |                       |
| TWORK CONTROL                       | Show SNMP v3 password:                        |                       |
| advanced tools                      | SNMP v3 authentication proto:                 | SHA 🗸                 |
| VANCED SETTINGS                     |   |                       |
| dvanced radio settings              | SNMP v3 encryption:                           | AES 🗸                 |
| tatic routes                        | SNMP v3 encryption passphrase:                | *****                 |
| illowlist / blocklist<br>nulticast  |   |                       |
| nmp                                 | Show SNMP v3 encryption passphrase:           |                       |
| adius                               | Enable SNMP periodic trap:                    | <ul><li>✓</li></ul>   |
| tp                                  | Enable SNMP event trap:                       | <ul><li>✓</li></ul>   |
| hernet filter                       | Engine ID:                                    | Currently Unavailable |
| 2tp configuration                   |   | ·                     |
| an settings                         | NMS hostname:                                 | 192.168.0.100         |
| luidity                             | Notification period (minutes):                | 1                     |
| lisc settings                       | Houncation period (minutes).                  |                       |
| mart license                        |   |                       |
| NAGEMENT SETTINGS                   | Reset   | Save                  |
| rmware upgrade                      |   |                       |
| atus                                |   |                       |
| enfiguration settings               |   |                       |
| set factory default                 |   |                       |
| boot                                |   |                       |
| ogout                               |   |                       |

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

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

- **Step 3** To change the current SNMP v3 password, enter the new password in the **SNMP v3 password** field.
- **Step 4** Choose the authentication type from the **SNMP v3 authentication proto** drop-down list. The available options are:
  - MD5
  - SHA

Important

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

- **Step 5** Choose the appropriate encryption protocol from the **SNMP v3 encryption** drop-down list. The available options are:
  - No Encryption
  - **DES** (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

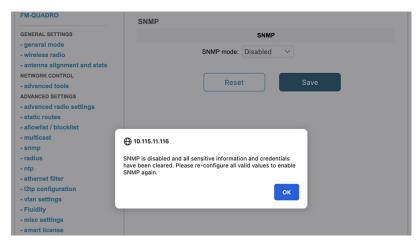
**Note** The same encryption protocol must be set for all the access points in the network.

- **Step 6** To change the encryption passphrase, enter a new passphrase in the **SNMP v3 encryption passphrase** field.
- **Step 7** Check the **Enable SNMP periodic trap** check box to enable the periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.
- **Step 8** Check the **Enable SNMP event trap** check box to enable the SNMP event traps for significant system-related events and then enter the host name of NMS in the **NMS hostname** field.

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

# Step 9 Click Save.

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





# **Configuring and Validating Key Controller** (Wireless Security)

• Configuring and Validating Key Controller (Wireless Security), on page 79

# **Configuring and Validating Key Controller (Wireless Security)**

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

# **Configuring Key Controller from CLI**

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

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

Device# configure dot11Radio <interface> crypto aes enable

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

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

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

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

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

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



Note

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

# Validating Key Controller from CLI

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

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



# **FIPS Certification**

- FIPS Certification, on page 81
- Enable or Disable FIPS Mode using CLI, on page 81
- Verify FIPS Mode using CLI, on page 81

# **FIPS Certification**

The Federal Information Processing Standard (FIPS) mode ensures that the SSH and GUI functionalities are in compliance with FIPS140-3 security standards from NIST. When FIPS is enabled, the AP ensures that the configuration is compliant with FIPS requirements.



Note FIPS certification does not support SNMP.

# **Enable or Disable FIPS Mode using CLI**

## Procedure

- Step 1 Device#configure fips {enable|disable}
- Step 2 Device#write
- Step 3 Device#reload

# **Verify FIPS Mode using CLI**

Use this command to verify FIPS mode on the AP.

Device#show fips FIPS: enabled

l



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

- Configuring and Verifying Country Code using CLI, on page 83
- Configuring Country Code using GUI, on page 84
- Supporting Fixed Domains and Country Codes (ROW), on page 87

# **Configuring and Verifying Country Code using CLI**

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

Device# configure countrycode [countrycode]

Example:

Configure countrycode GB

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



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

To verify status of country code, use the following show command:

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

To verify status of ROW country code, use the following show command:

Device# show dot11Radio <interface> config

Example:

......

Device# show dot11Radio 1 config

DFS region : GB DFS radar role : auto Radar Detected : 0 Indoor deployment: disable

# **Configuring Country Code using GUI**

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

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL |   | URWB IW9167EH Con<br>21.200.136 - MESH END MC                | 0  |
|-------------------------------------|---|--|--|
| IOTOD IW Cloud-Manage               | Select operating country  |  |  |
| FM-QUADRO                           |   |  |  |
| GENERAL SETTINGS                    | Please select ROW region operating<br>immediately rebooted on confirmation<br>be applied. | country. The device will be<br>on and all saved changes will | g '[apex] "[double apex] `[backtick]<br>dentifies your network. It MUST be |
| - wireless radio                    | ✓ Korea   |  |  |
| - antenna alignment and stats       | United Arab Emirates  |  |  |
| NETWORK CONTROL                     | United Kingdom  |  | ~  |
| - advanced tools                    | Vietnam   | Confirm  | eed to be operating on the same  |
| ADVANCED SETTINGS                   | vietnam   |  | sed to be operating on the same  |
| - advanced radio settings           |   | Radio 1 Settings   |  |
| - static routes                     | Polo  | Fluidmax Primary V   |  |
| - allowlist / blocklist             | Role.   |  |  |
| - multicast                         | Frequency (MHz):  | $\sim$   |  |
| - snmp                              |   |  |  |
| - radius                            | Channel Width (MHz):  | $\checkmark$   |  |
| - ntp                               |   | Radio 2 Settings   |  |
| - I2tp configuration                |   |  |  |
| - vlan settings                     | Role:   | Disabled V   |  |
| - Fluidity                          |   |  |  |
| - misc settings                     | Frequency (MHz):  | Y  |  |
| - smart license                     | Channel Width (MHz):  | $\sim$   |  |
| MANAGEMENT SETTINGS                 | , ,   |  |  |
| - remote access                     |   |  |  |
| - status<br>- reboot                |   |  |  |
| - logout                            |   |  |  |
| - logour                            |   |  |  |
|                                     | © 2023 Cisco and/or its affiliate   | es. All rights reserved.                                     |  |

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

A confirmation pop-up appears.

4. Click Confirm.

A reboot confirmation screen appears.

- 5. Click Yes.
- 6. In the MANAGEMENT SETTINGS, click status.

In the STATUS page, check the details of operating region and country for confirmation.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL | Cisco URWB IW9167EH Configurator<br>5.246.1.104 - MESH POINT MODE |
|-------------------------------------|---|
| OTOD IW Offline                     | STATUS  |
| W-MONITOR Disabled                  | Device: Cisco Catalyst IW9167E Heavy Duty Access Point            |
| SENERAL SETTINGS                    | Name: unset<br>ID: 5.246.1.104                                    |
|                                     | Serial: KWC2702000L   |
| general mode                        | Operating Mode: Mesh Point  |
| wireless radio                      | Uptime: 2 min   |
| antenna alignment and stats         | Firmware version: 8.8.1.10  |
| NETWORK CONTROL                     | DEVICE SETTINGS   |
| advanced tools                      | IP: 10.115.11.142   |
| ADVANCED SETTINGS                   | Netmask: 255.255.255.0<br>MAC address: 40:36:5a:f6:01:68          |
| advanced radio settings             | Configured MTU: 1530  |
| static routes                       | WIRED0  |
| allowlist / blocklist               | Status: up<br>Speed: 100 Mb/s                                     |
|                                     | Duplex: full  |
| snmp                                | MTU: 1530   |
| radius                              | WIRED1  |
| ntp                                 | Status: down  |
| ethernet filter                     | WIRELESS SETTINGS   |
| 12tp configuration                  | Passphrase: CiscoURWB-142   |
| vlan settings                       | Operating region: ROW<br>Country: GB                              |
| Fluidity                            | Country: GB   |
| misc settings                       | Radio 1   |
| MANAGEMENT SETTINGS                 | Interface: enabled  |
| remote access                       | Mode: fixed infrastructure<br>Frequency: 5500 MHz                 |
|                                     | Channel: 100  |
| firmware upgrade                    | Channel Width: 80 MHz   |
| status                              | Current tx power: -96 dBm<br>Current tx power level: 1            |
| configuration settings              | Antenna gain: not selected  |
| reset factory default               | Antenna number: 2   |
| reboot                              | Radio Mode: csma/ca<br>Maximum link length: 3 km                  |
| logout                              | Maximum link lengul. 5 km   |
|                                     | Radio 2   |
|                                     | Interface: disabled<br>Mode: fixed infrastructure                 |
|                                     | Mode: fixed infrastructure<br>Frequency: 5500 MHz                 |
|                                     | Channel: 100  |
|                                     | Channel Width: 80 MHz   |

7. To establish a wireless connection between devices, set the same operating frequency in radio devices.

Note

Shared Passphrase must be same for all the devices belonging to the same network.

| ULTRA RELIABLE<br>WIRELESS BACKHAUL              |   | URWB IW9167EH Configurator<br>21.201.88 - MESH POINT MODE   |
|--|---|---|
| IOTOD IW Offline                                 | WIRELESS RADIO  |   |
| W-MONITOR Disabled                               |   | Wireless Settings   |
| GENERAL SETTINGS<br>- general mode               | "Shared Passphrase" is an alphanu<br>\$[dollar] =[equal] \[backslash] and w<br>the same for all the Cisco URWB ur | meric string or special chara-cters excluding "[apex] "[double apex] '[backtick]<br>hitespace (e.g., "mysecurecamnet") that indentifies your network. It MUST be<br>lits belonging to the same network. |
| - wireless radio                                 | Shared Passphrase:  | CiscoURWB   |
| - antenna alignment and stats<br>NETWORK CONTROL | In order to establish a wireless conr<br>frequency.   | nection between Cisco URWB units, they need to be operating on the same   |
| - advanced tools                                 |   | Radio 1 Settings  |
| ADVANCED SETTINGS                                | Role:   | Fixed   |
| advanced radio settings                          | 100.  |   |
| static routes                                    | Frequency (MHz):  | 5260  |
| allowlist / blocklist                            |   |   |
| snmp<br>radius                                   | Channel Width (MHz):  | 20  |
| ntp  |   | Radio 2 Settings  |
| ethernet filter                                  |   | Et a d  |
| 12tp configuration                               | Role:   | Fixed   |
| vlan settings                                    | Frequency (MHz):  | 5180  |
| Fluidity   |   |   |
| misc settings                                    | Channel Width (MHz):  | 80  |
| ANAGEMENT SETTINGS                               |   |   |
| remote access                                    |   |   |
| firmware upgrade                                 |   | Reset Save  |
| status   |   |   |
| configuration settings                           |   |   |
| reset factory default                            |   |   |
| reboot   |   |   |
| logout   |   |   |

Following image shows the configuration of country code using GUI:

| CISCO   | Cisco URWB IW9167EH Configurator                         |
|---|--|
| ULTRA RELIABLE                                  | 5.21.201.88 - MESH POINT MODE                            |
| WIRELESS BACKHAUL                               |  |
|   | JEHAI. ** ! !*20030021\                                  |
| _   | Operating Mode: Mesh Point                               |
| IOTOD IW Offline                                | Uptime: 4 days, 16:23 (hh:mm)                            |
| W-MONITOR Disabled                              | Firmware version: 8.8.1.10                               |
|   | DEVICE SETTINGS  |
| GENERAL SETTINGS                                | IP: 10.115.11.118  |
| - general mode                                  | Netmask: 255.255.255.0<br>MAC address: 40:36:5a:15:c9:58 |
| - wireless radio                                | Configured MTU: 1530                                     |
|   | WIREDO   |
| <ul> <li>antenna alignment and stats</li> </ul> | Status: up   |
| NETWORK CONTROL                                 | Speed: 1000 Mb/s<br>Duplex: full                         |
| <ul> <li>advanced tools</li> </ul>              | MTU: 1530  |
| ADVANCED SETTINGS                               | WIRED1   |
| - advanced radio settings                       | Status: down   |
| - static routes                                 | WIRELESS SETTINGS  |
| - allowlist / blocklist                         | Passphrase: CiscoURWB-118                                |
| - snmp  | Operating region: B                                      |
| - radius  | Radio 1  |
| - ntp   | Interface: enabled                                       |
|   | Mode: fixed infrastructure                               |
| - ethernet filter                               | Frequency: 5260 MHz<br>Channel: 52                       |
| - I2tp configuration                            | Channel Width: 20 MHz                                    |
| - vlan settings                                 | Current tx power: 25 dBm                                 |
| - Fluidity                                      | Current tx power level: 1                                |
| - misc settings                                 | Antenna gain: not selected<br>Antenna number: 2          |
| MANAGEMENT SETTINGS                             | Radio Mode: csma/ca                                      |
| - remote access                                 | Maximum link length: 3 km                                |
| - firmware upgrade                              | Radio 2  |
| - status  | Interface: disabled                                      |
|   | Mode: fixed infrastructure                               |
| - configuration settings                        | Frequency: 5180 MHz<br>Channel: 36                       |
| - reset factory default                         | Channel: 36<br>Channel Width: 80 MHz                     |
| - reboot  | Current tx power: 19 dBm                                 |
| - logout  | Current tx power level: 1                                |
|   | Antenna gain: not selected<br>Antenna number: 2          |
|   | Antenna number: 2<br>Radio Mode: csma/ca                 |
|   | Maximum link length: 3 km                                |
|   | DIAGNOSTIC TOOL  |
|   | DIAGNOSTIC TOOL  |
|   | 1  |

# **Supporting Fixed Domains and Country Codes (ROW)**

The ROW reg domain simplifies the domain management of the manufacturing process for all the country codes that do not have a specific domain mapped. The fixed domain and country code support for the Catalysts IW9167E, IW9165E, and IW9165D access points are described in this section.

You are responsible for ensuring APs approval for use in your country. To verify approval and to identify the regulatory domain associated with a particular country. For more information, see Cisco Product Approval Status.

# **Catalyst IW9167E Supported Fixed Domains**

| Domain | Indoor Deployment Support |
|--------|---------------------------|
| А      | No                        |
| В      | N/A                       |
| Е      | Yes                       |
| F      | No                        |
| Q      | No                        |
| Ζ      | No                        |

Note

Outdoor and indoor frequencies are same for the B domain.

# Catalyst IW9167E Supported Country Codes (ROW)

| Domain ROW Country Code | Indoor Deployment Support | Support Version |
|-------------------------|---------------------------|-----------------|
| VN (Vietnam)            | N/A                       | 17.11.1         |
| GB (Great Britain)      | Yes                       | 17.11.1         |
| KR (Korea)              | No                        | 17.12.1         |
| IN (India)              | No                        | 17.12.1         |
| PE (Peru)               | No                        | 17.12.1         |
| PH (Philippines)        | No                        | 17.12.1         |
| ZA (South Africa)       | No                        | 17.13.1         |
| AR (Argentina)          | No                        | 17.13.1         |
| HK (Hong Kong)          | No                        | 17.13.1         |

| Domain ROW Country Code        | Indoor Deployment Support | Support Version |
|--------------------------------|---------------------------|-----------------|
| PK (Pakistan)                  | No                        | 17.13.1         |
| UY (Uruguay)                   | No                        | 17.13.1         |
| CO (Colombia)                  | No                        | 17.13.1         |
| BR (Brazil)                    | No                        | 17.13.1         |
| CN (China)                     | No                        | 17.13.1         |
| EC (Ecuador)                   | No                        | 17.13.1         |
| IQ (Iraq)                      | No                        | 17.13.1         |
| SG (Singapore)                 | No                        | 17.13.1         |
| SA (Saudi Arabia)              | No                        | 17.13.1         |
| QA (Qatar)                     | No                        | 17.13.1         |
| MX (Mexico)                    | No                        | 17.13.1         |
| TH (Thailand)                  | No                        | 17.13.1         |
| CL (Chile)                     | No                        | 17.13.1         |
| TW (Taiwan, Republic of China) | No                        | 17.13.1         |
| AE (United Arab Emirates)      | No                        | 17.13.1         |
| EG (Egypt)                     | No                        | 17.15.1         |
| MY (Malaysia)                  | No                        | 17.15.1         |
| MN (Mongolia)                  | No                        | 17.15.1         |



Note You can select only the listed country codes using CLI or GUI.

For ROW domain, select the country code for the device to work.

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

# **Catalyst IW9165E Supported Fixed Domains**

| Domain | Indoor Deployment Support |
|--------|---------------------------|
| А      | Yes                       |
| В      | N/A                       |
| Е      | Yes                       |

| Domain | Indoor Deployment Support |  |
|--------|---------------------------|--|
| Z      | Yes                       |  |
| Q      | Yes                       |  |
| F      | Yes                       |  |



Outdoor and indoor frequencies are same for B domain.

# Catalyst IW9165E Supported Country Codes (ROW)

| Domain ROW Country Code        | Indoor Deployment Support | Support Version |
|--------------------------------|---------------------------|-----------------|
| GB (Great Britain)             | Yes                       | 17.12.1         |
| ZA (South Africa)              | Yes                       | 17.13.1         |
| IN (India)                     | Yes                       | 17.13.1         |
| KR (Korea)                     | Yes                       | 17.13.1         |
| PE (Peru)                      | Yes                       | 17.13.1         |
| AE (UAE)                       | Yes                       | 17.13.1         |
| MX (Mexico)                    | Yes                       | 17.13.1         |
| BR (Brazil)                    | Yes                       | 17.13.1         |
| CL (Chile)                     | Yes                       | 17.13.1         |
| SA (Saudi Arabia)              | Yes                       | 17.13.1         |
| PH (Philippines)               | Yes                       | 17.13.1         |
| QA (Qatar)                     | Yes                       | 17.13.1         |
| SG (Singapore)                 | Yes                       | 17.13.1         |
| LK (Sri Lanka)                 | Yes                       | 17.13.1         |
| TH (Thailand)                  | Yes                       | 17.13.1         |
| VN (Vietnam)                   | Yes                       | 17.13.1         |
| TW (Taiwan, Republic of China) | Yes                       | 17.14.1         |
| EG (Egypt)                     | Yes                       | 17.15.1         |
| MY (Malaysia)                  | Yes                       | 17.15.1         |

| Domain ROW Country Code | Indoor Deployment Support | Support Version |
|-------------------------|---------------------------|-----------------|
| AR (Argentina)          | Yes                       | 17.15.1         |
| CN (China)              | Yes                       | 17.15.1         |
| CO (Colombia)           | Yes                       | 17.15.1         |
| EC (Ecuador)            | Yes                       | 17.15.1         |
| HK (Hong Kong)          | Yes                       | 17.15.1         |

Note You can select only the listed country codes using CLI or GUI.

For ROW domain, select the country code for the device to work.

OM (Oman) supports -E domain.

# **Catalyst IW9165D Supported Fixed Domains**

| Domain | Indoor Deployment Support |
|--------|---------------------------|
| А      | No                        |
| В      | N/A                       |
| Е      | Yes                       |
| Z      | No                        |
| Q      | No                        |
| F      | No                        |

Ŵ

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

# **Catalyst IW9165DH Supported Country Codes (ROW)**

| Domain ROW Country Code | Indoor Deployment Support | Support Version |
|-------------------------|---------------------------|-----------------|
| GB (Great Britain)      | Yes                       | 17.12.1         |
| ZA (South Africa)       | No                        | 17.13.1         |
| IN (India)              | No                        | 17.13.1         |
| KR (Korea)              | No                        | 17.13.1         |

| Domain ROW Country Code        | Indoor Deployment Support | Support Version |
|--------------------------------|---------------------------|-----------------|
| PE (Peru)                      | No                        | 17.13.1         |
| AE (UAE)                       | No                        | 17.13.1         |
| MX (Mexico)                    | No                        | 17.13.1         |
| BR (Brazil)                    | No                        | 17.13.1         |
| CL (Chile)                     | No                        | 17.13.1         |
| SA (Saudi Arabia)              | No                        | 17.13.1         |
| PH (Philippines)               | No                        | 17.13.1         |
| QA (Qatar)                     | No                        | 17.13.1         |
| SG (Singapore)                 | No                        | 17.13.1         |
| LK (Sri Lanka)                 | No                        | 17.13.1         |
| TH (Thailand)                  | No                        | 17.13.1         |
| VN (Vietnam)                   | No                        | 17.13.1         |
| TW (Taiwan, Republic of China) | No                        | 17.14.1         |
| EG (Egypt)                     | No                        | 17.15.1         |
| MY (Malaysia)                  | No                        | 17.15.1         |
| AR (Argentina)                 | No                        | 17.15.1         |
| CN (China)                     | No                        | 17.15.1         |
| CO (Colombia)                  | No                        | 17.15.1         |
| EC (Ecuador)                   | No                        | 17.15.1         |
| HK (Hong Kong)                 | No                        | 17.15.1         |

Note

8

You can select only the listed country codes using CLI or GUI.

For ROW domain, select the country code for the device to work.

OM (Oman) supports -E domain.

I



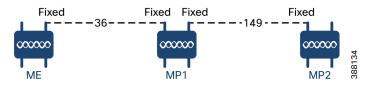
# **Configuring and Validating of Point-to-Point Relay Topology**

- Configuring and Validating of Point-to-Point Relay Topology, on page 93
- Configuring Point to Point Relay Topology from CLI, on page 93
- Validating Point to Point Relay Topology from CLI, on page 94

# Configuring and Validating of Point-to-Point Relay Topology

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

Figure 2: point to point relay topology



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

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

# **Configuring Point to Point Relay Topology from CLI**

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

- 1. Configure the wireless device with radio interface number <1 or 2>. Device# configure dot11Radio <interface>
- 2. Set wireless interface admin state to enable or disable mode.

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

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

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

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

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

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

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

#### Example:

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

Example for point-to-point relay topology configuration:

#### Mesh End (ME) Configuration

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

### Mesh Point (MP1) Configuration

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

#### MP2 Configuration

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

# Validating Point to Point Relay Topology from CLI

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

Device# show dot11Radio <interface> config

#### Mesh End (ME) Statistics

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

.....

### Mesh Point (MP1) Statistics

Device# show dotl1Radio 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

I

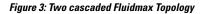


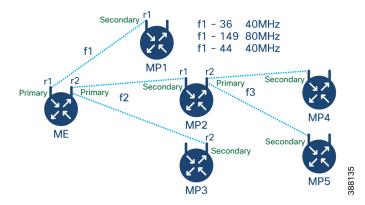
# **Configure and Validate Fluidmax Topology**

· Configure and Validate Fluidmax (point to multipoint) Topology, on page 97

# **Configure and Validate Fluidmax (point to multipoint) Topology**

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





# **Configure Point to Multipoint Topology from CLI**

Use these commands to configure a Fluidmax (point-to-multipoint) topology.

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 device, 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, and 160.

Device#wr

Example of point to multipoint (Fluidmax) topology configuration:

#### ME (Mesh End) Configuration

Device#configure dotl1Radio 1 enable Device#configure dotl1Radio 1 mode fluidmax primary Device#configure dotl1Radio 1 channel 36 Device#configure dotl1Radio 1 band-width 40 Device#configure dotl1Radio 2 enable Device#configure dotl1Radio 2 mode fluidmax primary Device#configure dotl1Radio 2 channel 149 Device#configure dotl1Radio 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 dotl1Radio 1 enable Device#configure dotl1Radio 1 mode fluidmax secondary Device#configure dotl1Radio 1 channel 149 Device#configure dotl1Radio 1 band-width 80 Device#configure dotl1Radio 2 enable Device#configure dotl1Radio 2 mode fluidmax primary Device#configure dotl1Radio 2 channel 44 Device#configure dot11Radio 2 band-width 40

#### MP3 Configuration

Device#configure dotllRadio 1 enable Device#configure dotllRadio 1 mode fluidmax secondary Device#configure dotllRadio 1 channel 149 Device#configure dotllRadio 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 dotllRadio 1 enable
Device#configure dotllRadio 1 mode fluidmax secondary
Device#configure dotllRadio 1 channel 44
Device#configure dotllRadio 1 band-width 40
```

Cluster ID: This is an ID assigned to an interface when it is set in Fluidmax mode. This ID should be the same for primary and backup primary nodes. It helps in identifying and grouping devices that belong to the same cluster.

Tower ID: This is used to enable or disable the Fluidmax Tower ID for a specified interface.

**Note** Tower ID is used in configurations where there is a Gateway + Mesh Point (MP) – MP with the same tower ID.

Use these commands to configure the interface, cluster id, and tower id in Fluidmax mode.

```
Fluidmax - Set the interface in Fluidmax mode.
Primary | Secondary - Fluidmax role for the device, 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.
```

### Validate Point to Multipoint Topology using CLI

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

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

Example:

#### ME (Mesh End) radio2

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

#### MP2 (Mesh Point)

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

I

Fluidmax Configuration Tower ID : 100 Cluster ID : fluidmesh Automatic scan : enabled Automatic scan threshold : disabled

#### MP4 radio1

Device# show dotl1Radio 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



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

- Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology, on page 101
- Configuring Mixed Mode Topology from CLI, on page 101

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

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

#### Figure 4: Mixed Mode Topologies



# **Configuring Mixed Mode Topology from CLI**

To configure a mixed mode topology, use the following CLI command: Device# configure fluidity id {vehicle-auto | vehicle ID | infrastructure | wireless- relay} Fluidity id – Configure Fluidity role for the device Vehicle-auto - Vehicle mode with automatic vehicle ID selection Vehicle ID (alphanumeric) - Vehicle mode with manual ID Infrastructure - Configure Infrastructure mode for the device Wireless-relay - Wireless infrastructure with no ethernet connection to the backhaul

Device# configure dot11Radio <interface>

Interface - <0-3> dot11Radio interface number

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

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

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

#### U3 Configuration

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

### Validating Mixed Mode Topology from CLI

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

Device# show dot11Radio <interface>config

U1 Statistics:

```
Device# show dotl1Radio 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 dotllRadio 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

l



# **Configure and Validate Fast Failover**

- Overview of Fast Failover, on page 105
- Configure and Validate Fast Failover, on page 105
- Configure Fast Failover from CLI, on page 106
- Validate Fast Failover from CLI, on page 106

# **Overview of Fast Failover**

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

Fast Failover mechanism:

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



Note Fast Failover is included in all the Network Licenses

# **Configure and Validate Fast Failover**



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

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

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

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



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

### **Configure Fast Failover from CLI**

Use this command to configure fast failover.

Device# configure modeconfig mode meshpoint

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

Device# configure mpls fastfail status [enable | disable]

Mpls - Configure mpls data frame packets for specified device.

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

Device# configure mpls fastfail timeout <0 - 65535>

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

Use this command to set the preempt delay.

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

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



Note

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

### Validate Fast Failover from CLI

Use this command to validate fast failover.

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

#### Example:

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

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

I



# **Configuring Indoor Deployment**

• Configuring Indoor Deployment, on page 109

# **Configuring Indoor Deployment**

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



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

By default, the devices are set to outdoor mode.

To enable indoor deployment, use the following CLI command:

Device# configure wireless indoor-deployment enable

To disable indoor deployment, use the following CLI command:

Device# configure wireless indoor-deployment disable

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

#### For enabled indoor deployment

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

#### For disabled indoor deployment

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

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



# **Configuring Layer 2 Mesh Transparency**

- Configuring Layer 2 Mesh Transparency, on page 111
- Configuring and Verifying Layer-2 Protocols Forwarding Using CLI, on page 112
- Configuring Layer-2 Protocol Forwarding using GUI, on page 114

# **Configuring Layer 2 Mesh Transparency**

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

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

#### Table 7: List of reserved ether-types

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

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

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

# Configuring and Verifying Layer-2 Protocols Forwarding Using CLI

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

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

#### Example:

```
Device# configure mpls ether-filter allow-list add 0x86DD
Device# write
Device# reload
Device# show mpls config
...
Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
...
```

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

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

#### Example:

```
Device# configure mpls ether-filter allow-list delete 0x86DD
Device# write
Device# reload
Device# show mpls config
...
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
```

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

Device# configure mpls ether-filter allow-list clear

#### Example:

. . .

```
Device# show mpls config
...
Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
...
Device# configure mpls ether-filter allow-list clear
Device# write
Device# write
Device# reload
Device# show mpls config
...
Ethernet Filter allow-list: none, ethernet-I block
...
```

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

Device# configure mpls ether-filter allow-list add all Example: Device# configure mpls ether-filter allow-list add all Device# write Device# reload Device# show mpls config ... Ethernet Filter allow-list: all, ethernet-I block

```
Note
```

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

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

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

Example:

```
Device# show mpls ether-filter

Ether-type Direction Description

0x8899 INGRESS ---

0x86DD INGRESS IPv6

Device# configure mpls ether-filter table clear

Cisco-81.160.136#show mpls ether-filter

Ether-type Direction Description

0x8899 INGRESS ---
```



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

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

```
Device# configure mpls ether-filter ethernet-I forward
Example:
Device# configure mpls ether-filter ethernet-I forward
         Device# write
         Device# reload
Deive# show mpls config
        . . .
        Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I forward
        . . .
Device# configure mpls ether-filter ethernet-I block
Example:
Device# configure mpls ether-filter ethernet-I block
         Device#write
         Device# reboot
         Device# show mpls config
         . . .
```

Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I block

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

```
Device# show mpls config

Example:

Device# show mpls config

...

Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block

...
```

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

```
Device# show mpls ether-filter table

Example:

Device# show mpls ether-filter table

Ether-type Direction Description

0x8899 INGRESS ----

0x86DD INGRESS IPv6
```

### **Configuring Layer-2 Protocol Forwarding using GUI**

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

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

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL  |                               | Cis  | co URWB IW9165E Co<br>5.81.160.244 - MESH END  |                                |  |
|--|-------------------------------|--|--|--------------------------------|--|
| IOTOD IW Offline   | Ethernet F                    | ilter  |  |                                |  |
| IW-MONITOR Disabled  |                               |  | Detected ethernet types  |                                |  |
| FM-QUADRO  | To add a detec                | ted ethertype to the :   | allowlist click on Add.  |                                |  |
|  | Ethertype                     | Description  |  | Action                         |  |
| GENERAL SETTINGS   |                               |  |  |                                |  |
| - wireless radio   | 0×8899                        |  | INGRESS  | Add                            |  |
| - antenna alignment and stats  | 0x86DD                        | IPv6   | INGRESS  | Add                            |  |
| NETWORK CONTROL  |                               |  |  |                                |  |
| - advanced tools<br>ADVANCED SETTINGS  |                               |  | Clear detected   |                                |  |
| - advanced radio settings  |                               |  | Clear delected   |                                |  |
| - static routes  |                               |  |  |                                |  |
| <ul> <li>allowlist / blocklist</li> <li>multicast</li> </ul>   |                               |  | II ethernet types  |                                |  |
| - snmp   |                               | Allow Ethe   | ernet 1 protocols  |                                |  |
| - radius   |                               |  |  |                                |  |
| - ntp  |                               |  | Allowed ethernet types   |                                |  |
| - ethernet filter<br>- I2tp configuration  | To add a speci                | ic ethertype to the al   | lowlist, insert it in the text field and cl  |                                |  |
| - vlan settings  | Ethertype                     |  | Description  | Action                         |  |
| - Fluidity   | 0x8892                        |  | PROFINET   | Delete                         |  |
| - misc settings  |                               |  |  |                                |  |
| - smart license<br>MANAGEMENT SETTINGS   | 0×8204                        |  | QNX Qnet   | Delete                         |  |
| - remote access  |                               |  |  | Add                            |  |
| - firmware upgrade   |                               |  |  |                                |  |
| - status<br>- configuration settings   |                               |  | Clear allowed  |                                |  |
| - reset factory default  |                               |  | Clear allowed  |                                |  |
| - reboot   |                               |  |  |                                |  |
| - logout   |                               |  | Save   |                                |  |
|  |                               |  |  |                                |  |
|  | © 202                         | 3 Cisco and/or its affi  | iliates. All rights reserved.  |                                |  |
| սիսիս  |                               |  |  |                                |  |
| ULTRA RELIABLE<br>WIRELESS BACKHAUL  |                               | Cisco UR<br>5.81.10  | WB IW9165E Configurato<br>60.244 - MESH END MODE   | r                              |  |
| IOTOD IW Offline   | Ethernet Filte                | er   |  |                                |  |
| IW-MONITOR Disabled  |                               |  |  |                                |  |
|  |                               | D  | etected ethernet types   |                                |  |
| FM-QUADRO  | To add a detected e           | D<br>thertype to the allowist  |  |                                |  |
| FM-QUADRO  | To add a detected o           |  |  | Action                         |  |
| GENERAL SETTINGS - general mode  |                               | thertype to the allowlist  | t click on Add.  | Action Add                     |  |
| GENERAL SETTINGS   | Ethertype<br>0x8899           | thertype to the allowlist<br>Description   | t click on Add.<br>Direction<br>INGRESS  |                                |  |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL   | Ethertype                     | thertype to the allowlist<br>Description   | t eliek on Add.<br>Direction   | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools   | Ethertype<br>0x8899           | thertype to the allowlist<br>Description   | t click on Add.<br>Direction<br>INGRESS<br>INGRESS   | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings   | Ethertype<br>0x8899           | thertype to the allowlist<br>Description   | t click on Add.<br>Direction<br>INGRESS  | Add                            |  |
| CENERAL SETTINOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINOS<br>- advanced radio settings<br>- static routes  | Ethertype<br>0x8899           | thertype to the allowlist<br>Description<br><br>IPv6   | tolok en Add.<br>Direction<br>INGRESS<br>INGRESS<br>Clear delected   | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings   | Ethertype<br>0x8899           | athertype to the allowist<br>Description<br><br>IPv6<br>Allow all ethe   | telok en Add. Direction INGRESS INGRESS Clear detected emet types  | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>- advanced radio settings<br>- static: routes<br>- allowiist / blocklist<br>- multicast<br>- simp  | Ethertype<br>0x8899           | thertype to the allowlist<br>Description<br><br>IPv6   | telok en Add. Direction INGRESS INGRESS Clear detected emet types  | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- writeless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>Advanced tools<br>- advanced tools<br>- a | Ethertype<br>0x8899           | therype to the allowist<br>Description<br><br>IPv6<br>Allow all ether<br>Allow Ethernet 1  | telok en Add. Direction INGRESS INGRESS Clear detected emet types  | Add                            |  |
| GENERAL SETTINOS<br>- general mode<br>- wireless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced radio settigs<br>- static routes<br>- advanced radio settigs<br>- static routes<br>- anuiticast<br>- multicast<br>- sing<br>- radius<br>- tip<br>- ethemet liter  | Ethertype<br>0x8899<br>0x88DD | therype to the allowlish Description UPV6 Allow all ether Allow Ethernet   | tala en Add. Direction INGRESS INGRESS Clear detected emet types protocols   | Add                            |  |
| GENERAL SETTINOS  - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced tools ADVANCED SETTINOS - advanced tools statu: routes - aliovatist / biocklist - snmp - radius - sntp - radius - statp - clips - filter - clips - configuration  | Ethertype<br>0x8899<br>0x88DD | ethertype to the allowlist Description IPv6 Allow all ethe Allow Ethernet :  | tala on Ads:<br>Direction<br>INGRESS<br>INGRESS<br>Clear detected<br>emet types  <br>1 protocols  <br>Nilowed ethemet types  | Add                            |  |
| GENERAL SETTINGS<br>- general mode<br>- writeless radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>Advancet otols<br>- advancet otols<br>- a | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | telake on Add. Direction INGRESS INGRESS Clear detected  areat types  areat types broket thermet types broket in the test field and diek on Add.                           | Add<br>Add                     |  |
| GENERAL SETTINGS  - general mode - writeless radio - antenna alignment and stats NETWORK CONTROL - advanced tools - advanced radio settings - advanced radio settings - static routes - allowlist / blocklist - multicast - sump - radius - ratu - ethernet filter - ethernet filter - lizbo configuration - vian settings - Fluidity - misc settings - fluidity - misc settings - fluidity - misc settings - setting - settings - setting - set   | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | tala on Add. Direction INGRESS INGRESS Clear detected emet types t protocols t protocols maart is in the suf field and click on Add. Description                           | Add<br>Add<br>Action<br>Delete |  |
| GENERAL SETTINOS  - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced tools ADVANCED SETTINOS - advanced radio settings - static routes - sumpiless - sinupiless - sinupiless - sinup - radius - sinp - ethernet filter - t2ipo configuration - vian settings - Fluidity - Fluidity - sinsat filtense - sinst filtens   | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | tala on Add. Direction INGRESS INGRESS Clear detected emet types t protocols t protocols maart is in the suf field and click on Add. Description                           | Add<br>Add<br>Action           |  |
| GENERAL SETTINOS  - general mode - wireless radio - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced rodos Activances Totols - static routes - aliowist / biocklist - multicast - simp - radius - ntp - title -   | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | telete on Add. Direction INGRESS INGRESS Clear detected arreet types Clear detected Utowed ethemet types Undered the here the field and clear on Add. Description PROFINET | Add<br>Add<br>Action<br>Delete |  |
| GENERAL SETTINOS  - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced tools ADVANCED SETTINOS - advanced radio settings - static routes - sumpiless - sinupiless - sinupiless - sinup - radius - sinp - ethernet filter - t2ipo configuration - vian settings - Fluidity - Fluidity - sinsat filtense - sinst filtens   | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | tala on Add. Direction INGRESS INGRESS Clear detected emet types t protocols t protocols maart is in the suf field and click on Add. Description                           | Add<br>Add<br>Action<br>Delete |  |
| GENERAL SETTINGS<br>- general mode<br>- wrietess radio<br>- antenna alignment and stats<br>NETWORK CONTROL<br>- advanced tools<br>Advancet otols<br>- advancet otols<br>- ad | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | telea en Add.  Direction  INGRESS  Clear detected  armet types  Clear adetected  Allowed athemet types  PROFINET  Clear allowed  | Add<br>Add<br>Action<br>Delete |  |
| GENERAL SETTINOS  - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced rodos Acvancet of colos Acvancet of colos - static routes - multicast - multicast - multicast - ntp - themet filter - i2ip configuration - vian settings - smart license MAMAGKINT SETTINOS - smart license - filtense - smart license - smart lic   | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | telete on Add. Direction INGRESS INGRESS Clear detected arreet types Clear detected Utowed ethemet types Utowed ethemet types Perception Perception                        | Add<br>Add<br>Action<br>Delete |  |
| GENERAL SETTINOS  - general mode - wireless radio - anterna algument and stats NETWORK CONTROL - advanced radio settings - static routes - advanced radio settings - ntil - advanced radio settings - ntil - tibrent filter - lizip configuration - wins cettings - static freess - filtidaty - static settings - status - remote access - filtimare upgrade - status - configuration settings - configuration - cettings - filtidaty - remote access - filtimare upgrade - status - configuration settings - configuration - settings - configuration - cettings - filtidaty - remote access - filtimare upgrade - status - configuration settings - configuration settings - configuration - cettings - cettings - configuration - cettings -  | Ethertype<br>0x8899<br>0x86DD | ethertype to the allowini<br>Description<br><br>IPv6<br>Allow all ethe<br>Allow Ethernet 1<br>Allow 1 | telea en Add.  Direction  INGRESS  Clear detected  armet types  Clear adetected  Allowed athemet types  ProPriNET  Clear allowed   | Add<br>Add<br>Action<br>Delete |  |

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL  | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH END MODE |                          |   |              |
|--|---|--------------------------|---|--------------|
| OTOD IW Offline<br>W-MONITOR Disabled  | Configuration con   | tains changes. App       | ly these changes? Discard                     | Review Apply |
| M-QUADRO   | Ethernet Fi   | Iter                     |   |              |
| ENERAL SETTINGS  |   |                          | Detected ethernet types                       |              |
| general mode   | To add a detecte  | d ethertype to the allow | rlist click on Add.                           |              |
| wireless radio<br>antenna alignment and stats  | Ethertype   | Description              | Direction                                     | Action       |
| TETWORK CONTROL<br>advanced tools  | 0×8899  |                          | INGRESS                                       | Add          |
| DVANCED SETTINGS<br>advanced radio settings<br>static routes<br>allowlist / blocklist<br>multicast | 0x86DD  | IPv6                     | INGRESS<br>Clear detected                     | Add          |
| snmp<br>radius   |   | Allow all e              | thernet types                                 |              |
| ntp<br>ethernet filter   |   | Allow Etherne            | et 1 protocols                                |              |
| I2tp configuration<br>vlan settings  |   |                          | Allowed ethernet types                        |              |
| Fluidity   | To add a specific   | ethertype to the allow   | ist, insert it in the text field and click on | Add.         |
| misc settings<br>smart license   | Ethertype   |                          | Description                                   | Action       |
| IANAGEMENT SETTINGS<br>remote access<br>firmware upgrade   |   |                          |   | Add          |
| status<br>configuration settings<br>reset factory default  |   |                          | Clear allowed                                 |              |
| reboot<br>logout   |   |                          | Save  |              |

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

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

- 2. Click Clear detected in the Detected ethernet types section to clear the detected ethernet types from allowlist.
- 3. Once you click Clear detected, you can see ethernet types cleared in the Detected ethernet types section.

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH END MODE |                             |  |        |
|-------------------------------------|---|-----------------------------|--|--------|
| OTOD IW Offline                     | Ethernet Fil  | ter                         |  |        |
| W-MONITOR Disabled                  |   |                             | Detected ethernet types                        |        |
| M-QUADRO                            | To add a detecte  | d ethertype to the allow    | list click on Add.                             |        |
| ENERAL SETTINGS                     | Ethertype   | Description                 | Direction                                      | Action |
| general mode                        |   |                             |  |        |
| wireless radio                      |   | ſ                           |  |        |
| antenna alignment and stats         |   |                             | Clear detected                                 |        |
| ETWORK CONTROL                      |   |                             |  |        |
| advanced tools                      |   | Allow all et                | hernet types                                   |        |
| DVANCED SETTINGS                    |   |                             |  |        |
| advanced radio settings             |   | Allow Etherne               | t 1 protocols                                  |        |
| static routes                       |   |                             |  |        |
| allowlist / blocklist               |   |                             | Allowed ethernet types                         |        |
| multicast                           | To add a cosoifie   | othertupe to the allowing   | st, insert it in the text field and click on a | lided  |
| snmp                                |   | concrepte to one one of the |  |        |
| radius                              | Ethertype   |                             | Description                                    | Action |
| ntp                                 | 0x8892  |                             | PROFINET                                       | Delete |
| ethernet filter                     |   |                             |  |        |
| 12tp configuration                  | 0x8204  |                             | QNX Qnet                                       | Delete |
| vlan settings                       |   |                             |  |        |
| Fluidity                            |   |                             |  | Add    |
| misc settings                       |   |                             |  |        |
| smart license                       |   | (                           |  |        |
| IANAGEMENT SETTINGS                 |   |                             | Clear allowed                                  |        |
| remote access<br>firmware upgrade   |   |                             |  |        |
| status                              |   |                             |  |        |
| configuration settings              |   |                             | Save   |        |
| reset factory default               |   |                             |  |        |
| reboot                              |   |                             |  |        |
| logout                              |   |                             |  |        |

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

- 2. Check the Allow all ethernet types check box in the Ethernet Filter section to allow all ethernet type to allowlist.
- 3. Click Save and then Apply to change the configuration.

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

| ULTRA RELIABLE<br>WIRELESS BACKHAUL              | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH END MODE |                         |                        |              |
|--|---|-------------------------|------------------------|--------------|
| IOTOD IW Offline<br>IW-MONITOR Disabled          | Configuration contain   | ns changes. Apply these | changes? Discard       | Review Apply |
| FM-QUADRO  |   | Eth                     | ernet Filter           |              |
|  |   | Detecte                 | d ethernet types       |              |
| GENERAL SETTINGS                                 | To add a date   |                         | e allowlist click on A | dd           |
| - general mode                                   | Ethertype   | Description             | Direction              | Action       |
| - wireless radio                                 | Enertype  | Description             | Direction              | Action       |
| - antenna alignment and stats<br>NETWORK CONTROL | 0x8899  |                         | INGRESS                | Add          |
| - advanced tools                                 | 0x86DD  | IPv6                    | INGRESS                | Add          |
| ADVANCED SETTINGS                                |   |                         |                        |              |
| - advanced radio settings                        |   |                         |                        |              |
| - static routes                                  |   | C                       | lear detected          |              |
| - allowlist / blocklist                          |   |                         |                        |              |
| - multicast                                      |   |                         |                        |              |
| - snmp   |   | Al                      | low all ethernet typ   | es 🗹         |
| - radius   |   | Allow                   | Ethernet 1 protoco     | ls 🗆         |
| - ntp  |   |                         |                        |              |
| - ethernet filter                                |   |                         |                        |              |
| - I2tp configuration                             |   |                         | Save                   |              |
| - vlan settings                                  |   |                         |                        |              |
| - Fluidity                                       |   |                         |                        |              |
| - misc settings                                  |   |                         |                        |              |
| - smart license                                  |   |                         |                        |              |
| MANAGEMENT SETTINGS                              |   |                         |                        |              |
| - remote access                                  |   |                         |                        |              |
| - firmware upgrade                               |   |                         |                        |              |
| - status   |   |                         |                        |              |
| - configuration settings                         |   |                         |                        |              |
| - reset factory default                          |   |                         |                        |              |
| - reboot   |   |                         |                        |              |
| - logout   |   |                         |                        |              |

To configure an ethernet 1 protocol, follow these steps:

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

- 2. Check the Allow Ethernet 1 protocols check box in the Ethernet Filter section to enable ethernet 1 protocol mode.
- 3. Click Save and then Apply to change the configuration.

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

I

| ULTRA RELIABLE<br>WIRELESS BACKHAUL                                | Cisco URWB IW9165E Configurator<br>5.81.160 244 - MESH END MODE |                          |  |        |
|--|---|--------------------------|--|--------|
| OTOD IW Offline  | Ethernet Fi   | lter                     |  |        |
| W-MONITOR Disabled   |   |                          | Detected ethernet types                      |        |
| FM-QUADRO  | To add a detecte  | d ethertype to the allow | list click on Add.                           |        |
| GENERAL SETTINGS   | Ethertype   | Description              | Direction                                    | Action |
| general mode<br>wireless radio                                     | 0×8899  |                          | INGRESS                                      | Add    |
| - antenna alignment and stats<br>NETWORK CONTROL                   | 0x86DD  | IPv6                     | INGRESS                                      | Add    |
| - advanced tools<br>ADVANCED SETTINGS<br>- advanced radio settings |   | (                        | Clear detected                               |        |
| - static routes<br>- allowlist / blocklist                         |   | Allow all et             | thernet types 🗌                              |        |
| - multicast<br>- snmp  |   | Allow Etherne            | t 1 protocols 🗹                              |        |
| - radius<br>- ntp  |   |                          | Allowed ethernet types                       |        |
| ethernet filter  | To add a specific   | ethertype to the allowli | st, insert it in the text field and click on | Add.   |
| I2tp configuration<br>vlan settings                                | Ethertype   |                          | Description                                  | Action |
| - Fluidity<br>misc settings  | 0×8892  |                          | PROFINET                                     | Delete |
| - smart license<br>MANAGEMENT SETTINGS                             | 0x8204  |                          | QNX Qnet                                     | Delete |
| - remote access<br>- firmware upgrade                              |   |                          |  | Add    |
| - status<br>- configuration settings                               |   |                          | Clear allowed                                |        |
| reset factory default  |   |                          |  |        |
| - reboot<br>- logout   |   |                          | Save   |        |

I



# **Configuring Multipath Operation**

- Overview of MPO, on page 121
- Working Functionality of MPO, on page 121
- MPO Packet Duplication and Deduplication, on page 121
- Configuring MPO Features Using CLI, on page 122
- Verifying MPO Features Using CLI (MPO Monitoring), on page 123
- MPO Limitations, on page 125

# **Overview of MPO**

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

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

### Working Functionality of MPO

By default, an MPLS establishes a single tunnel using a single wireless link between the vehicle and infrastructure for data transmission. You can set up four MPLS tunnels to send MPO-protected traffic when you use two radio interfaces on two vehicle radios. When configuring MPO to utilize multiple links for protected traffic, it creates an MPLS tunnel over each available wireless link. Each wireless link replicates MPO-protected traffic. Even if one wireless link fails, the other links replicate the traffic. As of UIW Release 17.14.1, Fast Failover is supported with MPO.

# **MPO Packet Duplication and Deduplication**

For MPO, a duplicate packet is sent through several wireless channels (to various access points). This helps to ensure reliability, and the spatial diversity of the receiving access points greatly increases the chances of

at least one of the copies to be received correctly. Deduplication is another aspect of MPO to remove any duplicates of a packet that are received along the different wireless paths.

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

The process of Duplication and Deduplication as shown:



Duplication and Deduplication algorithm performs the following:

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

### **Configuring MPO Features Using CLI**

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

Device# configure fluidity mpo

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

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

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

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

Device# configure fluidity mpo status

disabled: Disable MPO duplication/deduplication.

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

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

Example:

```
enabled: E=1 F=1
rx-only: E=1 F=0
disabled: E=0 F=1 (default))
```

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

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

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

Device# show fluidity mpo config

Example:

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

### Verifying MPO Features Using CLI (MPO Monitoring)

The output of the show mpls config command:

```
Device# show mpls config
                   5.42.42.43:
                   path id : 0
                   ilm : 136000
                   nhlfe : 16:
                   lbr : 5.42.42.42
                   age : 6.980000028 { 5.42.42.42 5.42.42.43 }
                   path_id : 1
                   ilm : 136001
                   nhlfe : 18:
                   lbr : 5.42.42.42
                   age : 6.970000026 { 5.42.42.42 5.42.42.43 }
The output of the show fluidity mpo statistics command:
Device# show fluidity mpo statistics (on Mesh End)
           table-size 2:
            MAC address : 40:36:5A:15:C8:50
                                                  8C:89:A5:83:EB:71
            Tx-1 : 0
                                                   2.08
            Tx-2
                        : 0
                                                   208
            Rx-Accept-1 : 178
                                                   0
            Rx-Accept-2 : 30
                                                   0
            Rx-Drop-1 : 30
                                                   0
            Rx-Drop-2 : 178
                                                   0
            Lost-1-only : 0
                                                   0
            Lost
                        : 0
                                                   0
Device# show fluidity mpo statistics (on Mobile Primary unit)
           table-size 2:
           MAC address : 40:36:5A:15:C8:50
                                                8C:89:A5:83:EB:71
           Tx-1 : 208
Tx-2 : 208
                                                  Ω
                                                  0
           Rx-Accept-1 : 0
                                                 182
           Rx-Accept-2 : 0
                                                  26
```

| Rx-Drop-1   | : | 0 | 26  |
|-------------|---|---|-----|
| Rx-Drop-2   | : | 0 | 182 |
| Lost-1-only | : | 0 | 0   |
| Lost        | : | 0 | 0   |

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

**Tx-1 and Tx-2:** These counters represent, respectively, the number of packets transmitted on the primary path and secondary paths (cumulative sum for all available secondary paths, that is path IDs 1 to 3).

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

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

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

The output of the show fluidity network command:

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

unit 5.21.201.60 infrastructure meshend primary vehicles 4 total\_mobiles 5 infrastructure 1 backbone 0 meshend 5.21.201.60 Vehicle ID : + 85313616 Path : 0 Infrastr.ID : 5.21.201.60 Via : R1 Mobile ID : 5.21.200.80 Via : R2 H/O seq : 5710 H/O age : 36.597 #M: 2 Primary ID : 5.21.200.80 Secondary IDs : 5.21.201.204 Vehicle ID : + 85313616 Path : 1 Infrastr.ID : 5.21.201.60 Via : R2 Mobile ID : 5.21.201.204 Via : R2 H/O seq : 5711 H/O age : 5.909 #M: 2 Primary ID : 5.21.200.80 Secondary IDs : 5.21.201.204



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

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

The output of the show eng-stats command:

```
Device# show eng-stats (on mobile primary unit)
....
Fluidity role : primary
```

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

```
Mobile : 4.21.200.80 [FC:58:9A:15:B9:13]
rssi : 42
dop : 40
chan : 132/40
updated : 74
skip : 0
static : 4.21.201.60 [FC:58:9A:15:C7:D3]
mobile : 4.21.201.204 [FC:58:9A:15:E4:D3]
rssi : 41
dop : 40
chan : 100/40
updated : 18
skip : 0
rssi_delta : 6 3
threshold : 35
```

### **MPO** Limitations

If MPO is enabled, the following handoff features are not available:

- Pole Ban and Pole Proximity
- Coloring
- · Load balancing

I



# **Configuring URWB Telemetry Protocol**

Configuring URWB Telemetry Protocol, on page 127

# **Configuring URWB Telemetry Protocol**

The URWB Telemetry Protocol is introduced from UIW Release 17.12.1 and it allows for custom external monitoring of real-time wireless performance. Third-party and custom applications can use this data. Pre-defined structured UDP packets sent at regular intervals contain various network metrics.

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

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

The telemetry UDP packet contains the following information:

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

#### **Configuration of URWB Telemetry Protocol using CLI**

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

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

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

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

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

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

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

Example:

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

```
Note
```

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

To verify telemetry configuration, use the following show command:

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

#### Live Configuration of URWB Telemetry Protocol using CLI

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

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

#### Example:

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

Example (telemetry export after server configuration):

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

```
Note
```

The command immediately affects the current configuration when the live modifier is specified. Only the configuration file is changed if the live modifier is not used.

#### **Configuration of GNSS Telemetry Protocol using CLI**

To enable GNSS telemetry, use the following CLI command:

Device# configure gnss telemetry enable

To disable GNSS telemetry, use the following CLI command:

Device# configure gnss telemetry disable To show GNSS telemetry, use the following CLI command:

Device# show gnss telemetry

I



# **Configuring IW Monitor Management**

• Configuring IW Monitor Management, on page 131

# **Configuring IW Monitor Management**

The UIW Release 17.12.1 introduces support for IW Monitor. It is a standalone on-premise monitoring application supporting the following features:

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

Table 8: IW Monitor features support from UIW Release 17.12.1 onwards.

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

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

UIW Release 17.12.1 provides following support for IW Monitor dashboard:

- Attach and detach functions.
- Telemetry protocol support.
- CLI and GUI management.

#### **Detaching IW Monitor Management using CLI**

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

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

#### Example:

Device# configure monitor detach

#### **Verifying IW Monitor Management using CLI**

To verify the IW Monitor management, use the following show command:

Device# show monitor

#### Example:

Device# show monitor IW MONITOR: enabled Status: Connected

#### **Configuring IW Monitor Management using GUI**

The following image shows the **IW MONITOR** is enabled in the **Cisco URWB IW9165E or IW9167E Configurator** window:

| ULTRA RELIABLE<br>WIRELESS BACKHAUL    | Cisco URWB IW9165E Configurator<br>5.81.160 .244 - MESH END MODE   |  |  |  |
|--|--|--|--|--|
| IOTOD IW Offline                       | GENERAL MODE   |  |  |  |
| IW-MONITOR Enabled                     | Genera   | Mode   |  |  |
| FM-QUADRO                              | Select MESH POINT mode if you are attaching an IP edg<br>Cisco IOT IW9185E Series Access Point or if you are usi | ge device (i.e. network camera, encoder, etc.) to this<br>ng this unit as a relay point in the mesh network. |  |  |
| GENERAL SETTINGS                       |  | mesh point   |  |  |
| - general mode                         | Mode:  |  |  |  |
| - wireless radio                       |  | O gateway  |  |  |
| - antenna alignment and stats          |  | galeway  |  |  |
| NETWORK CONTROL                        | Radio-off:   |  |  |  |
| - advanced tools                       | Natio-oil.   | 0  |  |  |
| ADVANCED SETTINGS                      | LAN Par  | ameters  |  |  |
| - advanced radio settings              |  |  |  |  |
| - static routes                        | Local IP:  | 10.115.11.180  |  |  |
| - allowlist / blocklist                |  |  |  |  |
| - multicast                            | Local Netmask:   | 255.255.255.0  |  |  |
| - snmp                                 | Default Gateway:   | 10 115 11 1  |  |  |
| - radius                               | Delaur Galeway.  | 10.115.11.1  |  |  |
| - ntp                                  | Local Dns 1:   | 8.8.8.8  |  |  |
| - ethernet filter                      |  |  |  |  |
| - 12tp configuration                   | Local Dns 2:   |  |  |  |
| - vlan settings                        |  |  |  |  |
| - Fluidity                             |  |  |  |  |
| - misc settings                        | Reset  | Save   |  |  |
| - smart license<br>MANAGEMENT SETTINGS |  |  |  |  |
| - remote access                        |  |  |  |  |
| - firmware upgrade                     |  |  |  |  |
| - status                               |  |  |  |  |
| - configuration settings               |  |  |  |  |
| - reset factory default                |  |  |  |  |
| - reboot                               |  |  |  |  |
| - logout                               |  |  |  |  |

Once IW-MONITOR option is enabled, IW-MONITOR connection info appears as follows:

| ULTRA RELIABLE<br>WIRELESS BACKHAUL                    | Cisco URWB IW9165E Configurator<br>5.81.160.244 - MESH END MODE |                           |  |
|--|---|---------------------------|--|
| OTOD IW Offline<br>W-MONITOR Enabled                   | IW-MONITOR  |                           |  |
|  |   | R connection info         |  |
| FM-QUADRO  |   |                           |  |
| GENERAL SETTINGS<br>general mode                       | Server Host:<br>Status:   | 10.115.11.53<br>Connected |  |
| wireless radio<br>antenna alignment and stats          |   |                           |  |
| NETWORK CONTROL<br>advanced tools<br>ADVANCED SETTINGS |   | Detach                    |  |
| advanced radio settings<br>static routes               |   |                           |  |
| allowlist / blocklist<br>multicast                     |   |                           |  |
| snmp<br>radius   |   |                           |  |
| ntp<br>ethernet filter                                 |   |                           |  |
| 12tp configuration<br>vlan settings                    |   |                           |  |
| Fluidity<br>misc settings                              |   |                           |  |
| Smart license<br>MANAGEMENT SETTINGS                   |   |                           |  |
| remote access<br>firmware upgrade                      |   |                           |  |
| status<br>configuration settings                       |   |                           |  |
| reset factory default<br>reboot                        |   |                           |  |
| logout   |   |                           |  |
|  |   |                           |  |

I



## **Upgrading the Device using TFTP**

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

- The device must be connected to the network.
- The device must be configured to communicate with the local TFTP server.
- The target device image must be uploaded to the root directory of the local TFTP server.
- Device Upgrade using TFTP, on page 135
- Automatic Device Upgrade using TFTP, on page 135
- Direct Device Upgrade using TFTP, on page 137
- TFTP Device Upgrade using CLI, on page 137

## **Device Upgrade using TFTP**

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

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

## **Automatic Device Upgrade using TFTP**

#### Before you begin

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

#### Procedure

| Step 1<br>Step 2 | Create <i>device.manifest</i> file and upload to the same TFTP server root directory where the device image is stored.<br>Before enabling the TFTP automatic upgrade, configure the TFTP server and time interval. |  |  |
|------------------|--|--|--|
|                  | <b>Note</b> The time interval must be specified in the hours format.   |  |  |
|                  | Caution  | Do not disconnect or reboot the device until the device download completes. Based on the image file size, the device upgrade may take some time. |  |

### **Configuring Manifest File on the TFTP Server**

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

### **Manifest File Format**

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

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

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

| Device Type                      | Manifest File Name |  |  |  |
|----------------------------------|--------------------|--|--|--|
| IW9167EH                         | IW9167EH.manifest  |  |  |  |
| IW9165E                          | IW9165E.manifest   |  |  |  |
| IW9165DH                         | IW9165DH.manifest  |  |  |  |
| Example format of manifest file: |                    |  |  |  |

| image_n | name=ap1g6 | m-k9cl-ta | r.202307110 | )910 |  |
|---------|------------|-----------|-------------|------|--|
|         |            |           |             |      |  |

```
image_md5=376e15acd4e82a49a81d42add904f5b0
```

```
image version=8.8.1.101
```

## **Direct Device Upgrade using TFTP**

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

| Purpose                                      | Command or Action   |
|--|---|
| To configure the TFTP server with IP address | Device#configure tftp server A.B.C.D<br>A.B.C.D: IP address of the TFTP server  |
| To configure the TFTP upgrade image          | Device#configure tftp upgrade <image file=""/><br>Device#write<br>Device#reload<br>Configure TFTP upgrade image <image bin="" file=""/> |

The device immediately starts the upgrade process.



Caution

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

## **TFTP Device Upgrade using CLI**

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

Example of show TFTP configuration:

```
Device#show tftp config
Automatic TFTP Upgrade settings:
Status: enabled
```

Server: A.B.C.D Check period (hours): 3

#### Example of automatic TFTP upgrade:

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

The device upgrade procedure fails to start:

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



## LED Pattern for Catalysts IW9167 and IW9165

- LED Pattern for Catalyst IW9167, on page 139
- LED Pattern for Catalyst IW9165, on page 140

## **LED Pattern for Catalyst IW9167**

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

#### Table 9: Definition of Booting LED Pattern

| Events   | LED State      |
|--|----------------|
| Boot loader status sequence:                             | Blinking green |
| 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                                |                |
| When you press the reset button for less than 20 seconds | Blinking red   |
| When you press the reset button for more than 20 seconds | Solid red      |

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

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

#### Table 10: Definition of URWB OS LED Pattern

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

## **LED Pattern for Catalyst IW9165**

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

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

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

#### **RSSI LED**

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

#### Table 12: RSSI LEDs

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

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

#### Table 13: URWB LED function for the Catalyst IW9165E

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

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

#### Table 14: URWB LED function for the Catalyst IW9165D

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

I



## **Configure and Verify Roaming Parameters**

- Packet Retries Limitation, on page 143
- Configure Maximum Retry Limit for Packet Retransmissions using CLI, on page 143
- Verify Maximum Retry Limit for Packet Retransmissions using CLI, on page 143

## **Packet Retries Limitation**

Starting from UIW Release 17.15.1, you can set the limit for the packet retransmissions of unicast packets. This includes both aggregate and non-aggregate packets.



**Note** The maximum retry limit for packet retransmission is 32.

# Configure Maximum Retry Limit for Packet Retransmissions using CLI

#### Procedure

| Step 1 | Device#configure dotllRadio <n> packet retries <retry-count></retry-count></n> |
|--------|--|
| Step 2 | Device#write   |
| Step 3 | Device#reload  |

# Verify Maximum Retry Limit for Packet Retransmissions using CLI

Device#show dot11Radio 1 config

•

DFS region: Q DFS radar role: auto Radar detected: 0 Indoor deployment: disable Rx-SOP Threshold: 0 dBm (AUTO) Max packet retries: 32

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

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

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

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

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.