cisco.



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

First Published: 2023-07-31 Last Modified: 2025-07-31

Americas Headquarters

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



CONTENTS

PREFACE	Preface ix
	About this Guide ix
	Related Documentation ix
	Communications, Services, and Additional Information ix
CHAPTER 1	Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1
	Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1
CHAPTER 2	Device Initial Configuration in Provisioning Mode 3
	Provisioning mode 3
	How Provisioning mode works 3
	Handling DHCP and IP Address in Provisioning mode 4
	Configure fallback IP address using GUI 4
	Configure fallback IP address using CLI 5
	Configure the AP using GUI (Offline) 6
	Configure the AP using IW Service (Online Cloud-Managed) 6
	Verify the AP status using GUI 7
	Verify the AP status using CLI 8
	Verify DHCP connection status using CLI 9
	LED behavior 10
	Troubleshoot IW Service connectivity in Provisioning mode 11
	Reset the Device to Factory Default using GUI 11
	Reboot the Device using GUI 13
	Save and restore the device settings 13
	Configure general settings 14

I

	Connect to the Access Point Console Port 16
CHAPTER 3	Upgrade the Device using GUI 19
	Upgrade the device using GUI 19
CHAPTER 4	Configuring URWB Operation Mode 21
	Configuring URWB Operation Mode 21
	Determining from CLI 21
	Reset Button Settings 22
	Configuring Image Conversion 22
	Instructions to Access the GUI 22
	URWB Catalyst IW9167E Configuration using GUI 23
	Committing CLI Configuration 24
	Configure IoT OD IW Online and Offline Mode using CLI 25
	Configuring Password (after first login) using CLI 25
	Configure IoT OD IW using GUI 27
CHAPTER 5	Configuring URWB Radio Mode 29
	Configuring URWB Radio Mode 29
	Configuring Radio-off Mode from CLI 30
	Configuring Radio Mode for URWB from CLI 31
	Configuring AMPDU from CLI 31
	Configuring Frequency from CLI 32
	Configuring Maximum Modulation Coding Scheme Index from CLI 32
	Configuring Maximum Number of Spatial Streams Index from CLI 33
	Configuring Rx-SOP Threshold from CLI 33
	Configuring RTS Mode from CLI 33
	Configuring WMM Mode from CLI 33
	Configuring NTP from CLI 34
	Configuring NTP using GUI 35
	Validating Radio Mode for URWB 35
	Configuring Radio-off Mode using GUI 36
	Configuring Radio Mode using GUI 36

I

CHAPTER 6	Configuring Radio Antenna Settings 41
	Configuring Radio Antenna Settings 41
	Configuring Antenna Gain 41
	Configuring Transmit and Receive Antennas 42
	Configuring Transmission Power 42
CHAPTER 7	Configure and validate radio channel and bandwidth 43
	Configuring Operating Channel from CLI 43
	Configure channel bandwidth from CLI 43
	Validating operating channel and bandwidth from CLI 44
	Configure radio channel and bandwidth from GUI 44
	Configure Fluidity using GUI 45
	Configure fluidity using CLI 49
	Configuring fluidity role using CLI 50
CHAPTER 8	Configuring and Validating of Point-to-Point Relay Topology 51
	Configuring and Validating of Point-to-Point Relay Topology 51
	Configuring Point to Point Relay Topology from CLI 51
	Validating Point to Point Relay Topology from CLI 52
CHAPTER 9	— Configure and Validate Fluidmax Topology 55
	Configure and Validate Fluidmax (point to multipoint) Topology 55
	Configuring Point to Multipoint Topology from CLI 55
	Validate Point to Multipoint Topology using CLI 57
CHAPTER 10	— Configuring and Validating Mixed Mode (Fixed infrastructure + Fluidity) Topology 59
	Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology 59
	Configuring Mixed Mode Topology from CLI 59
	Validating Mixed Mode Topology from CLI 60
CHAPTER 11	Configure and Validate Fast Failover 63
	Overview of Fast Failover 63

l

	Configure and Validate Fast Failover 63
	Configure Fast Failover from CLI 64
	Validate Fast Failover from CLI 64
CHAPTER 12	 Configuring and Validating High Efficiency (802.11 ax) 67
	Configuring and Validating High Efficiency 67
	Configuring Global Gateway using GUI 68
CHAPTER 13	Configuring Guard Interval for HE (High Efficiency) 71
	Configuring Guard Interval for HE (High Efficiency) 71
CHAPTER 14	Configuring Indoor Deployment 73
	Configuring Indoor Deployment 73
CHAPTER 15	Configuring and Validating SNMP 75
	Configuring and Validating SNMP 75
	Configuring SNMP from CLI 75
	Validating SNMP from CLI 77
	Configuring SNMP from GUI 77
CHAPTER 16	– Multicast 81
	Overview of multicast 81
	Configure multicast using GUI 82
	Configure multicast using CLI 83
	Delete multicast using CLI 84
	Verify multicast configuration using CLI 84
CHAPTER 17	Quality of Service 85
	Overview of Quality of Service 85
	QoS configuration using CLI 86
	Verify QoS configuration using CLI 86
	802.1p VLAN priority preference configuration using CLI 87
	Verify 802.1p VLAN priority preference configuration using CLI 8

I

	Configure CoS remapping using CLI 87	
	Verify CoS remapping using CLI 88	
	Configure QoS shaping using CLI 88	
	Verify QoS shaping using CLI 89	
CHAPTER 18	Frequency Scan 91	
	Frequency scan 91	
	Overview of Fluidity frequency scan 91	
	Configure Fluidity frequency scan using CLI 92	
	Verify Fluidity frequency scan configuration using CLI 94	
	Overview of Fluidmax frequency scan 94	
	Verify Fluidmax frequency scan status using GUI 95	
	Configure Fluidmax frequency scan using CLI 95	
	Verify Fluidmax frequency scan configuration using CLI 96	
CHAPTER 19	 Configuring and Validating Key Controller (Wireless Security) 99 	
	Configuring and Validating Key Controller (Wireless Security) 99	
	Configuring Key Controller from CLI 99	
	Validating Key Controller from CLI 100	
CHAPTER 20	– Smart Licensing 101	
	Smart Licensing Support 101	
CHAPTER 21	Configuring Layer 2 Mesh Transparency 103	
	Configuring Layer 2 Mesh Transparency 103	
	Configuring and Verifying Layer-2 Protocols Forwarding Using CLI 1	104
	Configuring Layer-2 Protocol Forwarding using GUI 106	
CHAPTER 22		
	Overview of MPO 113	
	Working Functionality of MPO 113	
	MPO Packet Duplication and Deduplication 114	
	Configuring MPO Features using CLI 114	

l

	Verifying MPO Features using CLI (MPO Monitoring) 115
	MPO Limitations 117
CHAPTER 23	New Features in Cisco Catalyst IW Access Points, Release 17.12.1 119
	Enabling and Disabling Wired Interface 119
	Configuring Maximum Transmission Unit Settings 120
	Configuring Fluidity Coloring 120
	Configuring IW Monitor Management 123
	Configuring URWB Telemetry Protocol 125
CHAPTER 24	LED Pattern for Catalysts IW9167 and IW9165 129
	LED Pattern for Catalyst IW9167 129
	LED Pattern for Catalyst IW9165 130
CHAPTER 25	Fixed domains and country codes (ROW) 133
	Configuring and Verifying Regulatory Domain from CLI 133
	Configuring Regulatory Domain from GUI 134
	Supporting Fixed Domains and Country Codes (ROW) 137
	Catalyst IW9167E Supported Fixed Domains 137
	Catalyst IW9167E Supported Country Codes (ROW) 137
	Catalyst IW9165E Supported Fixed Domains 138
	Catalyst IW9165E Supported Country Codes (ROW) 138
	Catalyst IW9165D Supported Fixed Domains 139
	Catalyst IW9165DH Supported Country Codes (ROW) 139

I

Contents

l



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 ix

About this Guide

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

Related Documentation

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

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

Communications, Services, and Additional Information

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

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

Cisco Bug Search Tool

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

Documentation Feedback

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



CHAPTER

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 Cisco Ultra-Reliable Wireless Backhaul (URWB), which offers seamless handoffs, low latency, and high availability. The Catalyst IW9165 is designed to take advantage of the 6 GHz band expansion to deliver a network that is more reliable and secure, with higher throughput, more capacity, and less device interference. The Catalyst IW9165 has the option to switch images by just updating the software to operate the Catalyst IW9165 in workgroup bridge (WGB) or URWB mode without changing the hardware.

The Catalyst IW9165 series is available in two models:

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

Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

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

Cisco Catalyst IW9165D Access Point

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



Device Initial Configuration in Provisioning Mode

- Provisioning mode, on page 3
- How Provisioning mode works, on page 3
- Handling DHCP and IP Address in Provisioning mode, on page 4
- Configure fallback IP address using GUI, on page 4
- Configure fallback IP address using CLI, on page 5
- Configure the AP using GUI (Offline), on page 6
- Configure the AP using IW Service (Online Cloud-Managed), on page 6
- Verify the AP status using GUI, on page 7
- Verify the AP status using CLI, on page 8
- Verify DHCP connection status using CLI, on page 9
- LED behavior, on page 10
- Troubleshoot IW Service connectivity in Provisioning mode, on page 11
- Reset the Device to Factory Default using GUI, on page 11
- Reboot the Device using GUI, on page 13
- Save and restore the device settings, on page 13
- Configure general settings, on page 14
- Connect to the Access Point Console Port, on page 16

Provisioning mode

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

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

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

How Provisioning mode works

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

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

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

- Username: Cisco
- · Password: Cisco

Handling DHCP and IP Address in Provisioning mode

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

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



Note

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

Configure fallback IP address using GUI

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

Before you begin

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

Procedure

- **Step 1** Launch the computer's web browser and enter the URL to open the URWB configurator login page.
- **Step 2** Enter the username and password in the respective fields.

Step 3 Click Login.

L

After successfully logging into the GUI, the URWB configurator page is displayed.

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

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

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

Configure DHCP to co	onnect to IW Service
Use this section to connect the radio to the Internet via D back IP settings if DHCP is not available.	HCP to use IW Service Cloud Management. Set fall-
DHCP fall-back	configuration
Local IP:	10.11.1.2
Local Netmask:	255.255.0.0
Default Gateway:	10.11.1.0
Local Dns 1:	8.8.8.8
Local Dns 2:	4.4.4.4
Save fallba	ack IP

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

Configure fallback IP address using CLI

Before you begin

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

Procedure

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

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

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

Example:

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

Configure the AP using GUI (Offline)

Procedure

Step 1	Launch the computer's web browser and enter the URL to open the URWB configurator login page.
Step 2	Enter the username and password in their respective fields.
Step 3	Click Login . After successfully logging into the GUI, the URWB configurator page is displayed.
Step 4	Click IW Service . IW Service Configuration Mode page appears.
Step 5	Select Offline . The device exits from Provisioning mode and switch to Fallback IP address.

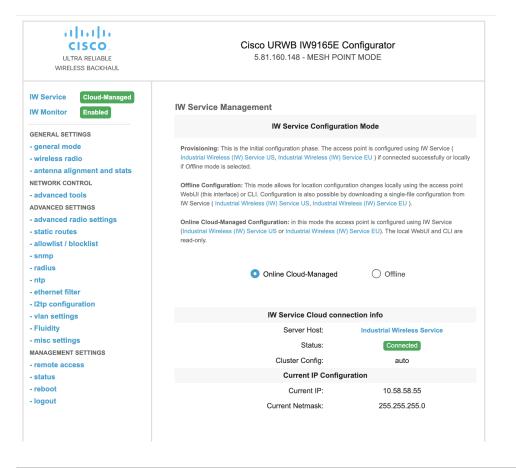
Configure the AP using IW Service (Online Cloud-Managed)

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

Procedure

Step 1	Launch the computer's web browser and enter the URL to open the URWB configurator login page.
Step 2	Enter the username and password in their respective fields.
Step 3	Click Login . After successfully logging into the GUI, the URWB configurator page is displayed.
Step 4	Click IW Service . IW Service Configuration Mode page appears.
Step 5	By default, the device is shown as Online Cloud-Managed.
	The device can be managed from IW Service cloud server (if it is connected to the internet). The device exits Provisioning

mode only if the user pushes the configuration from IW service or switches to offline mode.



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

Verify the AP status using GUI

Procedure

- **Step 1** Launch the computer's web browser and enter the URL to open the URWB configurator login page.
- **Step 2** Enter the username and password in their respective fields.
- Step 3 Click Login.

After successfully logging into the GUI, the URWB configurator page is displayed.

· Provisioning mode



• Device configurator in connected status

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

IW Service Cloud conne	ction info
Server Host:	Industrial Wireless Service
Status:	Connected
Cluster Config:	auto
Current IP Configur	ation
Current IP:	10.115.11.152 (dhcp)
Current Netmask:	255.255.255.0

• Device configurator in disconnected status.

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

	IW Service Cl	oud connect	tion info
	Server Ho	ost:	Industrial Wireless Service
	Stat	us:	Disconnected
	Cluster Con	fig:	auto
	Current I	P Configurat	tion
	Current	IP:	192.168.0.10 (fallback)
	Current Netmask:		255.255.255.0
•	Offline mode	2	
	IW Service	Offline	
	IW Monitor	Disabled	
	QUADRO		
•	Online cloud	-manage	d
	IW Service	Cloud-Ma	anaged
	IW Monitor	Enabled	

Verify the AP status using CLI

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

Procedure

L

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

Device#show iw-service status

Example:

• Device in Provisioning mode

Device#show iw-service status

IW Service mode: Provisioning

Status: Connected

Device in Offline mode

Device#show iw-service status

IW Service mode: Offline

Device in Online Cloud-Managed

Device#show iw-service status

IW Service mode: Online Cloud-Managed

Status: Connected

Verify DHCP connection status using CLI

Procedure

Step 1 This CLI example shows that the device is in provisioning mode and retrieved the IP address from the DHCP server: Use the show ip to view the status of DHCP.

• Example: DHCP Success

```
Device#show ip
```

IP: 192.168.0.10
Network: 255.255.255.0
Gateway:

Nameservers:

```
DHCP Address (PROVISIONING Mode):

IP: 10.0.0.2

Network: 255.255.255.0

Gateway: 10.0.0.1

Nameservers: 8.8.8.8

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

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

Use the show ip to view the status of DHCP.

• Example: DHCP Failure (uses default Fallback IP)

```
Device#show ip

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers:

DHCP Address (PROVISIONING Mode):

IP: 192.168.0.10

Network: 255.255.255.0

Gateway:

Nameservers: 127.0.0.1

Fallback Address (PROVISIONING Mode):

IP: 169.254.201.72

Network: 255.255.0.0
```

LED behavior

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

Troubleshoot IW Service connectivity in Provisioning mode

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

Procedure

Step 1 Step 2	Physical Connection: Verify the Ethernet cable is correctly connected. DNS Resolution: Ensures
	device.ciscoiot.com
	• us.ciscoiot.com
	• eu.ciscoiot.com
Step 3	Outbound HTTPS: Confirm the access point allows outbound HTTPS connections on tcp/443 for the domains listed in step2.
Step 4	Local Configuration: If IW Service remains offline, perform a local (offline) configuration using the device's configurator interface.
-	 eu.ciscoiot.com Outbound HTTPS: Confirm the access point allows outbound HTTPS connections on tcp/443 for the domains listed in step2. Local Configuration: If IW Service remains offline, perform a local (offline) configuration using the device's configuration

Reset the Device to Factory Default using GUI

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



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

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

IOTOD IW Offline IW-MONITOR Deabled GENERAL SETTINGS NO - general mode NO - wireless radio NO - antenna alignment and stats NO NETWORK CONTROL Advanced tools - advanced tools Advanced tools - advanced tools Solution - advanced radio settings Solution - static routes Solution - andlus Solution - totalution Solution - totalution Solution - totalutions Solution - totalutions Solution - mits cestings Solution - status Solution - status Solution - status Solution	ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9165E Configurator 5.81.160 244 - MESH POINT MODE	
general mode wireless radio antenna alignment and stats NETWORK CONTROL advanced tools ADVANCED SETTINGS advanced radio settings static routes allowlist / blocklist simp radius ntp ethernet filter l2tp configuration vian settings Fluidity miss settings remote access Immware upgrade status configuration settings		Are you sure you want to reset to factory default settings?	
- configuration settings	- Wireless radio - antenna alignment and stats NETWORK CONTROL - advanced tools Advanced tools ADVANCED SETTINGS - advanced radio settings - static routes - allowiist / blocklist - simp - radius - radius - radius - titpent filter - Litpe configuration - Vian settings - Fluidity - misc settings MANAGEMENT SETTINGS - remote access - firmware upgrade - status	NO YES	
- resertatory default - reboot - logout	- configuration settings - reset factory default - reboot		

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

V

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

Reset the Device to Factory Default using CLI

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

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

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

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

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

The following files are cleared as part of this process:

```
    Config, Bak config files
    Crashfiles
    syslogs
```

```
4) Boot variables
```

```
5) Pktlogs6) Manually created filesDo you want to proceed? (y/n)
```

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

Reboot the Device using GUI

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

1. In the MANAGEMENT SETTINGS, click reboot.

LITAR REIMARE S11.160.244 - MESH POINT MODE		
IOTOD IW Offline IW-MONITOR Disabled	Are you sure you want to reboot the unit? Any pending changes will be discarded.	
GENERAL SETTINOS - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced dould osettings - sdvanced dould osettings - static routes - static routes - aliowist / blocklist - sismp - radius - ntp - ethernet filter - i2tp configuration - vian settings - Fluidty - miss settings MNAGEMENT SETTINGS		
- remote access - firmware upgrade - status - configuration settings - reset factory default - reboot - logout		
	© 2023 Cisco and/or its affiliates. All rights reserved.	

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

Reboot the Device using CLI

To perform reboot, use the following CLI command:

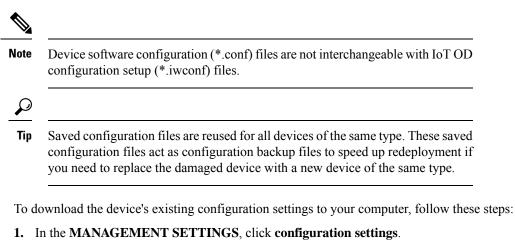
Device#reload Proceed with reload command (cold)? [confirm]

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

Save and restore the device settings

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

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



The LOAD OR RESTORE SETTINGS window appears.

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9165E Configurator 5.81.160.244 - MESH POINT MODE
IOTOD IW Offline IW-MONITOR Disabled	LOAD OR RESTORE SETTINGS Restore Settings
GENERAL SETTINGS	Restore settings from file: Browse No file selected
- wireless radio - antenna alignment and stats	Restore Save
- advanced tools ADVANCED SETTINGS	
- advanced radio settings - static routes	
allowlist / blocklist snmp	
radius ntp	
ethernet filter I2tp configuration vlan settings	
Fluidity misc settings	
MANAGEMENT SETTINGS	
firmware upgrade status	
configuration settings reset factory default	
- reboot - logout	
	© 2023 Cisco and/or 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.

Configure general settings

To change the General Mode settings, follow these steps:

1. In the GENERAL SETTINGS, click general mode.

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9165E Configurator 5.81.160.244 - MESH POINT MODE	
IOTOD IW Offline	GENERAL MODE	
IW-MONITOR Disabled	General	I Mode
GENERAL SETTINGS	Select MESH POINT mode if you are attaching an IP edg Cisco IOT IW9165E Series Access Point or if you are using	ge device (i.e. network camera, encoder, etc.) to this ng this unit as a relay point in the mesh network.
- general mode		mesh point
- wireless radio	Mode:	-
- antenna alignment and stats NETWORK CONTROL		O gateway
- advanced tools	Radio-off:	
ADVANCED SETTINGS	rtadio on.	
- 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	Default Gateway:	10 115 11 1
- ethernet filter	Delault Galeway.	10.113.11.1
- I2tp configuration	Local Dns 1:	8.8.8.8
- vlan settings - Fluidity		
- misc settings	Local Dns 2:	
MANAGEMENT SETTINGS		
remote access		
- firmware upgrade	Reset	Save
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		

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

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

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

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

Configure general settings using CLI

To configure general settings, use the following CLI command:

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

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

Change the LAN parameters

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

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

Configure LAN parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

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

Connect to the Access Point Console Port

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

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

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

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

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

Use these default credentials to log in:

- Username: Cisco
- Password: Cisco



Note

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



Upgrade the Device using GUI

• Upgrade the device using GUI, on page 19

Upgrade the device using GUI

Procedure

Step 1 Step 2	Launch the computer's web browser and enter the URL to open the URWB configurator login page. Enter the username and password in their respective fields.
Step 3	Click Login . After successfully logging into the GUI, the URWB configurator page is displayed.
Step 4	In the MANAGEMENT SETTINGS, click the firmware upgrade link to open the FIRMWARE UPGRADE window.
Step 5	Click the Browse button to locate and select the firmware upgrade file.
Step 6	Click the Upgrade button to initiate the upgrade process.
Step 7	Click OK to confirm uploading the firmware file to the device. Once the firmware is successfully uploaded to the device, the AP verifies the image and then reboots.

	Cisco Cisco URWB IW9165E Configurator ULTRA RELIABLE 5.81.160.164 - MESH END MODE WIRELESS BACKHAUL 5.81.160.164 - MESH END MODE		
IW Service Offline	FIRMWARE UPGRADE		
IW Monitor Disabled	Firmware upgrade		
QUADRO GENERAL SETTINGS	Upload and upgrade the firmware using a firmware upgrade file. Firmware upgrades are available to registered users at software.cisco.com. WARNING: POWERING OFF OR UNPLUGGING A Cisco URWB UNIT DURING A FIRMWARE UPGRADE PROCEDURE WILL PERMANENTLY DAMAGE THE UNIT		
- general mode	Current version: 17.16.0.80		
- wireless radio			
- antenna alignment and stats	Select the firmware file to upload and start the upgrade:		
NETWORK CONTROL	Browse ap1g6m-k9c1-tar.17.16.0.88.tar		
- advanced tools			
ADVANCED SETTINGS			
- advanced radio settings	Upgrade		
- static routes			
- allowlist / blocklist			
- multicast			
- snmp			
- radius			
- ntp			
- ethernet filter			
- I2tp configuration			
- vlan settings			
- Fluidity			
- misc settings			
- smart license			
MANAGEMENT SETTINGS			
- remote access			
- firmware upgrade			
- status			
- configuration settings			
 reset factory default reboot 			
- logout			
- iogoar			
	© 2024 Cisco and/or its affiliates. All rights reserved.		



Configuring URWB Operation Mode

- Configuring URWB Operation Mode, on page 21
- Determining from CLI, on page 21
- Reset Button Settings, on page 22
- Configuring Image Conversion, on page 22
- Instructions to Access the GUI, on page 22
- URWB Catalyst IW9167E Configuration using GUI, on page 23
- Committing CLI Configuration, on page 24
- Configure IoT OD IW Online and Offline Mode using CLI, on page 25
- Configuring Password (after first login) using CLI, on page 25
- Configure IoT OD IW using GUI, on page 27

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 WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.112 - MESH END MODE
	Login
Usernam Enable Passwor Show passwor	d:
© 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 WIRELESS BACKHAUL	Cisco URWB IW91 5.21.201.72 - ME	
IOTOD IW Offline	GENERAL MODE	
FM-QUADRO	Genera	I Mode
GENERAL SETTINGS - general mode - wireless radio - antenna alignment and stats NETWORK CONTROL	Select MESH POINT mode if you are attaching an IP edg Cisco Catalyst IV9167E Heavy Duty Access Point or if y network. Mode:	mesh point mesh end
- advanced tools) gateway
ADVANCED SETTINGS	Radio-off:	
- static routes	LAN Parameters	
- allowlist / blocklist		
- multicast	Local IP:	10.115.11.117
- snmp		
- radius	Local Netmask:	255.255.255.0
- ntp	D.(
- I2tp configuration	Default Gateway:	10.115.11.1
- vlan settings	Local Dns 1:	8.8.8.8
- Fluidity		
- misc settings	Local Dns 2:	
- smart license		
MANAGEMENT SETTINGS - remote access - firmware upgrade	Reset	Save
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		
	© 2022 Cisco and/or its affiliates. All rights reserved	L

URWB Catalyst IW9167E Configuration using GUI

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

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	
IOTOD IW Offline	GENERAL MODE	
FM-QUADRO	General Mode	
GENERAL SETTINGS	Select MESH POINT mode if you are attaching an IP edge device (i.e. network camera, encoder, etc.) to this Cisco Catalyst IW9167E Heavy Duty Access Point or if you are using this unit as a relay point in the mesh network.	
- wireless radio	 mesh point 	
- antenna alignment and stats	Mode: O mesh end	
NETWORK CONTROL	⊖ gateway	
- advanced tools		
ADVANCED SETTINGS	Radio-off:	
- advanced radio settings	Kadio-Off:	
static routes LAN Parameters		
- allowlist / blocklist		
- multicast	Local IP: 10.115.11.117	
- snmp		
- radius	Local Netmask: 255.255.255.0	
- ntp	D. (
- I2tp configuration	Default Gateway: 10.115.11.1	
- 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		
 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)

Configure IoT OD IW Online and Offline Mode using CLI

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

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

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

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

Device#configure iotod-iw {offline | online}

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

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

Configuring Password (after first login) using CLI

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

- The username length must be between 3 to 32 characters long.
- The password length must be between 8 to 32 characters long.
- The password must include the following:
 - At least one uppercase letter
 - · At least one lowercase character,
 - · At least one digit
 - At least one special character
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not allowed:
- " [double quote]
- '[single quote]
- ? [question mark]
- The password must not contain:
 - Three sequential characters or digits (ABC/CBA)
 - The same three characters or digits consecutively (AAA) or (666)

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

Example:

Default credentials:

username: Cisco password: Cisco enable password: Cisco

To reset the credentials, use the following sample credentials:

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

Example of configuring password using CLI:

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

User Access Verification: Username: Cisco Password: Cisco

After first login, reset the credentials:

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

Once the credentials are changed, re-login:

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

Device#



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

Configure IoT OD IW using GUI

This image shows the configuration of IoT OD:

IOTOD IW Conf	figuration Mode	
	iguration mode	
Provisioning: initial radio configuration phase. Th Centralized Web Interface (<u>IOTOD Industrial Wirel</u> connection is successful or manually if <i>Offline</i> con	eless US, IOTOD Industrial Wireless EU	
Offline Configuration: it supports local paramete upload of a single file downloaded from IOTOD IW Industrial Wireless US, IOTOD Industrial Wireless E	/ section in IOTOD Industrial Wireless (
Online Cloud-Managed Configuration: the radio Interface (IOTOD IW section in <u>IOTOD Industrial W</u> connected to the Internet and can access IOTOD I only.	Vireless US or IOTOD Industrial Wireles	ss EU) if i
Online Cloud-Mana	aged Offline	
UPLOAD IOTOD IW CONFIGURATION	N FILE	
Upload Confi	iguration File	
Select configuration file exported from IOTOD Industrial Wireless:	Browse No file selected	
	34	
Last configuration ID		
Last configuration ID		

l



Configuring URWB Radio Mode

- Configuring URWB Radio Mode, on page 29
- Configuring Radio-off Mode from CLI, on page 30
- Configuring Radio Mode for URWB from CLI, on page 31
- Configuring AMPDU from CLI, on page 31
- Configuring Frequency from CLI, on page 32
- Configuring Maximum Modulation Coding Scheme Index from CLI, on page 32
- Configuring Maximum Number of Spatial Streams Index from CLI, on page 33
- Configuring Rx-SOP Threshold from CLI, on page 33
- Configuring RTS Mode from CLI, on page 33
- Configuring WMM Mode from CLI, on page 33
- Configuring NTP from CLI, on page 34
- Configuring NTP using GUI, on page 35
- Validating Radio Mode for URWB, on page 35
- Configuring Radio-off Mode using GUI, on page 36
- Configuring Radio Mode using GUI, on page 36

Configuring URWB Radio Mode

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

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

Table 1: Radio Mode Configuration

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

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

Table 2: Operating Mode of Radio Interface

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

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

Table 3: Configuration of Multiple Radio interfaces

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

Configuring Radio-off Mode from CLI

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



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

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

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

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

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

3. To set the radio-off mode.

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

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

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

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

Configuring Radio Mode for URWB from CLI

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

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

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

Device# configure dot11Radio <interface>

2. Configure an operating mode for the specified interface.

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

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

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

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

3. Set Fluidmax role for Fluidmax interface mode.

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

Primary - set Fluidmax role to primary

Secondary - set Fluidmax role to secondary

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

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



Note

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

Configuring AMPDU from CLI

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

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

length: <0-255> integer number - microseconds.
Device# configure 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 index 7.

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

Configuring Frequency from CLI

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

Configuring Maximum Modulation Coding Scheme Index from CLI

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

Device# configure dot11radio <interface> mcs <maxmcs>

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

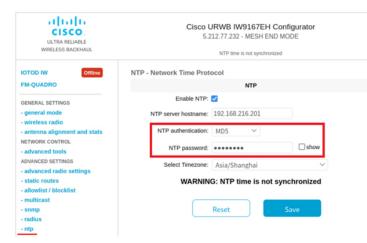
To validate the NTP configuration and status, use the following show commands:

```
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 using GUI

The following image shows the GUI of NTP:



Validating Radio Mode for URWB

To validate Radio mode, use the following show commands:

Device# show dot11Radio <interface> config

Example:

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

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

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

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

Configuring Radio-off Mode using GUI

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

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 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 end and connecting this unit to a wired network (i.e. LAN).
- general mode	() mesh point
- wireless radio	Mode: Mode:
- antenna alignment and stats	⊖ gateway
NETWORK CONTROL	
ADVANCED SETTINGS	Radio-off: 🗹 Fixed 🗸
- 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	
- I2tp configuration	Default Gateway: 10.115.11.1
- vian settings	Local Dns 1: 8.8.8.8
- Fluidity	
- misc settings	Local Dns 2:
- smart license	
MANAGEMENT SETTINGS - remote access	Reset
- remote access	Reset
- status	
- configuration settings	
- reset factory default	
- reboot	
- logout	
	© 2022 Cisco and/or its affiliates. All rights reserved.

Configuring Radio Mode using GUI

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

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

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

ULTRA RELIABLE WIRELESS BACKHAUL		URWB IW9167 5.21.201.72 - MESI	7EH Configurator H END MODE
IOTOD IW Offline	WIRELESS RADIO		
FM-QUADRO		Wireless Se	ettings
GENERAL SETTINGS - general mode		hitespace (e.g. "mysecu	characters excluding '(apex) "(double apex) '(back urecamnet") that indentifies your network. It MUS me network.
- wireless radio	Shared Passphrase:	PASSWORD	
 antenna alignment and stats 			URWB units, they need to be operating on the sa
NETWORK CONTROL	frequency.	lection between cisco o	brown units, they need to be operating on the sa
- advanced tools		Radio 1 Se	ettings
ADVANCED SETTINGS	Poloi	Fixed	~
- advanced radio settings - static routes	Kole.	Fixed	
- static routes - allowlist / blocklist	Frequency (MHz):	5180 ~	
- multicast			
- snmp	Channel Width (MHz):	80 ~	
- radius		Radio 2 Se	ettings
- ntp		(
- I2tp configuration	Role:	Disabled	\sim
- vlan settings			
- Fluidity		Decet	Cours
- misc settings		Reset	Save
- smart license			
MANAGEMENT SETTINGS			
- remote access			
- firmware upgrade			
- status			
- configuration settings			
- 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 WIRELESS BACKHAUL	Cisco URWB IW9167EH 5.21.201.72 - MESH END	
IOTOD IW Offline	ADVANCED RADIO SETTINGS	
FM-QUADRO	Radio 1	
GENERAL SETTINGS	FluidMAX Managem	ent
- general mode - wireless radio - antenna alignment and stats	Force the FluidMAX operating mode of this unit. If the operating mn ID can be set. If the FluidMAX Autoscen is enabled, the Secondary with the Primary with the same Cluster ID. In this case, the frequen disabled.	units will scan the frequencies to assor
NETWORK CONTROL - advanced tools	Radio Mode: PRIM	ARY
ADVANCED SETTINGS - advanced radio settings	FluidMAX Cluster ID: CLUS	TER_ID
- static routes	Max TX Power	
- allowlist / blocklist - multicast - snmp - radius	Select the max power level that the radio shall use to transmit (pow The Cisco URWB TPC (Transmit Power Control) will automatically according to the channel condition while not exceeding the MAX TO automatically enabled.	select the optimum transmission power
- radius - ntp	Select TX Max Power: 1	~
- 12tp configuration	Antenna Configurat	ion
- vlan settings - Fluidity	Select radio 1 antenna gain and antenna number.	
- misc settings - smart license	Select Antenna Gain: UNSE	ECTED V
MANAGEMENT SETTINGS - remote access	Antenna number: ab-an	enna 🗸
- firmware upgrade - status	Data Packet Encrypt	ion
- configuration settings - reset factory default	Enable AES to cypher all wireless traffic. This setting must be the s	ame on all the Cisco URWB units.
- reboot	Enable AES: Disabl	ed 🗸
- logout	Maximum link leng	th
	Insert the length of the longest link in the net, or let the system sele	ct an optimal value.
	© 2022 Cisco and/or its affiliates. All rights reserved.	(11)

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.

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

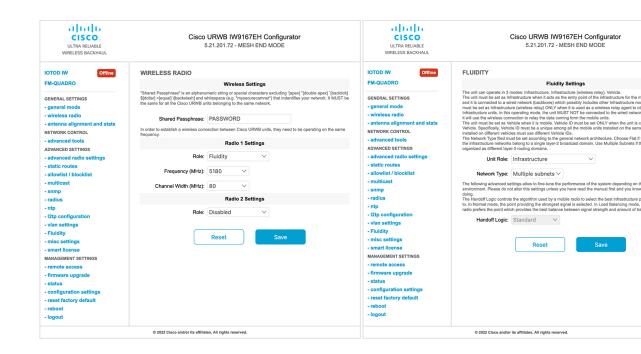


Note In Europe TPC is automatically enabled.

- 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.



l



Configuring Radio Antenna Settings

• Configuring Radio Antenna Settings, on page 41

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 dotl1radio <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 dotl1radio <interface> antenna < A > configure antenna chains (A) in use as follows a-antenna - configure dotl1 antenna a ab-antenna - configure dotl1 antenna ab abcd-antenna - configure dotl1 antenna abcd Device# write
```

Configuring Transmission Power

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

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



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

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



CHAPTER

Configure and validate radio channel and bandwidth

- Configuring Operating Channel from CLI, on page 43
- Configure channel bandwidth from CLI, on page 43
- Validating operating channel and bandwidth from CLI, on page 44
- Configure radio channel and bandwidth from GUI, on page 44
- Configure Fluidity using GUI, on page 45
- Configure fluidity using CLI, on page 49

Configuring Operating Channel from CLI

To configure operating channel, use the following CLI commands:

- Configure the wireless device with radio interface number < 1 or 2 > Device# configure dot11Radio <interface>
- 2. Set the operating channel id and the valid range is from 1 to 256 Device# configure dot11Radio <interface> channel id>
- 3. To end the current configuration, use the following CLI command: Device (configure dot11Radio <interface> channel <channel id>) # end Example:

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

Configure channel bandwidth from CLI

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

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

3. Returns to privileged EXEC mode.

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

Validating operating channel and bandwidth from CLI

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

Device# show dot11Radio <interface> config

Example:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fluidmax secondary
Frequency : 5180 MHz
Channel : 36
Channel width : 40 MHz
Device# show dot11Radio 2 config
Interface : enabled
Mode : fluidity
Frequency : 5785 MHz
Channel : 157
Channel width : 40 MHz
```

Configure radio channel and bandwidth from GUI

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

Following image shows the configuration of Radio channel and bandwidth:

ULTRA RELIABLE WIRELESS BACKHAUL		URWB IW9167EH Configurator 21.201.88 - MESH POINT MODE
IOTOD IW Offline	WIRELESS RADIO	
IW-MONITOR Disabled		Wireless Settings
GENERAL SETTINGS - general mode	"Shared Passphrase" is an alphanu \$[dollar] =[equal] (backstash) and w the same for all the Cisco URWB ur	meric string or special characters excluding '[apex] "[double apex] '[backtick hitespace (e.g. "mysecurecannet") that indentifies your network. It MUST b its belonging to the same network.
- wireless radio	Shared Passphrase:	CiscoURWB
 antenna alignment and stats 		nection between Cisco URWB units, they need to be operating on the same
NETWORK CONTROL	frequency.	rection between Cisco Orcivis units, they need to be operating on the same
- advanced tools		Radio 1 Settings
ADVANCED SETTINGS		
- advanced radio settings	Role:	Fixed
- static routes	Frequency (MHz):	5260
- allowlist / blocklist	riequency (in iz).	0200
- snmp	Channel Width (MHz):	20
- radius		De la Octavia
- ntp		Radio 2 Settings
- ethernet filter	Role:	Fixed
- I2tp configuration		
- vlan settings	Frequency (MHz):	5180
- Fluidity		
- misc settings	Channel Width (MHz):	80
MANAGEMENT SETTINGS		
- remote access		Reset Save
- firmware upgrade		Reset
- status		
- 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.

DEVICE SETTINGS PEVICE SETTINGS general mode Netmask: 252,252,253,253 wireless radio Outputs anterna alignment and stats Salurus up advanced footo Diputs: full advanced radio Diputs: full advanced radio settings Salurus dup static routes WIRELESS SETTINGS allowidt: // blocklist Pasphrazis: CacuONNB-118 general Terguange, CacuONNB-118 general Terguange, CacuONNB-118 general Terguange, CacuONNB-118 general Channel Midth: 20 Midt: 20 Midt Una settings Channel Midth: 20 Midt: 20 Midt Vian settings Channel Midth: 20 Midt: 20 Midt Miss astings Antenna number: 2 definition		
TURNELING TURNELING WITCH SEGNATION WITCH SEGNATION WITCH SEGNATION WITCH SEGNATION Barnal mode Witch SE STATUS Barnal mode Barnal mode Witch SE STATUS Status Control Barnal mode Barnal mode Witch SE Status Barnal mode	ahaha	
WIRELESS MACHAUL WIRELESS MACHAUL WIRELESS MACHAUL STOD IW Windown Ton	CISCO	Cisco URWB IW9167EH Configurator
WRELESS BACCHAU. To Data and a manufacture of the second		
Arten 11 File Operating Mode Mash Point Uptime: 4 days, 16:23 (hhrmm) WMONTOR Operating Mode Mash Point Uptime: 4 days, 16:23 (hhrmm) BERERAL EETTINGS Bererating Mode Mash Point Uptime: 4 days, 16:23 (hhrmm) BERERAL EETTINGS Netmask: 25:255.255.05 Advanced fools Nethols </td <td></td> <td></td>		
OTOD IW Operating Mode: Mash Point WAKONTOR Entered WENDATIOR Entered Status: Status: general mode MAC address: 40.26 23 015-02-08 0 writeless radio MAC address: 40.26 23 015-02-08 0 writeless radio MAC address: 40.26 25 05.56 0 advanced tools Depoint: 10.50 writeless radio Depoint: 10.50 status: com Status: com status: com Status: com status: com Status: com status: radios Writeless radio interdes: catable Comatil: 52 Channel Wdit: 52 Channel Wdit: 52 Channel Wdit: 52 Channel Wdit: 52 Channel Wdit		
AVACONTOR Firmware version: 8.8.1.0 Firmware version: 8.8.1.0 DEVCE SETTINGS general mode MAC address: 40.356.15.0 witeles ratio Configured MTL: 15.0 anterna alignment and stats Section MAC address: 40.356.15.0 advanced ratio Configured MTL: 15.0 advanced tools WIEED advanced ratio Configured MTL: 15.0 advanced ratio Configured MTL: 15.0 advanced ratio WIEED advanced ratio Configured MTL: 15.0 Configured MTL: 15.0 Maximum link length: 3 km Maximum link length: 3 km Conrect to power: 10 dBmL Configured MTL: 15.0 Maximum link length: 3 km Linger Antenna subt: 72 Maximum link length		
VALONTRO DEVICE SETTINGS general mode DEVICE SETTINGS pri to 115 1118 DEVICE SETTINGS pri to 115 1118 DEVICE SETTINGS advanced rools Configured MTU: 1530 advanced rools Speci: 1000 MU/s advanced rools MTU: 1530 advanced rools MTU: 1530 advanced rools MTU: 1530 allowist / blocklist Salue: four sinp Pasiphrasic CaceUNINE-118 general mode Prequency 5200 MHz Channel Wd/M: 20 MHz Channel: 52 Vain settings Channel: 52 Automa author: 2 Pasiphrasic CaceUNINE-118 general mode Prequency 5200 MHz Channel: 52 Channel: 52 Automa author: 2 Pasiphrasic CaceUNINE-118 general mode Prequency 5200 MHz Channel: 52 Pasiphrasic CaceUNINE-118 general mode Pasiphrasic CaceUNINE-118 general mode access Pasiphrasic CaceUNINE-118 general mode Patoma author: 2 MANCOURT SETTINGS	OTOD IW Offline	
ENCRAL SETTINGS general mode wireless radio antenna alignment ad stats sentenna alignment ad stats sentenna static routes sentenna static routes sentenna static routes sentenna static routes sentenna static routes sentenna static routes sentenna sentenna static routes sentenna s	W-MONITOR Disabled	Firmware version: 8.8.1.10
EXERCAL SETTINGS IP: 10.115.11.118 general mode MAC advass: 40.26 20.50.0 witeless radio MAC advass: 40.26 20.50.0 witeless radio MMEDIO anterna alignment and stats Status: up Status: up Status: up advanced tools Duptor: full unworkED 97 Mac advass: Status: up status: up Status: up status: up Status: up status: op Status: down status: op Status: down status: op Status: down status: op Status: down status: concultave Marchantave: CacudAve status: op Consenting region: B status: concultave Arasphanas: CacudAve status: op Consenting region: B status: concultave Charlen Status: CacudAve status: down Charlen Status: Concultave remota access Maximum link length: 3 Mm Ital op Interface: casted remota access Maximum link length: 3 Mm Itanop Interface: casted		DEVICE SETTINGS
general mode MAC address: 40.365.a150:c058 wireless radio configured MU: 1530 DVANCED SETTINGS static routs advanced radio settings Static routs allowint / bocisit Papers Configured MU: 1530 DVANCED SETTINGS static routs allowint / bocisit Papers Configured MU: 1530 DVANCED SETTINGS static routs allowint / bocisit Papers Configured MU: 1530 Coperating region: 5 Coperating reg	ENERAL SETTINGS	IP: 10.115.11.118
witeless radio Configured MTU: 1530 Nature MTRED0 anterna alignment and stats structure Status: up Nature MTRED0 Status: up Status: up structure Status: up MARED0 Date: 1500 Status: up Status: up MARED0 Date: 1530 Status: up Status: down advanced radio settings Status: down attict routes Pasephrana: Claco/URVB-118 Operating region: B Pasephrana: Claco/URVB-118 Operating region: B Operating region: B attor total Channel: 12 Van acttings Channel: 12 Van acttings Channel: 12 Van acttings Anterna muber: 2 Autorna pin: no steledod Anterna muber: 2 Maximutinik length: 3 km Configuration Channel Widt: 20 MHz Channel: 12 Fluidity Anterna muber: 2 Maximutinik length: 3 km Maximutinik length: 3 km Inferfac:: disabled Maximutinik length: 3 km Inferfac:: disabled Current ty power How:: 1	general mode	
Interna alignment and stats VIREDO Envoins Control. Speed: 100 Mb/s Subarcit Of Speed: 100 Mb/s Speed: 100 Mb/s Subarcit Of Speed: 100 Mb/s Speed: 100 Mb/s Subarcit Of Speed: 100 Mb/s WRED1 Subarcit Of Speed: 100 Speed: 1	-	
Emotors CourteoL Speed: 1000 Mb/s advanced tools Write 1 advanced tools WriteD1 advanced radio settings Status: down advanced radio settings advanced radio rad		
advanced tools Dupler: full Dupler: full D		
advances tools MTU: 1530 advances settings Status: down advanced radio settings Status: down satile routes Pasophrase: Ciscu/DRVB-118 opperating regions Particle: Tiscu/DRVB-118 via settings Mode: ford infrastructure status Channel: S2 Fluidity Current to power lowel: 1 via settings Antenna quin: not seleded maios cettings Antenna quin: not seleded finware upgrade Radio Addo: cimal can addo status Interface: Gasbled configuration settings Processor; 5100 MHz configuration settings Processor; 5100 MHz reveal tactory default Channel Wdith: S00 MHz configuration settings Processor; 5100 MHz configuration settings Processor; 5100 MHz reset tactory default Channel Wdith: S00 MHz content to power level: 1 Antenna suin: not selected	ETWORK CONTROL	
DUMANCED SETTINGS VIRED1 advanad radio settings Salus: down static routes VIRED: SS SETTINGS advanad radio settings Salus: down samp Operating region: B radius Advanced radio Settings radius Ninefrace: nabled radius Control Settings radio Settings Attenna gain: not selected radio Settings Frequency, Statings resolat Control Settings Frequency, Statings resolat Control Settings Frequency, Statings remote access Frequency, Statings remote access Control Settings readio Settings Frequency, St	advanced tools	
advanced radio settings	DVANCED SETTINGS	
allowiist / blocklist Pasphrase, Claud/RWB-118 omp annp radus Radio Pasphrase, Claud/RWB-118 Operating region: B radus Radio 1 rtp Radio 1 rtp Channel Vidit: 20 MHz Channel Vidit: 20 MHz Channel Vidit: 20 MHz Channel Siz Vian settings Channel Vidit: 20 MHz remota access Maximum Fir. 2 Satus Channel Vidit: 20 MHz remota Cacess Maximum Fir. 2 Satus Channel Vidit: 20 MHz resource Channel Vidit: 20 MHz Channel Vidit: 20 MHz Channel Vidit: 20 MHz Antenna pain: not selicided Antenna pain: not selicided A	advanced radio settings	Status: down
allowiar V blocklist Pasaphrasa: Ciscu/RWB-118 organitar regions Radio 1 radius Radio 1 rtp Mode: Tool infrastructure ethemati filter Floquency: 5280 MHz IZIP configuration Channel: 52 Van settings Channel: 52 Fluidatily Channel: 52 Fluidatily Channel: 52 Fluidatily Current b power level: 1 misc settings Antenna gain: not seleded Aukactuktra Termota Radio 12 remota access Maximum link length: 3 km remota access Maximum link length: 3 km restata factory defauit Channel Vidito: 00 MHz configuration access Maximum link length: 3 km remota access Maximum link length: 3 km restata factory defauit Channel Vidit: 00 MHz configuration actings and acting access Maximum link length: 3 km restata factory defauit Channel Vidit: 00 MHz restata factory defauit Channel Vidit: 00 MHz restata factory defauit Current to power level: 1 restata factory defauit Attenna Vidit: 00 MHz restata factory defauit Attenna Vidit: 00 MHz restata factory defauit Attenna Vidit: 00 MHz configuration acting acting acting ac	static routes	WIRELESS SETTINGS
smmp Operating region: B radius radio 1 radius Hadio 1 thefra: nabled thefra: requency: 5260 MHz Cipconfiguration Channel: 52 Charmed to: Current to power: 02 dBm Filedity Current to power: 100 MHz Value settings Antonna gain: not selected maics cettings Maximum link length: 3 km remote access Maximum link length: 3 km resolot Current to power 100 MHz Current to power 100 MHz Current to power 100 MHz contigration settings Frequency, 5180 MHz context Current to power 100 MHz current to power 100 MHz Current to power 100 MHz current to power 100 MHz Current to power 100 MHz current to power 100 MHz Current to power 100 MHz current to power 100 MHz Current to power 100 MHz current to power 100 MHz Current to po	allowlist / blocklist	Passphrase: CiscoURWB-118
radius Radio 1 htp Mode: food infrastructure defmant filter Pieupency, 5280 Mitz Ltip configuration Channel: 52 Huider Viewer to power 20 Mitz Current to power 20 Mitz Fuider Viewer to power 20 Mitz Fuider Viewer to power 20 Mitz Manastings Antenna muther: 2 Antenna gain: not selected Antenna funktioner 2 Antenna funk		Operating region: B
Interface: canabled Interface: canabled Interface: mobiled Interface: mobiled Interface: mobiled Interface: mobiled Interface: mobiled Interface: Interfac		Radio 1
Mode: Insel affrastructure Mode: Insel affrastructure Kithernet filter Findiguration Citte configuration Channel Width: 20 MHz Was actings Current ts power: 28 dBn Findity Anneel Width: 20 MHz Content ts power: 28 dBn Findity Anneel Width: 20 MHz Content ts power: 28 dBn Findity Anneel Width: 20 MHz Configuration actings Findity Anneel Width: 20 MHz Configuration settings Configuration settings Configuration settings Configuration settings Content ts power: 10 dBm		Interface: enabled
Iztp configuration Channels 22 Valan settings Channel Vidits: 22 MHz Valan settings Charnel Vidits: 20 MHz Plaidhy Charnel Vidits: 20 MHz Rest Charnel Vidits: 20 MHz Markatestring Charnel Vidits: 20 MHz Markatestring Charnel Vidits: 20 MHz Markatestring Antenna number: 2 MARAGESTRITS Radio Mode: cemarka Immare upgrade Radio Mode: cemarka Immare upgrade Radio 12 Interface: disabled Concent: 50 Content: 50 Status Mode: fixed infrastructure Frequency: 5180 MHz Content: 50 Current ts power 10 dBm Current ts power 10 dBm Current ts power 10 dBm Current ts power 10 dBm Antenna stati: not selected Maximum link length: 3 km DAGNOSTIC TOOL		
Lap Computation Channel Width: 20 MHZ Van settings Current tx power: 28 dBm Fluidity Auterna gain: role selected Macs settings Auterna gain: role selected macs settings Radio Mode: cemaña maca settings Radio Mode: cemaña maca settings Radio Mode: cemaña maca settings Radio Mode: cemaña configuration settings Frequency: 518 MHZ configuration settings Frequency: 518 MHZ reset factory default Channel: 36 channel Width: 30 MHZ Current tx power: 19 dBm contra tx power: 19 dBm Auteina MHZ contra tx power: 19 dBm Auteina MHZ channel Width: 20 MHZ Current tx power: 19 dBm channel Width: 30 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power: 19 dBm channel Width: 80 MHZ Current tx power		
Van settings Current to power 25 dBm Fluidhy Current to power 1994 miss settings Anterna to power 1994 Anterna pair: not selected Anterna pair not selected firmware upgrade Real 2 status Mode frod infrastructure configuration settings Frequency, 5180 MHz resolut Current to power 19 dBm Current to power 19 dBm Anterna surber: 2 Anterna surber: 2 Maximum link length: 3 km	12tp configuration	
Antenna gain: not seleded Antenna gain: not seleded Antenna gain: not seleded Antenna rumber: 20 ANAGEKENT SETTINGS ANAGEKENT SETTINGS ANAGEKENT SETTINGS ANAGEKENT SETTINGS ANAGEKENT SETTINGS ANAGEKENT SETTINGS ANAGEKENT ANTENNA A	vlan settings	
misc settings Antona number: 2 Antona nu	Fluidity	
ANAGEMENT SETTINGS Radio Mois: cemarka remote access firmware upprade Radio 2 status status configuration settings reset factory default channel Vidth: S0 MHz channel Vidth: S	misc settings	
Termota experies Radio 2 status Interface: disabled configuration settings Revinory 51 MMz configuration settings Channel: 36 channel Widh: 80 MMz Channel Widh: 80 MMz reset factory default Channel Widh: 80 MMz resolution Current to power 10 dBm logout Current to power 10 dBm Advance gain: noti-adio Mode: comarka Radio Mode: comarka Maximum link length: 3 km DIAGNOSTIC TOOL	ANAGEMENT SETTINGS	
Immars upgrade Radio 2 status Mode: fixed infrastructure configuration settings Frequency: 5180 MHz reset factory default Channel: 36 Channel Width: S0 MHz Channel: 30 Channel Width: S0 MHz Channel: 38 Liggout Channel S0 Antenna pair, mick solved Channel S0 Antenna number: 2 Radio Mode: cama/ca Radio Mode: cama/ca Maximum link length: 3 km DIAGNOSTIC TOOL Concel	remote access	Maximum link length: 3 km
status interface: disabled interface: disabled configuration settings interface: fixed infrastructure Prequency: 5180 MHz interface: disabled Courses to power: 19 dBm interface: disabled Courses to power: 19 dBm interface: disabled Antenna gain: not selected Antenna gain: not selected Maximum link length: 3 km interface: Tool		Padio 2
Mode: tixed infrastructure configuration settings Freed tactory default Channel: 30 Mode: tixed infrastructure resolt Channel: 30 Digout Charment brower 10 dBm Logout Antenna gain: not seleded Antenna mumber: 2 Radio Mode: cama'ca Maximum link length: 3 km DIAGNOSTIC TOOL		
reset factory default Channel 30 reboot Channel 30 reboot Channel Wdith: 80 MHz Current to power 19 d8m Current to power 19 d8m Current to power 19 d8m Anterna aurbare 2 Rado Mode: comarka Maximum link length: 3 km DIAGNOSTIC TOOL		
Channel Wilder: 60 MHz Channel Wilder: 60 MHz Current ts power 19 dBm Current ts power 19 dBm Current ts power 19 dBm Antonna gain: not seldedd Antonna wilder: 51 seldedd Antonna wilder: 51 seldedd Maximum link length: 3 km DIAGNOSTIC TOOL		
reboot Current to power 19 dBm Courrent to power 19 dBm Antonna gain: not selected Radio Mode: camarka Maximum link length: 3 km DIAGNOSTIC TOOL		
Antenna gain: not selected Antenna number: 2 Radio Mode: csmałca Maximum link length: 3 km DIAGNOSTIC TOOL		Current tx power: 19 dBm
Antenna number: 2 Rado Mode: cimalca Maximum link length: 3 km DIAGNOSTIC TOOL	logout	
Radio Mose: esmañea Maximum link length: 3 km DIAGNOSTIC TOOL		
DIAGNOSTIC TOOL		
		Maximum link length: 3 km
© 2023 Clisco and/or Its affiliates. All rights reserved.		DIAGNOSTIC TOOL
© 2023 Cisco and/or its affiliates. All rights reserved.		
		to zuza cisco and/or its affiliates. All rights reserved.

Configure Fluidity using GUI

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

1. In the GENERAL SETTINGS, click wireless radio.

The WIRELESS RADIO window appears.

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

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE
IOTOD IW Offline	WIRELESS RADIO
FM-QUADRO	Wireless Settings
GENERAL SETTINGS - general mode	"Shares Passphrase" is an alphanumeric strip or special characters excluding "(anext) "(Scuble apent) [Scuble apent] Soldaliar "(apent) (Backstah) and whitespace (a, ""measuremenner) that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.
- wireless radio	Shared Passphrase: PASSWORD
- antenna alignment and stats 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	Role: Fluidity
- advanced radio settings - static routes	Role. Fluidity
- static routes	Frequency (MHz): 5180 V
- multicast	
- snmp	Channel Width (MHz): 80 V
- radius	Radio 2 Settings
- ntp	Role: Disabled
- I2tp configuration	Role: Disabled V
- vlan settings	
- Fluidity	Reset
- misc settings	
- smart license	
MANAGEMENT SETTINGS	
- remote access - firmware upgrade	
- firmware upgrade - status	
- configuration settings	
- reset factory default	
- reboot	
- logout	
-	
	© 2022 Cisco and/or its affiliates. All rights reserved.

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



• 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 WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	
OTOD IW Offline	FLUIDITY	
M-QUADRO SENERAL SETTINGS general mode wireless radio antenna alignment and stats IETWORK CONTROL advanced tools DywarcED SETTINGS	Fluidity Settings The unit can operate in 3 modes: infrastructure, infrastructure, (wireless reliep), Vehicle. The unit must be set as infrastructure, when it can as the entry point of the infrastructure for the mobile vehicl and it is connected to a wirel network (backboon) which possibly includes ofter infrastructure necks. The unit infrastructure in the infrastructure in the infrastructure infrastructure in its insolue. Which can be availed and the infrastructure infrastructure infrastructure in its insolue. Which can be availed and the institute infrastructure infra	as it
advanced radio settings	Unit Role: Vehicle	
static routes		
allowlist / blocklist multicast	Automatic Vehicle ID: Enable	
snmp	Vehicle ID: 1234	
radius	Network Type: Flat V	
ntp	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 a	10
l2tp configuration vlan settings Fluidity	doing. The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to conn to. In Kormal modo, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.	
misc settings smart license MANAGEMENT SETTINGS	Handoff Logic: Standard V	
remote access	Reset	
- firmware upgrade - status		
- status - configuration settings		
- reset factory default		
- reboot		
logout	© 2022 Cisco andor its affiliatas. All rights reserved.	
	© 2022 Clisco and/or its affiliates. All rights reserved.	
Iligout CISCO. ULTRA RELABLE WIRELESS BACKHAUL	© 2022 Clisco and/or its atfiliates. All rights reserved. Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	
ULTRA RELABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator	
ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	
UITTA RELIABLE WIRELESS BACKHAUL OTOD IW EM-QUADRO CM-QU	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	as
UTTOR RELARCE WIRELESS BACKHAUL UTTOR RELARCE WIRELESS BACKHAUL OTOD IW MCULARON STORE STINOS Beneral mode wireless radio antenna alignment and stats entroyokk control. advanced tools LOVANCED SETTINOS advanced radio settings	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDTY Fuldity Settings To unit can operate in 3 models. Vehicle. The unit materials end as the structure of the end you of the final structure for the mobile web and its connected to a wired network (basichood yells) possibly includes other infrastructure node. The unit materials. In this operation groups, the structure of the mobile web and its connected to a wired network (basichood yells) possibly includes other infrastructure node. The unit materials. In this operating mode, the unit MUST NOT be connected to the wired network backbo Its will use the wireless connection to relay the data coming form the mobile units. The unit materials and a Woldwide with its models. The unit materials and with the wireless of the wireless connections to relay the data coming form the mobile units. The unit materials and a Woldwide with its models.	as
LILTA RELABLE URELESS BACKHAUL WIRELESS BACKHAUL OTOD IW CM-QUADRO OTOD IW CM-QUADRO SENERAL SETTINGS ageneral mode wireless ratio antenna alignment and stats retwork control. advanced fors statvanced fors statvanced radio settings static routes	Elizabet in the second se	as
UTTAN RELIABLE UITAN RELIABLE WIRELESS BACKHAUL UITAN RELIABLE WIRELESS BACKHAUL OTOD IW Offline TM-QLADRO TM-QLAD	EVENTS	as
UITA RELABLE UITA RELABLE WIRELESS BACKHAUL OTOD IW Office TM-QUADRO OTOD IW Office TM-QUADRO SEVERAL SETTINGS ageneral mode wireless radio antenna alignment and stats setting coutes advanced todis settings static routes atlavinet / blocklist multicast simp	CISCO URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE	ie as as Unit and
ULTRA RELABLE WIRELESS BACKHAUL UUTRA RELABLE WIRELESS BACKHAUL OTOD IW OFM.QLARO OFM.QLARO SenterAL SETTINGS general mode wireless radio antenna alignment and stats general mode wireless radio antenna alignment and stats settor routes advanced tools static routes alowalich blocklist multicast simp radius static settings	ELUDITE ELUDITEE ELU	as Junit and
ULTRA RELABLE WIRELESS BACKHUL ULTRA RELABLE WIRELESS BACKHUL OTOD IW CMILO MAQUADRO SENERAL SETTINGS ageneral mode wirrielses radio antenna alignment and stats (ErWORK CONTROL advanced tools ULVANCE SETTINGS advanced tools ULVANCE SETTINGS advanced tools ULVANCE SETTINGS advanced tools ULVANCE SETTINGS advanced tools ULVANCE SETTINGS advanced tools ULVANCE SETTINGS advanced tools	CISCO URWB IW9167EH Configurator C.2.12.01.72 - MESH END MODE	as Junit and
UTTAN RELIABLE UITAN RELIABLE WIRELESS BACKHAUL UITAN RELIABLE WIRELESS BACKHAUL OTOD IW Offline M-QUADRO OTOD IW Offline M-QUADRO OTOD IW Offline M-QUADRO OTOD IW Offline M-QUADRO OTOD IW Offline M-WIRESS BACKHAUL OTOD IW Offline M-WIRESS BACKHAUL OTOD IW Offline M-WIRESS BACKHAUL OTOD IW Offline M-WIRESS BACKHAUL OTOD IW Offline Second Second Seco	Electronic December 2012 Control of the product of the produc	as Junit and
LI L	CISCO URWB IW9167EH Configurator C.2.12.01.72 - MESH END MODE	as Junit and
UTTAN RELIABLE ULTAN RELIABLE WIRELESS BACKHALL UUTAN RELIABLE WIRELESS BACKHALL OTOD IW CMILLO	Electronic December 2012 Control of the product of the produc	as Junit and
LITRA RELARLE WIRELESS BACKHAUL ULTRA RELARLE WIRELESS BACKHAUL OTOD IW CMULACO COD IW CMULACO COD IW CMULACO COD IW CMULACO COD IW CMULACO CM	<section-header><text><section-header><section-header><section-header></section-header></section-header></section-header></text></section-header>	as Junit and
UTTO RELABLE WRELESS BACKHAUL WRELESS BACKHAUL COTOD IW Office FM-QUADRO GENERAL SETTINGS - general mode - writelass radio - antenna alignment and stats - writelass radio - advanced to SETTINGS - advanced to SETTINGS - advanced settings - static routes - advanced settings - static routes - antenna settings - inp - fulcity - Flucity - Flucity - Flucity - inse settings - samt license - May Settings	Electronic December 2012 Control of the product of the produc	as Junit and
IIIIIII CISCO. ULTRA RELARIE WIRELESS BACKHAUL	<section-header><text><section-header><section-header><section-header></section-header></section-header></section-header></text></section-header>	as Junit and
UTTOR RELIANCE UTTOR RELIANCE UTTOR RELIANCE UTTOR RELIANCE UTTOR DELIANCE UTTOR DI COTINO COTI	<section-header><text><section-header><section-header><section-header></section-header></section-header></section-header></text></section-header>	as Junit and
UTTAN RELABLE WIRELESS BACKHAUL UTTAN RELABLE WIRELESS BACKHAUL OTOD IW Office FM-QUAORO Sevenal SETTINGS ageneral mode wirdless ratio antenna alignment and stats wirdless ratio advanced atols settings advanced atols settings advanced tools settings advanced tools settings advanced ratio settings alowist / blocklist multicast settie routes advanced ratio settings fillelity antenna settings fillelity sings cettings smart licens mart licens firmware upgrade status configuration settings	<section-header><text><section-header><section-header><section-header></section-header></section-header></section-header></text></section-header>	as Junit and
LITRA RELABLE WIRELESS BACKHAUL UITRA RELABLE WIRELESS BACKHAUL OTOD IW Offline M-QUADRO DEMERAL SETTINGS general mode wireless ratio antenna alignment and stats wireless ratio antenna alignment and stats wireless ratio antenna settings attatic routes allowlist / blocklist multicast somp - radius multicast 	<section-header><text><section-header><section-header><section-header></section-header></section-header></section-header></text></section-header>	as Junit and

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

ULTRA RELIABLE WIRELESS BACKHAUL		Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE		
	Offline	WIRELESS RADIO		
FM-QUADRO		Wireless Settings		
GENERAL SETTINGS		"Shared Passphrase" is an alphanumeric string or special characters excluding "(apex) "(double apex) "(backtick) S(dollar) =[equal] (backsiash) and whitespace (e.g., mysecurecamer)" that indentifies your network. It MUST be the same for all the Cisco URVB units belonging to the same network.		
- general mode - wireless radio		Shared Passphrase: PASSWORD		
- antenna alignment	and stats	In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same		
- advanced tools		frequency. Radio 1 Settings		
ADVANCED SETTINGS - advanced radio set	ttings	Role: Fluidity V		
- static routes - allowlist / blocklist		Frequency (MHz): 5180		
- allowlist / blocklist - multicast		Channel Width (MHz): 80 V		
- snmp - radius		Radio 2 Settings		
- ntp		Role: Disabled V		
- I2tp configuration - vlan settings		Role: Disabled		
- Fluidity		Reset		
- misc settings - smart license				
MANAGEMENT SETTING	GS			
- remote access - firmware upgrade				
- status				
 configuration setting reset factory defaultion 				
- reboot				
- logout				
ahal	1.	Φ 2022 Cisco and/or its affiliates. All rights reserved.		
ULTRA RELA WIRELESS BAC	O _	© 2022 Cisco and/or its atflittets. All rights reserved. Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE		
ULTRA RELIA	O _ ABLE KHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE		
ULTRA RELIA WIRELESS BAC	O _	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE		
ULTRA RELIA WIRELESS BAC	O _ ABLE KHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
ULTRA RELA WIRELESS BAC	O _ ABLE KHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
OTOD IW FM-QUADRO SENERAL SETTINGS general mode wireless radio	ABLE KKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
CISC ULTRA RELIX WIRELESS BAC OTOD IW FM-QUADRO SENERAL SETTINGS general mode wireless radio antenna alignment VETWORK CONTROL	ABLE KKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
ULTRA RELIX WIRELESS BAC OTOD IW FM-QUADRO DEENERAL SETTINGS general mode wireless radio antenna alignment NETWORK CONTROL advanced tools	ABLE KKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
ULTRA RELIX WIRELESS BAC OTOD IW M-QUADRO BENERAL SETTINOS general mode wireless radio antenna alignment (ETWORK CONTROL advanced tools advanced radio set advanced radio set advanced radio set	O LABLE KHAUL Offline and stats	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE FLUIDITY Fluidity Settings		
ULTRA RELU ULTRA RELU WIRELESS BAC OTOD IW M-QUADRO DEENEAL SETTINGS general mode wireless radio antenna alignment kerwork control. advanced tools advanced radio set static routes alowair / blocklist	O BILE KHAUL Offline and stats	Clisco URWB IW9167EH Configurator S.12.01.72 - MESH END MODE FLUIDITY FLUIDITY Neuritational set as a infrastructure, infrastructure (vertiless relay). While Model and the set as infrastructure, infrastructure, infrastructure, for the infrastructure for the nordine vertiles must be set as infrastructure, infrastructure, infrastructure, for the infrastructure for the nordine vertiles must be set as infrastructure, infrastructure, for the infrastructure for the nordine vertiles must be set as infrastructure, infrastructure, for the infrastructure for the nordine vertiles must be set as infrastructure, infrastructure, for the infrastructure for the nordine vertiles must be set as infrastructure, infrastructure, the vertiles must be set as infrastructure, infrastructure, infrastructure, the vertile infrastructure as the set as vertiles were infrastructure, infrastructure, infrastructure, infrastructure, infrastructure, infrastructure, the vertile infrastructure, choose Fuit fithen ensiste vertile infrastructure, infrastruc		
ULTRA REL/ WIRELESS BAC VOTOD IW FM-QUADRO DENERAL SETINGS general mode - wireless radio -	O BILE KHAUL Offline and stats	Cisco URWB IW9167EH Configurator 5.21201.72 - MESH END MODE FLUIDITY FLUIDITY Fluiding Sector S		
ULTRA RELIX WIRELESS BAC OTOD IW M-QUADRO DENERAL SETTINGS ogeneral mode wireless radio antenna alignment vertwork controct. advanced tools babAvAccD SETTINGS advanced radio settino static routes allowlist / blocklist multicast simp	O BILE KHAUL Offline and stats	<section-header> Creation of the section of the</section-header>		
CISC ULTRA REL/ WIRELESS BAC TOTOD IW MM-QUADRO DEENERAL SETTINGS - general mode - wireless radio - wireless	O BILE KHAUL Offline and stats	Classo URWB IW9167EH Configurator S.12.01.72 - MESH END MODE FUIDITY FUIDITY Media		
ULTRA REL/ ULTRA REL/ WIRELESS BAC OTOD IW FM-QUADRO SENERAL SETTINGS general mode wireless radio antenna alignment EWYORK CONTROL advanced roots advanced roots static routes advanced radio set static routes advanced roots static routes advanced roots advanced roo	O BILE KHAUL Offline and stats	<section-header> Creation of the section of the</section-header>		
UTRA REL/ WHELESS BAC OTOD IW M-QUADRO DENERAL SETTINGS -general mode wireless radio -antenna alignment verworkk cowtrocl. -advanced radio set advanced radio set -advanced radio set -adv	O BILE KHAUL Offline and stats	Ciaco URWB IW9167EH Configurator 5.12.01.72 · MESH END MODE FLUIDTY FLUIDTY FLUIDTY Internet and a constraint of the state of the internet of the system depending on the specific density of the state of the system depending on the specific density of the state of the system depending on the specific density of the state of the system depending on the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific		
CISC ULTRA REL/ WRIELESS BAC OTOD IW M-QUADRO SENERAL SETTINGS general mode wineless radio wineless radio wineless radio wineless radio wineless radio wineless radio wineless radio wineless radio wineless radio wineless radio advanced cols stator routes wineless radio advanced radio set stator routes wineless radio radius wineless radio radius wineless radio radius wineless radio radius wineless radio radius wineless radio radio radius wineless radio r	O. VALE VALE OTTIMO and stats	Ciaco URWB IW9167EH Configurator 5.12.01.72 · MESH END MODE FLUIDTY FLUIDTY FLUIDTY Internet and a constraint of the state of the internet of the system depending on the specific density of the state of the system depending on the specific density of the state of the system depending on the specific density of the state of the system depending on the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific density of the system depending on the specific density of the specific		
UTRA RELIX WIRELESS BAC OTOD IW M-QUADRO Senters and the senter wireless radio antenna alignment wireless radio advanced tools advanced tools advanced tools advanced radio set static routes allowlist / blocklist multicast salowlist / blocklist salowlist / blocklist multicast salowlist / blocklist salowlist / blocklist multicast salowlist / blocklis	O. VALE VALE OTTIMO and stats	<section-header></section-header>		
CIDEC ULTRA REL/ WIRELESS BAC TOTOD IW MM-QUADRO DENERAL SETTINGS - general mode wireless radio - antenna alignment NetWork CONTROL - advanced Dock - advanced tools - advanced - advanced tools - advanced - adv	O. VALE VALE OTTIMO and stats	<section-header></section-header>		
UTTA RELU WIRELESS BAC DOTOD IW FM-QUADRO GENERAL SETTINGS - general mode - wireless radio - advanced fools - advanced fools - advanced radio set - static routes - static route	O. WILE WILE (Offline) and stats ttings	<section-header></section-header>		
UTRA RELIX WIRELESS BAC OTOD IW M-QUADRO Seneral mode wireless ratio antenna alignment extransitive advanced tools advanced tools advanced ratio settin static routes allowlist / blocklist multicast allowlist / blocklist allowlist / blocklist multicast allowlist / blocklist allowlist / blocklist allowlist allowlist / blocklist allowlist allowlist / blocklist allowl	O. WRLE WRLE OTTIMO and stats and stats ttings	<section-header></section-header>		
UTRA RELIV WIRELESS BAC OTOD IW -M-QUADRO DERRAL SETTINGS general mode wireless radio antenna alignment werwork control. advanced tools advanced tools advanced tools advanced tools advanced tools static routes alowlar / blocklat multicast static routes alignment radius ritp ponfiguration vian settings smart license WanAced Wart SETTING remote access firmware upgrade status	O. WRLE WRLE OTTIMO and stats and stats ttings	<section-header></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.

48

ULTRA RELIABLE WIRELESS BACKHAUI	5	URWB IW9167EH Configurator .21.201.88 - MESH POINT MODE
	WIRELESS RADIO	
W-MONITOR Disa	bled	Wireless Settings
	"Shared Passphrase" is an alphani	
SENERAL SETTINGS	\$[dollar] =[equal] \[backslash] and the same for all the Cisco LIRWB i	umeric string or special characters excluding '[apex] "[double apex] '[backtick] whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be nits belonging to the same network.
general mode		nits belonging to the same network.
wireless radio	Shared Passphrase:	CiscoURWB
antenna alignment and s	tats	
ETWORK CONTROL	frequency.	nection between Cisco URWB units, they need to be operating on the same
advanced tools		Radio 1 Settings
ADVANCED SETTINGS		
advanced radio settings	Role:	Fixed ~
static routes	Frequency (MHz):	5260
allowlist / blocklist	Frequency (WHZ):	5260 \$
snmp	Channel Width (MHz):	20 ×
radius	onamer main (in iz).	
ntp		Radio 2 Settings
ethernet filter	Bala	Fluidity
- I2tp configuration	Role.	Fididity
vlan settings	Frequency (MHz):	5500 ~
Fluidity	, (
misc settings	Channel Width (MHz):	80 ~
MANAGEMENT SETTINGS		
- remote access		
firmware upgrade		Reset Save
status		
- configuration settings		
- reset factory default		
reboot		
logout		
	© 2023 Cisco and/or its affilia 10.115.11.118 says	Mes. All rights reserved.
		with radio configuration.
dhalh Cisco	10.115.11.118 says Error: unit role vehicle is not compatible	with radio configuration.
LITA BELABLE WRELESS BACHALE	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit	with radio configuration. y for role vehicle.
ILITA RELABLE WRELESS BACKHALE WRELESS BACKHALE	10.115.11.118 says Error: unit role vehicle is not compatible	with radio configuration. y for role vehicle.
ILITA RELABLE WRELESS BACKHALE WRELESS BACKHALE	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes. Appl	with radio configuration. y for role vehicle.
ULTRA RELABLE UNRELESS BACKHALK INTO IN WWMONITOR GENERAL SETTINGS	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit	with radio configuration. y for role vehicle.
UTTA RELABLE WRELESS BACKHAU WRELESS BACKHAU WRANNITOR GENERAL SETTINGS general mode	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes. Appl FLUIDITY	with radio configuration. y for role vehicle. OK y these changes? Discard Review Apply
LITER RELABLE WIRELESS RACCHAUL WIRELESS RACCHAUL WIRELESS RACCHAUL GOTOD IW Ommu WIRELESS RAIO antenna aligament and stat segenaral mode wireless radio antenna aligament and stat NETWORK CONTROL advanced tools advanced tools advanced tools	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes. Appl FLUIDITY	with radio configuration. y for role vehicle. OK y these changes? Discard Review Apply
IIIIII CISCO UTRA ELIANE WRELESS BACGHAUL OTOD IW WMONITOR CISAN SENERAL SETTINGS general mode wireless radio antenna alignment and sta workers radio antenna alignment and sta advanced radio settings static routes aldvanced blocklist	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUIDITY Units in this operate in 3 modes: Infeator The unit can operate in 3 modes: Infeator The	with radio configuration. y for role vehicle. with sease changes?
UTRA RELABLE UTRA RELABLE WRELESS BACCHAL WRELESS BACCHAL WREDS BACCHAL WREDS BACCHAL WREDS BACCHAL WREDS BACCHAL BACCHAL Second Bacchal Ministry State Second Bacchal Second Bacc	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUDITY Hendit and contains changes: Apply FLUDITY Hendit and contains changes: Apply Configuration co	with radio configuration. y for role vehicle. These changes? Discard Preview Apply Review Apply
UTRA RELABLE ULTRA RELABLE WIRELESS RACIONAUL WIRELESS RACIONAUL ULTRA RELABLE WIRELESS RACIONAUL DISABLE	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUIDITY Units in this operate in 3 modes: Infeator The unit can operate in 3 modes: Infeator The	with radio configuration. y for role vehicle. These changes? Discard Preview Appy Review Ap
ULTRA RELABLE UUTRA RELABLE WRELESS BACKAUL WRELESS BACKAUL OTOD IW W-MONITOR DISAU WW-MONITOR DISAU WW-MONITOR DISAU WW-MONITOR DISAU WW-MONITOR DISAU DIS	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUDITY Hendit and contains changes: Apply The unit and contains changes: Apply FLUDITY Hendit and contains changes: Apply The unit and the unit and the act actions to the unit and the act actions to the unit and the act actions the unit and the unit and the unit and the act actions the unit and the unit and the act actions the unit and the u	with radio configuration. y for role vehicle. These changes? Discard Preview Appy Review Ap
UTTAN RELIABLE ULTAN RELIABLE WIRELESS BACKHAUL WIRELESS BACKHAUL WIRELESS BACKHAUL OTOD IW WIRELESS BACKHAUL OTOD IW WIRELESS BACKHAUL MANNITOR EXPERAL SETTINGS Expended Tadio settings advanced tools tadio settings advanced tools satiscr outse satiscr outse satiscr outse enterned filter	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply Configuration Conf	with radio configuration. y or role vehicle. vetesse changes? biscar bis
LITTA RELIABLE URTA RELIABLE WRELESS BACKINUT WWMONITOR BENERAL SETINOS general mode wirrieless radio antenna alignment and sta wirrieles radio antenna alignment and sta seture control. advanced tools backwace tools backwace tools advanced tools backwace tools advanced tools backwace tools advanced tools backwace tools advanced tools backwace tools advanced tools backwace tools advanced tools	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply Configuration Conf	with radio configuration. y or role vehicle. vetesse changes? biscar bis
UTTRA RELABLE WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL DOTOD IW WIRELESS BACCHALL DOTOD IW WIRELESS BACCHALL MANNONTOR COMMIN WIRELESS BACCHALL COMMIN COMMIN WIRELESS BACCHALL COMMIN CO	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply Configuration Conf	with radio configuration. y or role vehicle. vetesse changes? biscar bis
IIIIII CISCO UTTA REINARE WRELESS BACONAUL WRELESS BACONAUL WRELESS BACONAUL OTTOD IW WMONITOR Grand Gran	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply Configuration Conf	with radio configuration. y or role vehicle. vetesse changes? biscar bis
UTTOR RELABLE UUTTOR RELABLE WRELESS BACCHALL WRELESS BACCHALL WRELESS BACCHALL WRELESS BACCHALL WRELESS BACCHALL OTOD IW W.MONITOR CHALL SETTINGS - general mode - wireless radio - antenna alignment and sta - wireless radio - wireless radio - antenna alignment and sta - wireless radio - wireless radio - static routes - alignwist / blockist - static routes - align - thora filter - 12tp configuration - vian settings - Fluidity - mics settings	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUDITY Hennis and a set as infrastructure with the unit must be as as infrastructure with and the unit must be as as infrastructure with and the infrastructure networks being to be as the infrastructure networks being to b	with radio configuration. y or role vehicle. retrees changes? bic or retree of the provide of
LUTAR ARLANE WRELESS BACCHAIL WRELESS BACCHAIL WRELESS BACCHAIL WRELESS BACCHAIL WRELESS BACCHAIL WRENAL SETTINGS general mode wirdless radio antenna alignment and st wirdless radio antenna alignment and st wirdless radio advanced tools advanced tools advanced tools tatic routes advanced tools tatic routes tatic rou	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply Configuration Conf	with radio configuration. y or role vehicle. retrees changes? bic or retree of the provide of
LITTOR RELABLE UNTELESS DACHAUX WRELESS DACHAUX WRELESS DACHAUX UNTELSS DACHAUX WRELESS DACHAUX UNTELSS DACHAUX DENERAL SETTINGS general mode writelss radio antenna alignment and sta writelss radio antenna alignment and sta satur coutes advanced tools ADVANCE DESTINGS advanced tools ADVANCED SETTINGS advanced tools ADVANCED SETTINGS advanced tools ADVANCED SETTINGS advanced tools ADVANCED SETTINGS - static routes allowist / blocklist - simp - ethernet filter - Fluidity - misc settings SMANGAEMERT SETTINGS - remote access	10.115.11.118 says Error: unit role vehicle is not compatible Both radios must be configured as fluidit Configuration contains changes: Apply FLUDITY Hennis and a set as infrastructure with the unit must be as as infrastructure with and the unit must be as as infrastructure with and the infrastructure networks being to be as the infrastructure networks being to b	with radio configuration. y or role vehicle. retrees changes? bic or retree of the provide of
ULTRA RELABLE UNRELESS BACKHALK INTO IN WWMONITOR GENERAL SETTINGS	10.115.11.118 says Torr unit role vehicle is not compatible Both radios must be configured as fuldid Configuration contains changes: Appp Configuration contains changes: Appp FULDITY The time of the start of the start of the start of the start the time of the start of the start of the start of the start the start of the start of the start of the start of the start Contains and Start of the start of th	<pre>with radio configuration y or role vehicle. y r these changes?</pre>
LITER RELARSE ULTER RELARSE WRELESS BACCHAL WRELESS BACCHAL WRELESS BACCHAL WRELESS BACCHAL WRELESS BACCHAL OTOD IW WRENTS - general mode - wireless radio - antenna sligoment and sta - advanced tradio settings - advanced radio settings - radius - nip - redius - Fluidity - Wins settings - Fluidity - Fluidity - Imase access - Imware upgrade	10.115.11.118 says Torr unit role vehicle is not compatible Both radios must be configured as fuldid Configuration contains changes: Appp Configuration contains changes: Appp FULDITY The time of the start of the start of the start of the start the time of the start of the start of the start of the start the start of the start of the start of the start of the start Contains and Start of the start of th	with radio configuration. y or role vehicle. retrees changes? bic or retree of the provide of
UTTRA RELABLE UUTRA RELABLE WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL WIRELESS BACCHALL WIRELSS BACCHALL OTOD IW W.M.MONITOR DEALERST Searchall	10.115.11.118 says Torr unit role vehicle is not compatible Both radios must be configured as fuldid Configuration contains changes: Appp Configuration contains changes: Appp FULDITY The time of the start of the start of the start of the start the time of the start of the start of the start of the start the start of the start of the start of the start of the start Contains and Start of the start of th	<pre>with radio configuration y or role vehicle. y r these changes?</pre>
LITTA RELABLE URTEA RELABLE URTEAR SELABLE URT	10.115.11.118 says Torr unit role vehicle is not compatible Both radios must be configured as fuldid Configuration contains changes: Appp Configuration contains changes: Appp FULDITY The time of the start of the start of the start of the start the time of the start of the start of the start of the start the start of the start of the start of the start of the start Contains and Start of the start of th	<pre>with radio configuration y or role vehicle. y r these changes?</pre>

Configure fluidity using CLI

To enable Fluidity, use the following CLI commands:



Note

At least one radio interface should be in Fluidity mode.

Device# configure dot11Radio <interface> mode fluidity

Example to enable Fluidity for radio 1:

configure dot11Radio 1 mode fluidity

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

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

Configuring fluidity role using CLI

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

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

Device# configure fluidity id

2. Configure Fluidity id mode.

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

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

Device (configure fluidity id {mode}) # end

Device# wr

Example:

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



CHAPTER O

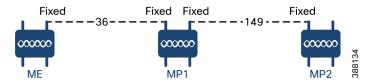
Configuring and Validating of Point-to-Point Relay Topology

- Configuring and Validating of Point-to-Point Relay Topology, on page 51
- Configuring Point to Point Relay Topology from CLI, on page 51
- Validating Point to Point Relay Topology from CLI, on page 52

Configuring and Validating of Point-to-Point Relay Topology

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

Figure 1: point to point relay topology



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

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

Configuring Point to Point Relay Topology from CLI

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

- 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

l



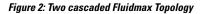
CHAPTER 🖜

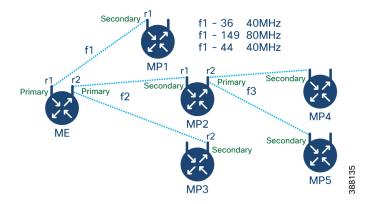
Configure and Validate Fluidmax Topology

• Configure and Validate Fluidmax (point to multipoint) Topology, on page 55

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).





Configuring Point to Multipoint Topology from CLI

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

Device# configure dot11Radio <interface>

Interface - <0-3> Dot11Radio interface number.

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

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

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

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

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

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

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

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

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

Device#wr

Example of point to multipoint (Fluidmax) topology configuration

ME (Mesh End) Configuration

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

MP1 (Mesh point) Configuration

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

MP2 Configuration

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

MP3 Configuration

```
Device# Configure 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 dotl1Radio 1 enable
Device# Configure dotl1Radio 1 mode fluidmax secondary
Device# Configure dotl1Radio 1 channel 44
Device# Configure dotl1Radio 1 band-width 40
```

L

Validate Point to Multipoint Topology using CLI

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

Device# show dot11Radio <interface> config

Example:

ME (Mesh End) radio2

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

MP2 (Mesh Point)

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

MP4 radio1

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

l



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

- Configuring and Validating Mixed Mode (Fixed Infrastructure + Fluidity) Topology, on page 59
- Configuring Mixed Mode Topology from CLI, on page 59

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

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

Figure 3: Mixed Mode Topologies



Configuring Mixed Mode Topology from CLI

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

Device# configure dot11Radio <interface>

Interface - <0-3> dot11Radio interface number

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

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

Device# configure 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 63
- Configure and Validate Fast Failover, on page 63
- Configure Fast Failover from CLI, on page 64
- Validate Fast Failover from CLI, on page 64

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 and Validating High Efficiency (802.11 ax)

- Configuring and Validating High Efficiency, on page 67
- Configuring Global Gateway using 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 dotllRadio 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 using GUI

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

1. In the GENERAL SETTINGS, click general mode.

The GENERAL MODE window appears.

2. Click gateway from Mode.

Following images shows the GUI configuration of global gateway mode:

I

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.201.72 - MESH END MODE		
OTOD IW Offline	GENERAL MODE		
FM-QUADRO	General Mode		
GENERAL SETTINGS	Global Gateway mode automatically enforces MPLS layer 3 and radio-off. Radio status cannot be changed in Global Gateway mode.		
- general mode	() mesh point		
- wireless radio	Mode: O mesh end		
• antenna alignment and stats NETWORK CONTROL	o gateway		
advanced tools Advanced Settings	Radio-off: 🗹 Fluidity 🗸		
advanced radio settings	LAN Parameters		
- static routes - allowlist / blocklist	LAN Farameters		
- multicast	Local IP: 10.115.11.117		
- snmp - radius	Local Netmask: 255.255.255.0		
- radius - ntp			
- I2tp configuration	Default Gateway: 10.115.11.1		
- vlan settings	Local Dns 1: 8.8.8.8		
- Fluidity			
- misc settings	Local Dns 2:		
- smart license			
MANAGEMENT SETTINGS	Reset		
- firmware upgrade	Reset		
- 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 freq

lucitoy.				
	Radio 1	Settings		
Role:	Disabled	\sim		
	Radio 2	Settings		
Role:	Disabled	\sim		
	Reset	Sav	ve 🔰	

FLUIDITY

Fluidity Settings

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

The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.

Unit Role:	Infrastructure	\sim

Network Type: Multiple subnets \vee

The following advanced settings allow to fine-tune the performance of the system depending on the specific environment. Please do not alter this settings unless you have read the manual first and you know what you are doing. The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to connect

to. In Normal mode, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.

Handoff Logic: Standard

Reset Save



CHAPIER I

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 Indoor Deployment

• Configuring Indoor Deployment, on page 73

Configuring Indoor Deployment

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



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

By default, the devices are set to outdoor mode.

To enable indoor deployment, use the following CLI command:

Device# configure wireless indoor-deployment enable

To disable indoor deployment, use the following CLI command:

Device# configure wireless indoor-deployment disable

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

For enabled indoor deployment

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

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 and Validating SNMP

• Configuring and Validating SNMP, on page 75

Configuring and Validating SNMP

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

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

Figure 4: SNMP Process



Configuring SNMP from CLI

To configure SNMP, use the following CLI commands:



Note

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

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

Device#configure snmp [enable | disable]

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

Device#configure snmp version {v2c | v3}

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

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

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

Device#configure snmp v3 username <length 32>

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

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

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

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

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

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

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

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

Device#configure snmp secret <length 8-64>

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

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

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

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

Notification value trap period measured in minutes.

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

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

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

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

To disable SNMP configuration, use the following CLI command:

Device#configure snmp disabled

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

Example of SNMP configuration:

CLI for SNMP v2:

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

CLI for SNMP v3:

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

Validating SNMP from CLI

To validate the SNMP, use the following show command:

Device# show snmp SNMP: enabled Version: v3 Username: username Password: password Authentication method: SHA Encryption: AES Encryption Passphrase: passphrase Engine ID: 0x800000903c0f87fe5f314 Periodic Trap: enabled Notification Period (minutes): 5 Event Trap: enabled NMS hostname: 192.168.116.11 Device# show snmp SNMP: enabled Version: v2c Community ID: test Periodic Trap: enabled Notification Period (minutes): 5 Event Trap: enabled NMS hostname: 192.168.116.11 Device# show system status snmpd Service Status Service Name : snmpd Loaded : loaded Active : active (running) Main ProcessID : 6437 Running Since : Mon 2022-09-19 14:45:27 UTC; 3h 34min ago Service Restart : 0

Configuring SNMP from GUI

The following images shows the configuration of SNMP from GUI

GUI for SNMP v2:

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.200.136 - MESH END MODE		
TOD IW Offline	SNMP		
-MONITOR Disabled	SN	MP	
A-QUADRO	SNMP mode:	v2c ~	
ENERAL SETTINGS	Community ID:	test	
jeneral mode vireless radio	Enable SNMP periodic trap:		
Intenna alignment and stats	Enable SNMP event trap:		
Idvanced tools	NMS hostname:	192.168.0.100	
VANCED SETTINGS	Notification period (minutes):	1 0	
static routes			
illowlist / blocklist nulticast	Reset	Save	
inmp			
adius			
ntp			
thernet filter			
2tp configuration			
lan settings			
luidity			
nisc settings			
mart license			
NAGEMENT SETTINGS			
mote access			
rmware upgrade			
tatus			
onfiguration settings			
set factory default			
boot			
ogout			

GUI for SNMP v3:

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH 5.21.200.136 - MESH EI	
IOTOD IW Offline	SNMP	
IW-MONITOR Disabled	SNMP	
FM-QUADRO	SNMP mode:	v3 ~
GENERAL SETTINGS	SNMP v3 username;	user
- general mode	Sivier vo username.	usei
- wireless radio	SNMP v3 password:	****
- antenna alignment and stats	Show SNMP v3 password:	
NETWORK CONTROL	Show Share vo password.	
- advanced tools	SNMP v3 authentication proto:	SHA 🗸
ADVANCED SETTINGS - advanced radio settings	SNMP v3 encryption:	AFC
- static routes	SNMP V3 encryption.	AES V
- allowlist / blocklist	SNMP v3 encryption passphrase:	*****
- multicast	Show SNMP v3 encryption passphrase;	
- snmp		_
- radius	Enable SNMP periodic trap:	
- ntp	Enable SNMP event trap:	
- ethernet filter	Engine ID:	Currently Unavailable
- I2tp configuration		
- vlan settings	NMS hostname:	192.168.0.100
- Fluidity	Notification period (minutes):	1
- misc settings	Roundation period (minutes).	•
- smart license		
MANAGEMENT SETTINGS	Reset	Save
- firmware upgrade		
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		
- logout	© 2023 Cisco and/or its affiliates. All rights reserved.	

Disable SNMP via GUI

I

FM-QUADRO	SNMP
GENERAL SETTINGS	SNMP
- general mode - wireless radio - antenna alignment and stats NETWORK CONTROL - advanced tools ADVANCED SETTINGS - advanced radio settings - static routes - allowlist / blocklist	SNMP mode: Disabled V Reset Save
- multicast - snmp	⊕ 10.115.11.116
- radius - ntp - ethernet filter	SNMP is disabled and all sensitive information and credentials have been cleared. Please re-configure all valid values to enable SNMP again.
- I2tp configuration - vlan settings	ок
- Fluidity - misc settings - smart license	

I



Multicast

- Overview of multicast, on page 81
- Configure multicast using GUI, on page 82
- Configure multicast using CLI, on page 83
- Delete multicast using CLI, on page 84
- Verify multicast configuration using CLI, on page 84

Overview of multicast

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



Note

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

Reserved IP address range for multicast protocols

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

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

Advantages of multicast configuration

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

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

Configure multicast using GUI

Before you begin

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

Procedure

e.
s.

- **Step 5** In the Add a new multicast route section, enter these details:
 - Multicast IP address in the Multicast Group field.
 - Netmask IP address in the Netmask field.
 - Destination IP address in the Destination Address field.

Note

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

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

Tip

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

Step 6 Click add.

Once you have successfully added a rule, the new multicast route appears in the Multicast routes section.

Step 7

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9165DH Configurator 5.127.234.140 - MESH END MODE				
W Service Offline	MULTICAST				
W Monitor Disabled		Multicast rou	utes		
QUADRO	List of multicast routes already present. You can manually add multicast routes.				
GENERAL SETTINGS	Multicast Group	Netmask	Destination Address		
- wireless radio		Add a new multica	ast route		
- antenna alignment and stats NETWORK CONTROL - advanced tools	Use these forms to add new static multicast routes. The Destination Address field accepts the following special values: - 5.255.255.255 is a wildcard address that indicates all units of the mesh network. - 5.0.0.0 is special address that forces each unit to send multicast traffic to the primary mesh end. This is particularly useful when the mesh ends fast-failover is enabled.				
ADVANCED SETTINGS • advanced radio settings • static routes • allowlist / blocklist • multicast	Multicast Group	Netmask	Destination Address add		

Configure multicast using CLI

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

Example:

```
Device#configure multicast group add 224.5.5.5 255.255.255.255 5.255.255
```



Note

This configuration takes effect only after the reboot.

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

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

Delete multicast using CLI

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

Example:

Device#configure multicast group delete 224.5.5.5 255.255.255.255 5.255.255



This configuration takes effect only after the reboot.

Verify multicast configuration using CLI

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

Device#show multicast configuration Multicast Group 224.5.5.5/255.255.255 Destination Address 5.255.255.255



Quality of Service

- Overview of Quality of Service, on page 85
- QoS configuration using CLI, on page 86
- Verify QoS configuration using CLI, on page 86
- 802.1p VLAN priority preference configuration using CLI, on page 87
- Verify 802.1p VLAN priority preference configuration using CLI, on page 87
- Configure CoS remapping using CLI, on page 87
- Verify CoS remapping using CLI, on page 88
- Configure QoS shaping using CLI, on page 88
- Verify QoS shaping using CLI, on page 89

Overview of Quality of Service

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

Traffic classification based on QoS

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

Advantages of QoS

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

QoS marking

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

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

802.1p

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

QoS shaping

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

QoS configuration using CLI

By default, QoS feature is disabled on the device.

Enable or disable QoS using CLI

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

Device#configure qos status enabled



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

Verify QoS configuration using CLI

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

Enabled:

```
Device#show qos

QoS: enabled

CoS map:

0 1 2 3 4 5 6 7

| | | | | | | | |

[ 0 1 2 3 4 5 6 7 ]
```

qos-shaping disabled qos-8021p disabled

Disabled:

Device#show qos QoS: disabled

802.1p VLAN priority preference configuration using CLI

Enable or disable 802.1p VLAN priority preference using CLI

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

Device#configure qos 8021p enabled



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

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

Verify 802.1p VLAN priority preference configuration using CLI

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

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

Configure CoS remapping using CLI

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

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

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

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

CoS 0 remains 0

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

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

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

C/

Important

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

Verify CoS remapping using CLI

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

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

Configure QoS shaping using CLI

Configure per-CoS rates

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

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



Note All eight bandwidths cannot be with zero.

Example:

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

In this example, configure bandwidth for each CoS value.

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

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

Enable or disable QoS shaping

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

Device#configure qos shaping enabled



Note

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

Verify QoS shaping using CLI

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

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

I



Frequency Scan

- Frequency scan, on page 91
- Overview of Fluidity frequency scan, on page 91
- Configure Fluidity frequency scan using CLI, on page 92
- Verify Fluidity frequency scan configuration using CLI, on page 94
- Overview of Fluidmax frequency scan, on page 94
- Verify Fluidmax frequency scan status using GUI, on page 95
- Configure Fluidmax frequency scan using CLI, on page 95
- Verify Fluidmax frequency scan configuration using CLI, on page 96

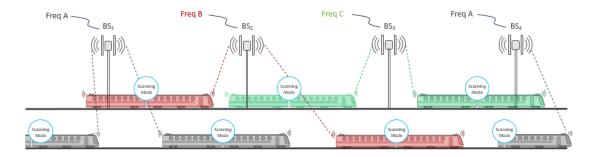
Frequency scan

URWB devices support two types of frequency scans:

- 1. Fluidity frequency scan
- 2. Fluidmax frequency scan

Overview of Fluidity frequency scan

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



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

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

Scanning can be performed in two modes:

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

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



Note

• Frequency scan is applicable only to fluidity vehicle devices, not to infrastructure devices.

• If the scan-periodic and scan-isolation parameters are set to zero, the frequency scan feature is disabled.

Configure Fluidity frequency scan using CLI

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

Clear the Fluidity frequency scan list using CLI

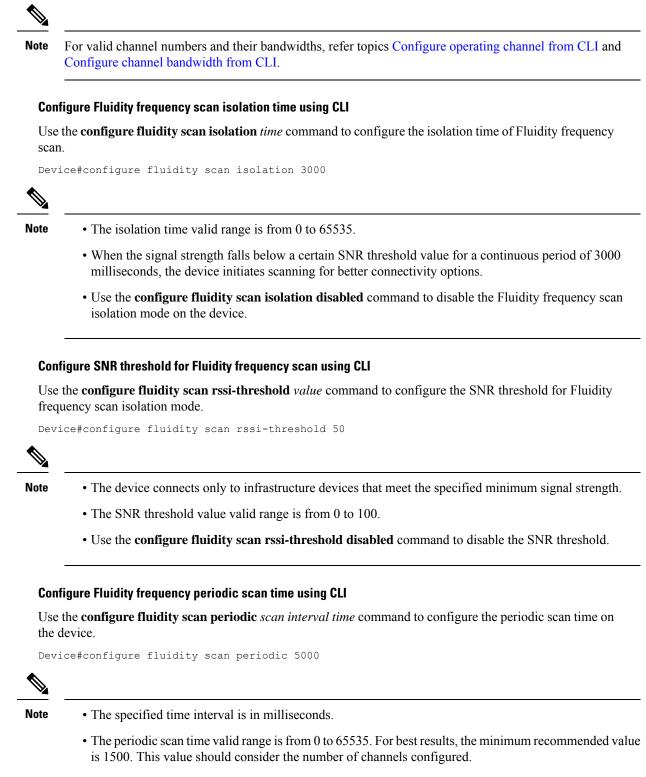
Use the **configure fluidity scan list clear** command to clear the Fluidity frequency scan list on the device.

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

Configure channels for Fluidity frequency scan list using CLI

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

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



• Use the **configure fluidity scan periodic disabled** command to disable the periodic frequency scan.

Onboard radios Fluidity frequency allocation using CLI

On the same channel

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

Device#configure frequency scan vehicle-frequency locked

On the separate channels

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

Device#configure fluidity scan vehicle-frequency open

Verify Fluidity frequency scan configuration using CLI

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

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

Overview of Fluidmax frequency scan

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

Verify Fluidmax frequency scan status using GUI

Before you begin

Note	

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

Procedure

- **Step 1** Launch the computer's web browser and enter the URL to open the configurator login page.
- **Step 2** Enter the username and password in the respective fields.
- Step 3 Click Login.

Once you successfully log into the GUI, the URWB configurator displays.

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

 Note
 Note

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

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9165DH 5.81.160.216 - MESH PC			
IW Service Offline IW Monitor Disabled				
GENERAL SETTINGS	ADVANCED RADIO SETTINGS			
- general mode - wireless radio	Radio 1			
- antenna alignment and stats	FluidMAX Management			
NETWORK CONTROL - advanced tools ADVANCED SETTINGS	Force the FluidMAX operating mode of this unit. If the operating mo ID can be set. If the FluidMAX Autoscan is enabled, the Secondary with the Primary with the same Cluster ID. In this case, the frequence disabled.	units will scan the frequencies to associate		
- advanced radio settings - static routes	Radio Mode: SECO	NDARY		
- allowlist / blocklist	FluidMAX Cluster ID: CiscoU	IRWB		
- snmp - radius	FluidMAX Autoscan: 🗹			

Configure Fluidmax frequency scan using CLI

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

Enable or disable Fluidmax frequency scan using CLI

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

Device#configure dot11Radio 1 mode fluidmax automatic-scan enable

 \otimes

Note

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

Configure threshold value for Fluidmax frequency scan using CLI

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

Device#configure dot11Radio 1 mode fluidmax threshold 90

Ø

Note

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

Verify Fluidmax frequency scan configuration using CLI

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

```
Device #show dot11Radio 1 config
Interface: enabled
Mode: fluidmax secondary
Frequency: 5200 MHz
Channel: 40
Channel width: 20 MHz
Antenna number: 2
TX power level: 2
TX power: 14 dBm
Antenna gain: 15 dBi
Maximum tx mcs: 9
High-efficiency: disabled
Maximum tx nss: 2
RTS protection: 512
guard-interval: 800 ns
ampdu max length: 255
distance: 3000 m
The ampdu Tx
priority 0: enabled
priority 1: enabled
priority 2: enabled
priority 3: enabled
priority 4: enabled
```

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

Fluidmax configuration

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

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

Passphrase: 58acle597fda4e37bc0c2472d8c8c69f AES encryption: disabled AES key-control: disabled Key rotation: disabled Key rotation timeout: 0(second)

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

I



Configuring and Validating Key Controller (Wireless Security)

• Configuring and Validating Key Controller (Wireless Security), on page 99

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)



Smart Licensing

• Smart Licensing Support, on page 101

Smart Licensing Support

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

I



Configuring Layer 2 Mesh Transparency

- Configuring Layer 2 Mesh Transparency, on page 103
- Configuring and Verifying Layer-2 Protocols Forwarding Using CLI, on page 104
- Configuring Layer-2 Protocol Forwarding using GUI, on page 106

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

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

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

Example:

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

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

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

Device# configure mpls ether-filter allow-list clear

Example:

. . .

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

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

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

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

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

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

Example:

Device# show mpls ether-filter

Ether-type Direction Description

0x8899 INGRESS ---

0x86DD INGRESS IPv6

Device# configure mpls ether-filter table clear

Cisco-81.160.136#show mpls ether-filter

Ether-type Direction Description

0x8899 INGRESS ---
```

```
Note
```

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

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

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

Example:

Device# configure mpls ether-filter ethernet-I forward

Deive# show mpls config

Ethernet Filter allow-list: 0x88F8 0x891D, ethernet-I forward \ldots

Device# configure mpls ether-filter ethernet-I block

Example:

Device# configure mpls ether-filter ethernet-I block

Device# show mpls config

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

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

Device# show mpls config

Example:

Device# show mpls config

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

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

```
Device# show mpls ether-filter table

Example:

Device# show mpls ether-filter table

Ether-type Direction Description

0x8899 INGRESS ---

0x86DD INGRESS IPv6
```

Configuring Layer-2 Protocol Forwarding using GUI

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

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

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

ULTRA RELIABLE WIRELESS BACKHAUL			URWB IW9165E Configu 1.160.244 - MESH END MOD		
IOTOD IW Offline	Ethernet Fi	iter			-
IW-MONITOR Disabled			Detected ethernet types		
FM-QUADRO	To add a detecte	d ethertype to the allowi	ist click on Add.		
GENERAL SETTINGS	Ethertype	Description	Direction	Action	
- general mode - wireless radio	0×8899		INGRESS	Add	
- antenna alignment and stats NETWORK CONTROL	0×86DD	IPv6	INGRESS	Add	I
- advanced tools ADVANCED SETTINGS - advanced radio settings - static routes		(Clear detected		l
- allowlist / blocklist		Allow all et	hernet types 🗌		
- multicast - snmp - radius		Allow Ethernet	t 1 protocols		I
- ntp			Allowed ethernet types		
- ethernet filter	To add a specific ethertype to the allowlist, insert it in the text field and click on Add.				
 I2tp configuration vlan settings 	Ethertype		Description	Action	
- Fluidity - misc settings	0x8892		PROFINET	Delete	I
- smart license MANAGEMENT SETTINGS	0x8204		QNX Qnet	Delete	
- remote access - firmware upgrade				Add	
- status - configuration settings - reset factory default		(Clear allowed		l
- reboot - logout			Save		•
	© 2023	Cisco and/or its affiliates	All rights reserved.		

hernet Fil add a detected hertype 8899 86DD	dethertype to the allowf Description IPv6 Allow all et	Detected ethemet types est disk on Add. Direction INGRESS INGRESS Clear detected hemet types	Action Add Add
nertype 8899	d ethertype to the allowf Description IPv6	ist click on Add. Direction INGRESS INGRESS Clear detected	Add
nertype 8899	Description IPv6 Allow all et	Direction INGRESS INGRESS Clear detected	Add
8899	IPv6	INGRESS INGRESS Clear detected	Add
	Allow all et	INGRESS Clear detected	
86DD	Allow all et	Clear detected	Add
		hernet types	
		incluct types	
	Allow Etherne	t 1 protocols 🗌	
		Allowed ethernet types	
add a specific	ethertype to the allowin	it, insert it in the text field and click or	Add
nertype		Description	Action
8892		PROFINET	Delete
			Add
	(Clear allowed	
		Save	
	ertype	ertype 1892	Clear allowed

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

1. In the ADVANCED SETTINGS, click ethernet filter.

The Ethernet Filter window appears.

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

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

ULTRA RELIABLE WIRELESS BACKHAUL			WB IW9165E Configur 60.244 - MESH END MODE	
OTOD IW Offline W-MONITOR Disabled	Configuration con	tains changes. Apply	these changes? Discard	d Review Apply
M-QUADRO	Ethernet Fil	Iter		
ENERAL SETTINGS		ſ	etected ethernet types	
general mode	To add a detected	d ethertype to the allowis	t click on Add.	
wireless radio antenna alignment and stats	Ethertype	Description	Direction	Action
antenna angrinent and stats IETWORK CONTROL advanced tools	0×8899	-	INGRESS	Add
DVANCED SETTINGS advanced radio settings static routes	0x86DD	IPv6	INGRESS	Add
allowlist / blocklist multicast			Clear detected	
snmp radius		Allow all eth	ernet types	
ntp ethernet filter 12tp configuration		Allow Ethernet		
vlan settings			Allowed ethernet types	
Fluidity	To add a specific	ethertype to the allowlist	insert it in the text field and click on	Add.
misc settings smart license	Ethertype	1	Description	Action
IANAGEMENT SETTINGS remote access				Add
firmware upgrade status configuration settings reset factory default			Clear allowed	
reboot logout			Save	

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 WIRELESS BACKHAUL			RWB IW9165E Configur 160.244 - MESH END MODE	ator
OTOD IW Offline	Ethernet Fi	ter		
W-MONITOR Disabled			Detected ethernet types	
FM-QUADRO	To add a detecte	d ethertype to the allow	rlist click on Add.	
GENERAL SETTINGS	Ethertype	Description	Direction	Action
general mode				
wireless radio		(
antenna alignment and stats			Clear detected	
NETWORK CONTROL				
- advanced tools		A 11 mm a 11 a	thernet types	
ADVANCED SETTINGS				
advanced radio settings		Allow Etherne	et 1 protocols	
- static routes				
allowlist / blocklist			Allowed ethernet types	
multicast				
snmp	To add a specific	ethertype to the allow	ist, insert it in the text field and click on i	Add.
radius	Ethertype		Description	Action
ntp	0x8892		PROFINET	Delete
ethernet filter	0,0092		FROFINET	Delete
- I2tp configuration	0x8204		QNX Qnet	Delete
vlan settings				Delete
Fluidity				Add
- misc settings				
- smart license				
MANAGEMENT SETTINGS			Clear allowed	
- remote access				
firmware upgrade				
- status			Save	
- configuration settings				
- 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 WIRELESS BACKHAUL			IW9165E Configura 4 - MESH END MODE	ator
IOTOD IW Offline 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 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 WIRELESS BACKHAUL			URWB IW9165E Config 31.160.244 - MESH END MOE	
IOTOD 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 wireless radio	0×8899		INGRESS	Add
- antenna alignment and stats NETWORK CONTROL	0x86DD	IPv6	INGRESS	Add
- advanced tools ADVANCED SETTINGS - advanced radio settings		(Clear detected	
- static routes - allowlist / blocklist		Allow all e	thernet types	
- multicast - snmp			et 1 protocols 🗹	
- radius - ntp			Allowed ethernet types	
ethernet filter	To add a specific	ethertype to the allowi	ist, insert it in the text field and click on	Add.
I2tp configuration vlan settings	Ethertype		Description	Action
- Fluidity - misc settings	0×8892		PROFINET	Delete
- smart license MANAGEMENT SETTINGS	0x8204		QNX Qnet	Delete
- remote access - firmware upgrade				Add
- status - configuration settings			Clear allowed	
- reset factory default - reboot				
- repoor			Save	

I



Configuring Multipath Operation

- Overview of MPO, on page 113
- Working Functionality of MPO, on page 113
- MPO Packet Duplication and Deduplication, on page 114
- Configuring MPO Features using CLI, on page 114
- Verifying MPO Features using CLI (MPO Monitoring), on page 115
- MPO Limitations, on page 117

Overview of MPO

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

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

Working Functionality of MPO

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

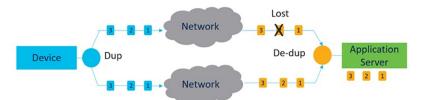
To protect the system from interference on wireless links, the control traffic is replicated over many MPLS tunnels, and copies of each packet are made and sent to various pathways. The receiver from the infrastructure side, receives more than one copy of the same packet after multiple copies of the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

MPO Packet Duplication and Deduplication

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

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

The process of Duplication and Deduplication as shown:



Duplication and Deduplication algorithm performs the following:

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

Configuring MPO Features using CLI

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

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

Device# configure fluidity mpo

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

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

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

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

Device# configure fluidity mpo status

disabled: Disable MPO duplication/deduplication.

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

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

Example:

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:

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 : 0 0 Lost

Device# show fluidity mpo statistics (on Mobile Primary unit) table-size 2: 8C:89:A5:83:EB:71 MAC address : 40:36:5A:15:C8:50 Tx-1 : 208 0 Tx-2 : 208 0 Rx-Accept-1 : 0 182 Rx-Accept-2 : 0 26 Rx-Drop-1 : 0 26 Rx-Drop-2 : 0 182 Lost-1-only : 0 0 Lost : 0 0

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

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

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

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

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

The output of the show fluidity network command:

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

unit 5.21.201.60 infrastructure meshend primary vehicles 4 total mobiles 5 infrastructure 1 backbone 0 meshend 5.21.201.60 Vehicle ID : + 85313616 Path : O 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

Ŋ

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

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

L

The output of the show eng-stats command:

```
Device# show eng-stats (on mobile primary unit)
. . . .
Fluidity role : primary
vehicle id : 0
static : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile : 4.21.200.80 [FC:58:9A:15:B9:13]
snr : 42
rssi : -54
dop : 40
chan : 132/40
handoff: 21.518258794
time : 2
Current:
ho seq: 7 pending: false age: 21.518303221 primary: 5.21.200.80
[0] - <3.21.201.60 - 4.21.200.80> status SUCCESS seq 6 id 0 age 59.469266332 rssi 42
[1] - <4.21.201.60 - 4.21.201.204> status SUCCESS seq 7 id 1 age 21.518317752 rssi 41
last primary: <3.21.201.60 - 4.21.200.80>
free ids: 7 6 5 4 3 2
current missing path mask: 1111110
HO Table
static : 3.21.201.60 [FC:58:9A:15:C7:D2]
mobile : 4.21.200.80 [FC:58:9A:15:B9:13]
rssi : 42
dop : 40
chan : 132/40
updated : 74
skip : 0
static : 4.21.201.60 [FC:58:9A:15:C7:D3]
mobile : 4.21.201.204 [FC:58:9A:15:E4:D3]
rssi : 41
dop : 40
chan : 100/40
updated : 18
skip : 0
rssi delta : 6 3
```

MPO Limitations

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

threshold : 35

· Load balancing

I



New Features in Cisco Catalyst IW Access Points, Release 17.12.1

The following URWB features are introduced in the release 17.12.1:

- Enabling and Disabling Wired Interface, on page 119
- Configuring Maximum Transmission Unit Settings, on page 120
- Configuring Fluidity Coloring, on page 120
- Configuring IW Monitor Management, on page 123
- Configuring URWB Telemetry Protocol, on page 125

Enabling and Disabling Wired Interface

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

Enabling or disabling wired interface using CLI

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

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

Example:

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

Error handling configuration

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

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

Verifying enabling and disabling wired interface using CLI

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

```
Device# #show wired <0-1> config
Example:
Device# show wired 0 config
WIRED0 status: enabled
Device# show wired 1 config
WIRED1 status: disabled
```

Configuring Maximum Transmission Unit Settings

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

Configuring MTU setting using CLI

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

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

Example:

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

Verifying MTU setting using CLI

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

```
Device# show wired mtu
```

Example:

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

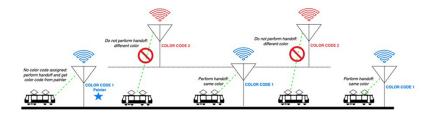
Configuring Fluidity Coloring

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

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

Fluidity Coloring Logic

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



The process of Fluidity coloring as follows:

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

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

Table 5: Fluidity Coloring Role

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

Configuring Fluidity Coloring using CLI

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

```
Device# configure fluidity color mode

Disabled: disable coloring

Enabled: enable coloring

Device# configure fluidity color value

WORD quoted list of colors from 1 to 7 or "p X" for painter (e.g. "1 2 6","4", "p 1").

"clear" to reset
```

Example (painter):

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

Example (non-painter):

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

Example (clear):

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

Verifying Fluidity Coloring using CLI

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

Device# #show fluidity config

Example (painter):

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

Example (non-painter):

Device# show fluidity config

Color: enabled, current: 3 4 5

Example (clear):

Device# show fluidity config

Color: enabled, current: 0 ...

Configuring Fluidity Coloring RSSI Threshold

. . .

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

Configuring Fluidity Coloring RSSI Threshold using CLI

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

Example:

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

Verifying Fluidity Coloring RSSI Threshold using CLI

Device# show fluidity config

Example:

Device# show fluidity config

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

Configuring IW Monitor Management

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

Table 6: IW Monitor features support in release 17.12.1

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

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

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

Release 17.12.1 provides following support for IW Monitor dashboard:

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

Detaching IW Monitor Management using CLI

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

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

Example:

Device# configure monitor detach

Verifying IW Monitor Management using CLI

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

Device# show monitor

Example:

Device# show monitor IW MONITOR: enabled Status: Connected

Configuring IW Monitor Management using Web UI

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

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9' 5.81.160.244 - Mi	
IOTOD IW Offline	GENERAL MODE	
IW-MONITOR Enabled	Genera	Mode
FM-QUADRO	Select MESH POINT mode if you are attaching an IP edg Cisco IOT IW9185E Series Access Point or if you are usi	ge device (i.e. network camera, encoder, etc.) to this ing this unit as a relay point in the mesh network.
GENERAL SETTINGS		o mesh point
- general mode	Mode:	O mesh end
- wireless radio		O gateway
- antenna alignment and stats		() galona,
NETWORK CONTROL	Radio-off:	
- advanced tools	Naulo-on.	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		
- radius	Default Gateway:	10.115.11.1
- ntp	Local Dns 1:	0000
- ethernet filter	Eocal Dils 1.	0.0.0.0
- I2tp configuration	Local Dns 2:	
- vlan settings		
- Fluidity		
- misc settings	Reset	Save
- 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	8.

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

L

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW916 5.81.160.244 - MES	
IOTOD IW Offline		
W-MONITOR Enabled	IW-MONITOR	
FM-QUADRO	IW-MONITOR of	connection info
	Server Host:	10.115.11.53
GENERAL SETTINGS	Status:	Connected
- general mode	States.	
wireless radio		
- antenna alignment and stats		
NETWORK CONTROL		
- advanced tools		Detach
ADVANCED SETTINGS		Detach
- advanced radio settings		
- static routes		
- allowlist / blocklist		
- multicast		
- snmp		
- radius		
- ntp		
- ethernet filter		
- 12tp configuration		
- vlan settings		
- Fluidity		
- misc settings		
- smart license		
MANAGEMENT SETTINGS		
- remote access		
- firmware upgrade		
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		

Configuring URWB Telemetry Protocol

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

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

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

The telemetry UDP packet contains the following information:

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

Configuration of URWB Telemetry Protocol Using CLI

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

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

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

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

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

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

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

Example:

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

Ì

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

To verify telemetry configuration, use the following CLI command:

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

Live Configuration of URWB Telemetry Protocol Using CLI

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

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

Example:

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

Example (telemetry export after server configuration):

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



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

I



LED Pattern for Catalysts IW9167 and IW9165

- LED Pattern for Catalyst IW9167, on page 129
- LED Pattern for Catalyst IW9165, on page 130

LED Pattern for Catalyst IW9167

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

Table 7: Definition of Booting LED Pattern

Events	LED State
Boot loader status sequence:	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 8: Definition of URWB OS LED Pattern

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

LED Pattern for Catalyst IW9165

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

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

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

RSSI LED

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

Table 10: RSSI LEDs

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

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

Table 11: URWB LED function for the Catalyst IW9165E

LED Function Label	Color/State	Description (Default = off)	
System Status	Tricolor RGB	Indicates varies system status	
RSSI	Yellow or Green	RSSI < - 86 dBm: yellow - 86 dBm =< RSSI =< - 81 dBM: blinking green RSSI > - 81 dBm: green	
	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 12: URWB LED function for the Catalyst IW9165D

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

I



Fixed domains and country codes (ROW)

- Configuring and Verifying Regulatory Domain from CLI, on page 133
- Configuring Regulatory Domain from GUI, on page 134
- Supporting Fixed Domains and Country Codes (ROW), on page 137

Configuring and Verifying Regulatory Domain from CLI

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

Device# configure countrycode [countrycode]

Example:

Configure countrycode GB

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



```
Note
```

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

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

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

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

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

Example:

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

Configuring Regulatory Domain from GUI

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

- 1. Click the wireless radio under GENERAL SETTINGS in the left-hand settings menu.
- 2. For ROW domain, if the country code is not selected, the following pop-up appears:

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.21.200.136 - MESH END MODE			
IOTOD IW Cloud-Manage	Select operating country			
FM-QUADRO GENERAL SETTINGS - general mode	Please select ROW region operatin immediately rebooted on confirmation be applied.			g "[apex] "[double apex] `[backtick] dentifies your network. It MUST be
- wireless radio - antenna alignment and stats	✓ Korea United Arab Emirates			
NETWORK CONTROL	United Kingdom Vietnam	Co	nfirm	eed to be operating on the same
- advanced radio settings		Radio 1 Setti	ngs	
- static routes - allowlist / blocklist	Role:	Fluidmax Primary	~	
- multicast - snmp	Frequency (MHz):	×		
- radius - ntp	Channel Width (MHz):	~		
- I2tp configuration		Radio 2 Setti	ngs	
- vian settings - Fluidity - misc settings - smart license MANAGEMENT SETTINGS - remote access - remote access - status - status - reboot - logout	Role: Frequency (MHz): Channel Width (MHz):	Disabled V	~	
	© 2023 Cisco and/or its affiliat	tes. All rights reserved.		

3. To select a country code, click the pop-up displays in the below image then it redirects to Web UI wireless section for selecting country code. In the **Wireless Settings** section, choose country from drop-down list. A confirmation pop-up appears.

ULTRA RELIABLE WIRELESS BACKHAUL	Cisco	Cameroon Chile China Colombia Costa Rica	ator
IOTOD IW Offline	WIRELESS RADIO	Ecuador Egypt	
IW-MONITOR Disabled FM-QUADRO	"Shared Passphrase" is an alphan \$[dollar] =[equal] \[backslash] and the same for all the Cisco URWB (Fiji Ghana Hong Kong	[apex] "[double apex] '[backtick] intifies your network. It MUST be
GENERAL SETTINGS - general mode - wireless radio	Shared Passphrase:	India Iraq	
- antenna alignment and stats	Country:	✓ Korea	
NETWORK CONTROL - advanced tools ADVANCED SETTINGS	In order to establish a wireless cor frequency.	Kuwait Libya Macau	id to be operating on the same
 advanced radio settings static routes 	Role:	Malaysia Mexico	
- allowlist / blocklist - multicast	Frequency (MHz):	Morocco Pakistan	
- snmp - radius	Channel Width (MHz):	Panama	
- ntp		Peru	
- ethernet filter - I2tp configuration	Role:	Philippines Qatar	
- vlan settings - Fluidity		Saudi Arabia Singapore	
- misc settings		South Africa	
- smart license MANAGEMENT SETTINGS		Sri Lanka	
- remote access		Taiwan Thailand	
- firmware upgrade		Trinidad	
- status		Tunisia	
- configuration settings		Turkey	
- reset factory default - reboot		Ukraine	
- logout		United Arab Emirates United Kingdom	
	© 2023 Cisco and/or its affili	Uruguay Vietnam	

- 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 WIRELESS BACKHAUL	Cisco URWB IW9167EH Configurator 5.246.1.104 - MESH POINT MODE		
OTOD IW Offline	STATUS		
W-MONITOR Disabled	Device: Cisco Catalyst IW9167E Heavy Duty Access Point		
GENERAL SETTINGS	Name: unset ID: 5.246.1.104		
general mode	Serial: KWC2702000L		
•	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		
- advanced radio settings	MAC address: 40:36:5a:16:01:68 Configured MTU: 1530		
	WIRED0		
- static routes	Status: up		
- allowlist / blocklist	Speed: 100 Mb/s		
- snmp	Duplex: full MTU: 1530		
- radius	WIRED1		
- ntp	Status: down		
- ethernet filter			
- I2tp configuration	WIRELESS SETTINGS Passphrase: CiscoURWB-142		
	Operating region: ROW		
- vlan settings	Country: GB		
- Fluidity			
- misc settings	Radio 1 Interface: enabled		
MANAGEMENT SETTINGS	Mode: fixed infrastructure		
- remote access	Frequency: 5500 MHz		
- firmware upgrade	Channel: 100		
- status	Channel Width: 80 MHz Current tx power: -96 dBm		
	Current tx power level: 1		
- configuration settings	Antenna gain: not selected		
 reset factory default 	Antenna number: 2 Radio Mode: csma/ca		
- reboot	Radio Mode: csma/ca Maximum link length: 3 km		
- logout	maantan min longat. o lan		
	Radio 2		
	Interface: disabled		
	Mode: fixed infrastructure Frequency: 5500 MHz		
	Channel: 100		
	Channel Width: 80 MHz		
	Current tx power: -96 dBm		

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

ULTRA RELIABLE WIRELESS BACKHAUL		URWB IW9167EH Configurator 21.201.88 - MESH POINT MODE
IOTOD IW Offline	WIRELESS RADIO	
IW-MONITOR Disabled		Wireless Settings
GENERAL SETTINGS		meric string or special characters excluding "apex) "[double apex) [backtick] whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be nits belonging to the same network.
- wireless radio	Shared Passphrase:	CiscoURWB
- antenna alignment and stats NETWORK CONTROL		nection between Cisco URWB units, they need to be operating on the same
- advanced tools		Radio 1 Settings
ADVANCED SETTINGS	Polo	Fixed
- advanced radio settings	Role.	Fixed
- static routes	Frequency (MHz):	5260
- allowlist / blocklist		
- snmp - radius	Channel Width (MHz):	20
- ntp		Radio 2 Settings
- ethernet filter	Data	Fixed
- I2tp configuration	Role:	Fixed
- vian settings	Frequency (MHz):	5180
- Fluidity		
- misc settings	Channel Width (MHz):	80
MANAGEMENT SETTINGS		
- remote access		
- firmware upgrade		Reset Save
- status		
- configuration settings		
- reset factory default		
- reboot		
- logout		
	© 2023 Cisco and/or its affilia	tes. All rights reserved.

The below image shows the configuration of regularity domain from GUI:

	Cisco URWB IW9167EH Configurator 5.21.201.88 - MESH POINT MODE
WIRELESS BACKHAUL	3.21.201.00 - WEST FORT WODE
	Operating Mode: Mesh Point
OTOD IW Offline	Uptime: 4 days, 16:23 (hh:mm)
W-MONITOR Disabled	Firmware version: 8.8.1.10
	DEVICE SETTINGS
ENERAL SETTINGS	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	WIREDO
ETWORK CONTROL	Status: up Speed: 1000 Mb/s
advanced tools	Duplex: full
	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
	Interface: enabled
ntp	Mode: fixed infrastructure
ethernet filter	Frequency: 5260 MHz
12tp configuration	Channel: 52
- vlan settings	Channel Width: 20 MHz Current tx power: 25 dBm
Fluidity	Current tx power level: 1
- misc settings	Antenna gain: not selected
	Antenna number: 2
MANAGEMENT SETTINGS	Radio Mode: csma/ca Maximum link length: 3 km
remote access	Maximum ink lengur. 5 km
firmware upgrade	Radio 2
status	Interface: disabled
- configuration settings	Mode: fixed infrastructure
· reset factory default	Frequency: 5180 MHz Channel: 36
	Channel Width: 80 MHz
- reboot	Current tx power: 19 dBm
- logout	Current tx power level: 1
	Antenna gain: not selected Antenna number: 2
	Radio Mode: csma/ca
	Maximum link length: 3 km
	DIAGNOSTIC TOOL

Supporting Fixed Domains and Country Codes (ROW)

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

Catalyst IW9167E Supported Fixed Domains

Domain	Indoor Deployment Support
А	No
В	*
Е	Yes
F	No
Q	No
Z	No

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

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
IW9167EH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9167E Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support
KR (Korea)	No
VN (Vietnam)	*
GB (Great Britain)	Yes
IN (India)	No
PE (Peru)	No
PH (Philippines)	No

Note Only the listed country codes can be selected using CLI or Web UI.

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

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
IW9167EH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9165E Supported Fixed Domains

Indoor Deployment Support
Yes
*
Yes
Yes

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

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
IW9165E supports indoor deployment on domain A,E,Z and ROW(GB) only.
```

Catalyst IW9165E Supported Country Codes (ROW)

	Domain ROW Country Code	Indoor Deployment Support	
	GB (Great Britain)	Yes	
Note	Only the listed country codes can be selected using CLI or Web UI.		

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

Configuration for error handling using CLI

Example:

L

```
Device# configure wireless indoor-deployment enable
IW9165E supports indoor deployment on domain A,E,Z and ROW(GB) only
```

Catalyst IW9165D Supported Fixed Domains

Indoor Deployment Support
No
*
Yes
No

Note

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

Configuration for error handling using CLI

Example:

```
Device# configure wireless indoor-deployment enable
IW9165DH supports indoor deployment on domain E and ROW(GB) only.
```

Catalyst IW9165DH Supported Country Codes (ROW)

Domain ROW Country Code	Indoor Deployment Support	
GB (Great Britain)	Yes	
Only the listed country codes can be selected using CLI or Web UI.		

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

Configuration for error handling using CLI

Example:

Device# configure wireless indoor-deployment enable IW9165DH supports indoor deployment on domain E and ROW(GB) only.

I

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

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

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

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

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

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

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

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

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

© 2023 Cisco Systems, Inc. All rights reserved.