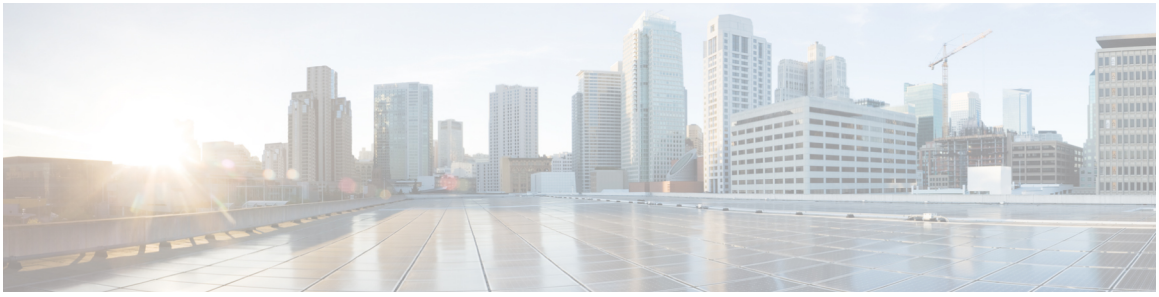


Cisco Ultra-Reliable Wireless Backhaul for Catalyst IW Access Points, Software Configuration Guide, Release 17.18.x

First Published: 2025-08-08

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 xi

About this Guide xi

Related Documentation xi

Communications, Services, and Additional Information xi

CHAPTER 1

Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1

Overview of Cisco Catalyst IW9167E and IW9165 Access Points 1

CHAPTER 2

Initial configuration of the unit in Provisioning Mode 3

Initial configuration of devices in provisioning mode 3

Provisioning mode behavior 3

Verify provisioning mode using GUI 4

Verify provisioning mode using CLI 6

Configure the fallback address 7

Troubleshoot connectivity 8

Reset the device to factory default using GUI 9

Reset the device to factory default using CLI 11

Reboot the device using GUI 11

Save and RESTORE the device SETTINGS 12

Configure GENERAL SETTINGS 13

Connect to the access point console port 15

CHAPTER 3

SSH and Web UI Access 17

Enable SSH access 17

Disable SSH access 17

Enable web UI access 18
Disable web UI access 18

CHAPTER 4 Upgrade the Device using GUI 19
Upgrade the device using GUI 19

CHAPTER 5 Upgrade the Device using TFTP 21
Device Upgrade using TFTP 21
Automatic Device Upgrade using TFTP 21
Configuring Manifest File on the TFTP Server 22
Manifest File Format 22
Direct Device Upgrade using TFTP 23
TFTP Device Upgrade using CLI 24

CHAPTER 6 Smart Licensing 27
Smart licensing support 27

CHAPTER 7 Fixed domains and country codes (ROW) 29
Fixed domains and country codes for Catalyst APs (ROW) 29
Supported fixed domains for Catalyst IW9167E 29
Supported country codes for Catalyst IW9167E 30
Supported fixed domains for Catalyst IW9165E 31
Supported country codes for Catalyst IW9165E 32
Supported fixed domains for Catalyst IW9165DH 33
Supported country codes for Catalyst IW9165DH 34
Configure and verify country code using CLI 35
Configure country code using GUI 36

CHAPTER 8 Indoor Deployment 41
Configuring Guard Interval for HE 41

CHAPTER 9 LED Pattern for Catalysts IW9167 and IW9165 43
LED pattern for Catalyst IW9167 43

LED pattern for Catalyst IW9165 44

CHAPTER 10 IPv6 Support 47

IPv6 Support 47
IPv6 address types 47
IPv6 limitations on the AP 48
Enable or disable IPv6 using CLI 48
Enable or disable IPv6 RA autoconfig using CLI 48
Configure static IPv6 address with eui-64, gateway, and DNS server address 49
Verify static IPv6 address with eui-64, gateway, and DNS server address 49
Configure static IPv6 address without eui-64, gateway, and DNS server address 50
Verify static IPv6 address without eui-64, gateway, and DNS server address 50
Configure static IPv6 address with EUI-64 50
Verify static IPv6 address with eui-64 51
Configure static IPv6 address without eui-64 51
Verify static IPv6 address without eui-64 51
Clear the IPv6 gateway and DNS servers configuration 51
Verify the cleared IPv6 gateway and DNS servers configuration 52
Enable and configure static IPv6 using GUI 52
Verify static IPv6 using GUI 54

CHAPTER 11 FIPS Certification 55

FIPS certification 55
Enable or disable FIPS mode 55
Verify FIPS mode using CLI 56

CHAPTER 12 URWB Operation Mode 57

URWB operation mode 57
Identify Software Images from CLI 57
Reset button settings 58
Configure image conversion 58
Access the GUI 59
Verify URWB Catalyst IW9167E configuration using GUI 60
Commit CLI configuration 60

Configure IW Service Cloud-Managed and Offline Mode using CLI 61
Configure password after first login using CLI 62
Configure IW Service using GUI 64

CHAPTER 13 URWB Radio Mode 65
Configure URWB radio mode 65
Configure radio-off mode from CLI 66
Configure radio mode for URWB from CLI 67
Configure AMPDU using CLI 68
Configure frequency from CLI 69
Configure maximum modulation coding scheme index from CLI 69
Configure maximum number of spatial streams index from CLI 70
Configure Rx-SOP threshold from CLI 70
Configure RTS mode from CLI 71
Configure WMM mode from CLI 71
Configure NTP from CLI 72
Configure NTP using GUI 73
Validate radio mode for URWB 74
Configure radio-off mode using GUI 74
Configure Radio mode using GUI 75

CHAPTER 14 IW Service Cluster 81
IW Service cluster 81
Configure IW Service Cluster from CLI 81
Verify IW Service Cluster 82

CHAPTER 15 Wired Interface 83
Enable or disable wired interfaces 83
Configure maximum transmission unit settings 84

CHAPTER 16 Radio Antenna Settings 85
Radio antenna settings 85
Configure antenna gain 85
Configure transmit and receive antennas 86

Configure transmission power 86
Validate URWB individual antenna RSSI values 87

CHAPTER 17 Radio Channel and Bandwidth 89
4900-4990 MHz frequency support for US and canada with license enforcement 89
Enable 4900-4990 MHz frequency bands 90
5855-5935 MHz frequency support 90
Restrictions for wireless frequency configuration 91
Enabling 5855-5935 MHz frequency bands 91
Configure operating channel and bandwidth using CLI 92
Validate operating channel and bandwidth using CLI 94
Configure operating channel and bandwidth using GUI 95
UNII-3 band with DFS support 95
How DFS works 96
Benefits 96
Restrictions for UNII-3 band with DFS support 96
Configure DFS channel 97
Configure operating channel using CLI 97
Configure channel bandwidth from CLI 98
Validate operating channel and bandwidth from CLI 99
Configure radio channel and bandwidth from GUI 99
Configure VLAN SETTINGS 101
Rules for packet management 102
Configure Fluidity using GUI 103
Configure fluidity using CLI 107
Configure fluidity role using CLI 108
Configure fluidity coloring 108

CHAPTER 18 High Efficiency (802.11 ax) 113
Configure and validate high efficiency 113
Configure global gateway using GUI 114
Configuring Guard Interval for HE 116

CHAPTER 19 Roaming Parameters 119

Packet retries limitation 119
Configure maximum retry limit for packet retransmissions using CLI 119
Verify maximum retry limit for packet retransmissions using CLI 120

CHAPTER 20 Key Controller (Wireless Security) 121
Key controller wireless security 121
Configure key controller from CLI 121
Validate key controller from CLI 122

CHAPTER 21 SNMP 123
Simple network management protocol 123
Configure SNMP from CLI 123
Validate SNMP from CLI 126
Configure SNMP version v2c using GUI 126
Configure SNMP version v3 using GUI 128

CHAPTER 22 URWB Telemetry Protocol 131
URWB telemetry protocol 131
Configure URWB Telemetry Protocol using CLI 131
Live Configuration of URWB Telemetry Protocol using CLI 132
Configure GNSS Telemetry Protocol using CLI 133

CHAPTER 23 IW Monitor Management 135
IW MONITOR management 135
Configure IW MONITOR management using CLI 136
Configure IW MONITOR management using GUI 136

CHAPTER 24 Multicast 139
Multicast 139
Configure Multicast using GUI 140
Configure multicast using CLI 141
Delete multicast using CLI 142
Verify multicast configuration using CLI 142

CHAPTER 25 **Quality of Service** 143

Quality of service 143
Configure QoS using CLI 144
Verify QoS configuration using CLI 145
Configure 802.1p VLAN priority preference using CLI 145
Verify 802.1p VLAN priority preference configuration using CLI 146
Configure CoS remapping using CLI 146
Verify CoS remapping using CLI 147
Configure QoS shaping using CLI 147
Verify QoS shaping using CLI 148

CHAPTER 26 **Frequency Scan** 149

Frequency scan 149
Fluidity frequency scan 149
Configure fluidity frequency scan using CLI 150
Verify fluidity frequency scan configuration using CLI 152
Fluidmax frequency scan 152
Verify fluidmax frequency scan status using GUI 153
Configure fluidmax frequency scan using CLI 154
Verify fluidmax frequency scan configuration using CLI 154

CHAPTER 27 **Network Address Translation** 157

Network address translation 157
Downstream data flow using NAPT for AGVs 158
Assign port numbers using NAPT for AGVs 159
NAPT rule on AP 160
Upstream data flow using SNAT for AGVs 160
Configure NAPT using CLI 161
NAPT configuration example 162
Configure SNAT using CLI 162
SNAT configuration example 163
Delete NAT rule using CLI 163
Delete all NAT rules 164

Verify NAT configuration using CLI 164
Verify NAT translations using CLI 164

CHAPTER 28 Layer 2 Mesh Transparency 167
Layer 2 mesh transparency 167
Configure and verify Layer-2 protocols forwarding using CLI 168
Configure Layer-2 protocol forwarding using GUI 169

CHAPTER 29 Multipath Operation 175
Multipath operation 175
MPO working functionality 176
MPO packet duplication and deduplication 176
MPO limitations 176
Configure MPO features using CLI 177
Verify MPO features using CLI (MPO monitoring) 178

CHAPTER 30 Fluidmax Topology 181
Fluidmax topology configuration and validation 181
Configure point to multipoint topology from CLI 182
Configuration examples: Point to multipoint topology 183
Validate point to multipoint topology using CLI 184

CHAPTER 31 Point-to-Point Relay Topology 187
Configure and validate point-to-point relay topology 187
Configure point-to-point relay topology from CLI 188
Validate point to point relay topology from CLI 189

CHAPTER 32 Mixed Mode (Fixed infrastructure + Fluidity) Topology 191
Mixed mode topology 191
Configure mixed mode topology from CLI 192
Configuration examples: mixed mode topology 193
Validate mixed mode topology from CLI 193

CHAPTER 33 **Fast Failover** 195

Fast failover 195

Configure and validate fast failover 195

Configure fast failover from CLI 196

Validate fast failover from CLI 197

CHAPTER 34 **Network Address Translation** 199

Network address translation 199

Downstream data flow using NAPT for AGVs 200

Assign port numbers using NAPT for AGVs 201

NAPT rule on AP 202

Upstream data flow using SNAT for AGVs 202

Configure NAPT using CLI 203

NAPT configuration example 204

Configure SNAT using CLI 204

SNAT configuration example 205

Delete NAT rule using CLI 205

Delete all NAT rules 206

Verify NAT configuration using CLI 206

Verify NAT translations using CLI 206



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 xi
- Related Documentation, on page xi
- Communications, Services, and Additional Information, on page xi

About this Guide

This guide details the configuration of the URWB mode of operation for the Cisco Catalyst IW9167E, IW9165E, and IW9165D access points. UWRB is supported as part of the Unified Industrial Wireless (UIW) software. UIW Release 17.16.1 introduces these new features:

- 4900-4990 MHz Frequency Support for US and Canada with License Enforcement
- Additional Country Codes Support
- Network Address Translation

Related Documentation

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

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

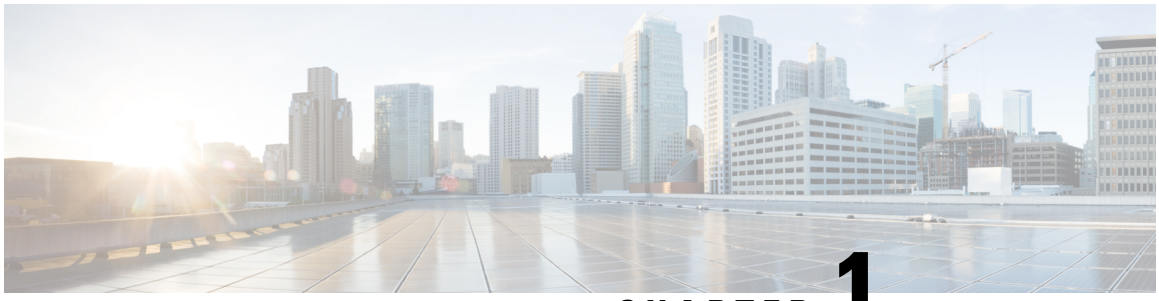
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking,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

Cisco Bug Search Tool

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

Documentation Feedback

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



CHAPTER 1

Overview of Cisco Catalyst IW9167E and IW9165 Access Points

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

Overview of Cisco Catalyst IW9167E and IW9165 Access Points

The Cisco Catalyst IW9167E and IW9165 series are industrial-grade access points designed to deliver secure, high-throughput wireless connectivity and ultra-reliable wireless backhaul (URWB) for mission-critical applications.

- Support for Wi-Fi 6E and tri-band operation.
- Flexible operational modes including URWB, CAPWAP, and WGB.
- Ruggedized hardware designs suitable for industrial and outdoor deployments.

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.

Cisco Catalyst IW9165

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

The Catalyst IW9165 series is available in two models:

- Catalyst IW9165E Rugged Access Point and Wireless Client

- Catalyst IW9165D Access Point

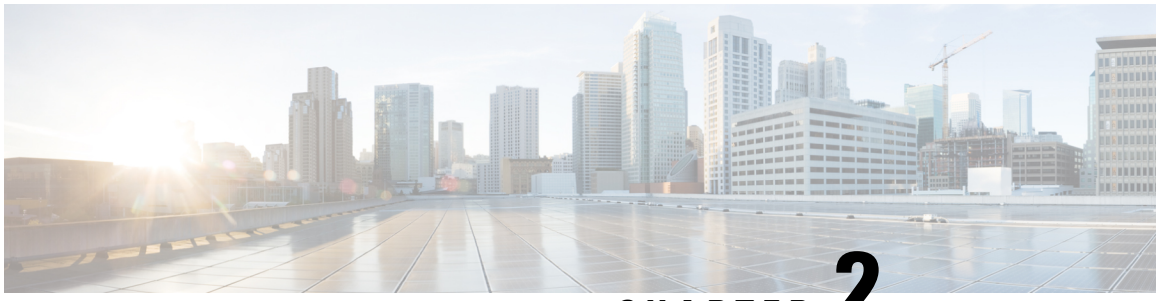
Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

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

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

Cisco Catalyst IW9165D Access Point

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



CHAPTER 2

Initial configuration of the unit in Provisioning Mode

- Initial configuration of devices in provisioning mode, on page 3
- Provisioning mode behavior, on page 3
- Verify provisioning mode using GUI, on page 4
- Verify provisioning mode using CLI, on page 6
- Configure the fallback address, on page 7
- Troubleshoot connectivity, on page 8
- Reset the device to factory default using GUI, on page 9
- Reset the device to factory default using CLI, on page 11
- Reboot the device using GUI, on page 11
- Save and RESTORE the device SETTINGS, on page 12
- Configure GENERAL SETTINGS, on page 13
- Connect to the access point console port, on page 15

Initial configuration of devices in provisioning mode

Initial configuration of devices in provisioning mode is a process that

- allows access points with no configuration to receive initial configuration from Industrial Wireless (IW) Service
- enables network configuration using DHCP when network connectivity exists, and
- provides local configuration options through GUI or CLI when network connectivity is unavailable.

Note From UIW Release 17.16.1, IoT OD IW changes to IW Service.

Provisioning mode behavior

This section provides provisioning mode behavior, default access credentials, DHCP addressing behavior, fallback IP behavior, cloud connectivity requirements, and CLI examples.

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

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

Default login credentials

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

- Username: Cisco
- Password: Cisco

DHCP addressing and IW service cluster selection

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

Static IP requirement for normal operation

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

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

Verify provisioning mode using GUI

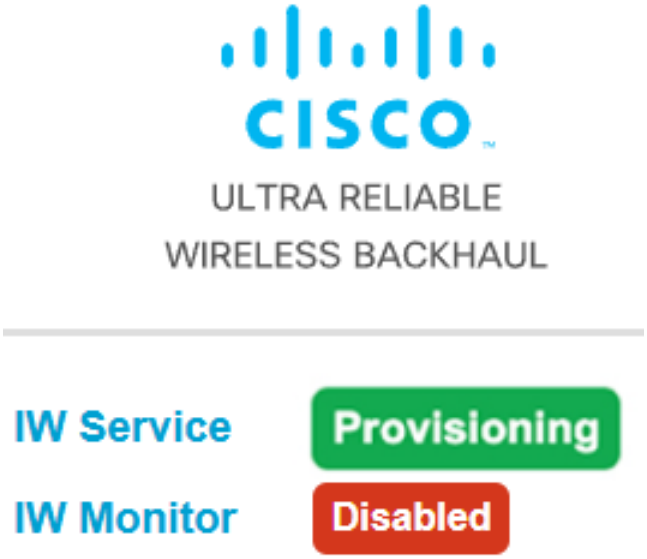
These steps show how to verify if the device is in provisioning mode:

Procedure

Step 1 To verify if the device is in provisioning mode, go to the device configurator interface. The status is shown as **Provisioning**:

Example:

Figure 1: Provisioning mode page



Step 2 If the status is shown as **Cloud-Managed** or **Offline**, choose either of these options:

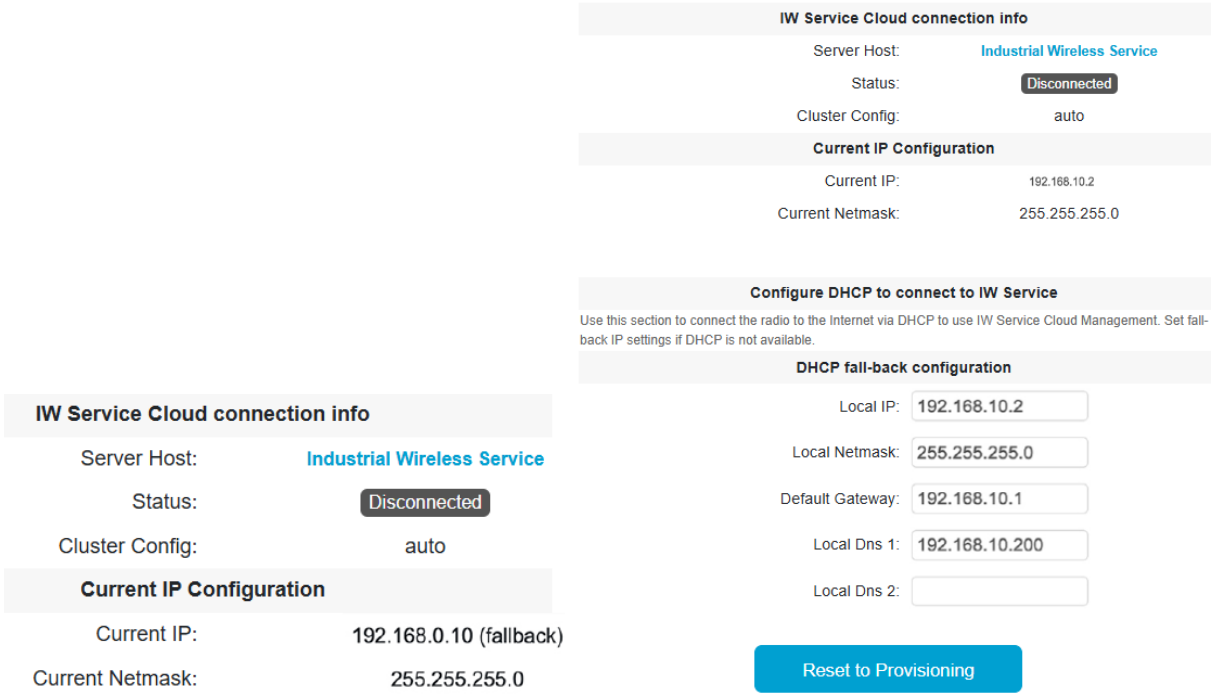
- To configure a new device, revert the wireless device to provisioning mode and reset the device, see Reset the device to factory default using GUI, on page 9.
- To change the connection settings with current configuration, see Configure GENERAL SETTINGS, on page 13.

Step 3 If the device is in provisioning mode, the device configurator interface is shown:

The device's status and LEDs blink continuously and LEDs repeat this cycle until the device either enters a fallback condition, or enters **Cloud-Managed**, or **Offline** mode. To know more about LED status, see LED pattern for Catalyst IW9165, on page 44 or LED pattern for Catalyst IW9167, on page 43.

Example:

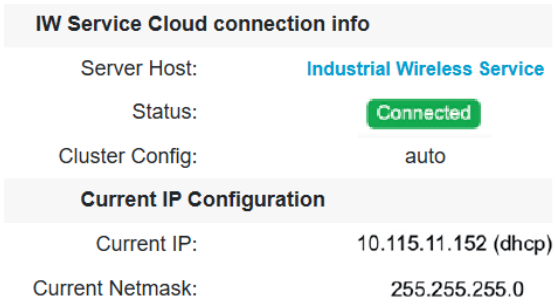
Figure 2: Cloud connection info



If the connection to Industrial Wireless (IW) Service is successful, the cloud connection info status is shown as **Connected**.

Example:

Figure 3: Cloud connection info



Verify provisioning mode using CLI

These steps show how to verify if the device is in provisioning mode:

Procedure

Use the **show iw-service status** command to verify whether the device is in provisioning mode.

Example:

```
Device#show iw-service status
  IW Service mode: Provisioning
  Status: Connected
```

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

```
Device# show ip
 IP:             192.168.0.10
 Network:        255.255.255.0
 Gateway:
 Nameservers:

 DHCP Address (PROVISIONING Mode):
 IP:             10.0.0.2
 Network:        255.255.255.0
 Gateway:        10.0.0.1
 Nameservers:    8.8.8.8

 Fallback Address (PROVISIONING Mode):
 IP:             169.254.201.72
 Network:        255.255.0.0
```

This example shows the device in provisioning mode failed to retrieve the IP address from the DHCP server and using the default fallback IP address 192.168.0.10:

```
Device# show ip
 IP:             192.168.0.10
 Network:        255.255.255.0
 Gateway:
 Nameservers:

 DHCP Address (PROVISIONING Mode):
 IP:             192.168.0.10
 Network:        255.255.255.0
 Gateway:
 Nameservers:    127.0.0.1

 Fallback Address (PROVISIONING Mode):
 IP:             169.254.201.72
 Network:        255.255.0.0
```

Configure the fallback address

This task ensures that the device remains reachable on the network by using either the default fallback IP address or a user-configured static IP address.

This task is used in provisioning mode to assign a fallback IPv4 address configuration to the device when DHCP is unavailable or does not provide an address.

Procedure

Use the **configure ip address ipv4** *static-IP-address static-netmask default-gateway-ip* [*dns-ip*] command to configure fallback address.

Note
In provisioning mode, the IP address, netmask, default gateway, primary DNS, and secondary DNS can be configured using the IP command.

The device automatically sets the fallback address (192.168.0.10 by default) or the configured IP address if it does not receive an address from the DHCP server.

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
```

Troubleshoot connectivity

This task guides you through basic connectivity checks, including Ethernet, DNS resolution, HTTPS access on TCP port 443, and fallback IP configuration, so the device can reconnect or remain reachable for offline setup.

This task helps you when a device cannot connect to IoT Operations Dashboard Industrial Wireless Service or cannot reach the network while in provisioning mode.

Procedure

Step 1 If the device fails to connect to Industrial Wireless (IW) Service, verify these items to reach Industrial Wireless (IW) Service:

a. Check if the ethernet cable leading to the device is connected correctly.

b. Check if the local DNS server can fix the IP address of Industrial Wireless (IW) Service cloud server and if the address can be reached.

c. Check if access point uses an outbound HTTPS connection on tcp/443 for these domains:

- device.ciscoiot.com
- US.ciscoiot.com
- EU.ciscoiot.com

d. If Industrial Wireless (IW) Service is still offline, perform a local (offline) configuration using the device's configurator interface.

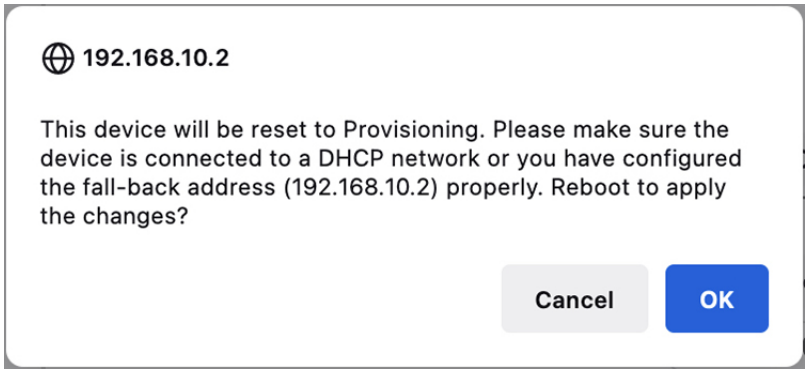
Step 2 If the device fails to connect to the network in provisioning mode, follow these steps:

a) Enter alternative **Local IP**, **Local Netmask**, **Default Gateway**, **Local DNS 1**, and **Local DNS 2** values as needed, using Industrial Wireless (IW) Service image and click the **Save fallback IP**.

A reboot confirmation pop-up appears:

Example:

Figure 4: Reboot confirmation popup



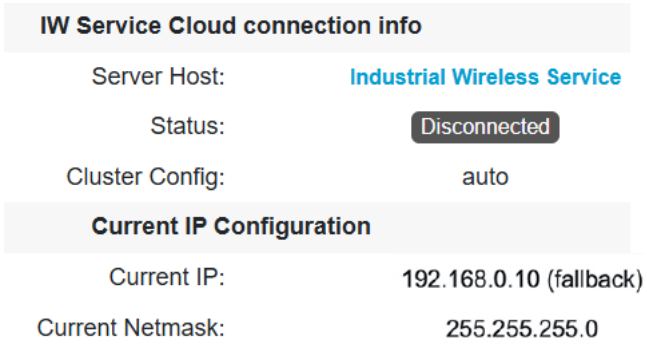
b) Click **OK** or **Reset** to go back to Industrial Wireless (IW) Service and adjust the settings.

- Once you click **OK**, the device reboots and remains in provisioning mode.
- The device attempts to connect to the network using the new connection values.

If the device fails to connect to the network using the **DHCP** settings, **IW Service Cloud connection Status** is shown as **Disconnected**.

Example:

Figure 5: Connection Status



Reset the device to factory default using GUI

Reset the device to factory default to revert all device configuration SETTINGS, including the device IP address and administrator password, to factory defaults.

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.

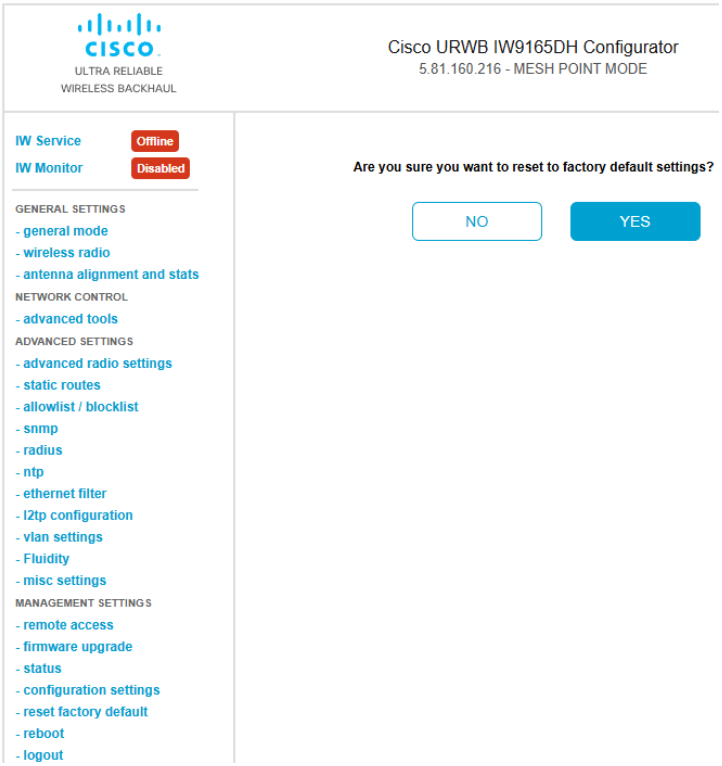
Note A hard reset reverts all device configuration SETTINGS, including the device IP address and administrator password to factory defaults. Instead if you want to reboot the device, see Reboot the device using GUI, on page 11.

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.

To reset of the device configuration, use the steps:

Procedure

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



Step 2 Click **YES** in the confirmation pop-up window. To abort the factory reset, click **NO**.

Step 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 12.

Reset the device to factory default using CLI

Reset the device to factory default to revert all device configuration SETTINGS, including the device IP address and administrator password, to factory defaults.

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

Procedure

Step 1 Use the **configure factory reset config** command to reset of the device configuration.

Example:

```
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.

Step 2 Use the **configure factory reset default** command to reset the device configuration and data wipe.

Example:

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

Example:

The following files are cleared as part of this process:

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

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

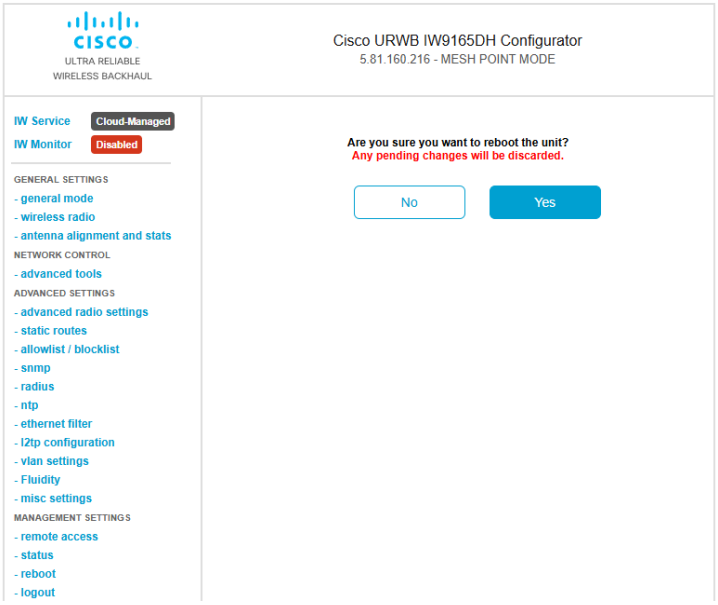
Reboot the device using GUI

Reboot the device's operating system to restart all system processes and apply configuration changes.

Use this procedure when you need to restart the device after making configuration changes or when troubleshooting system issues.

Procedure

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



Step 2 In the confirmation pop-up window, click **Yes**.

To abort the reboot, click **No**.

Step 3 To perform reboot using CLI, use the following command:

Example:

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

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

Save and RESTORE the device SETTINGS

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

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

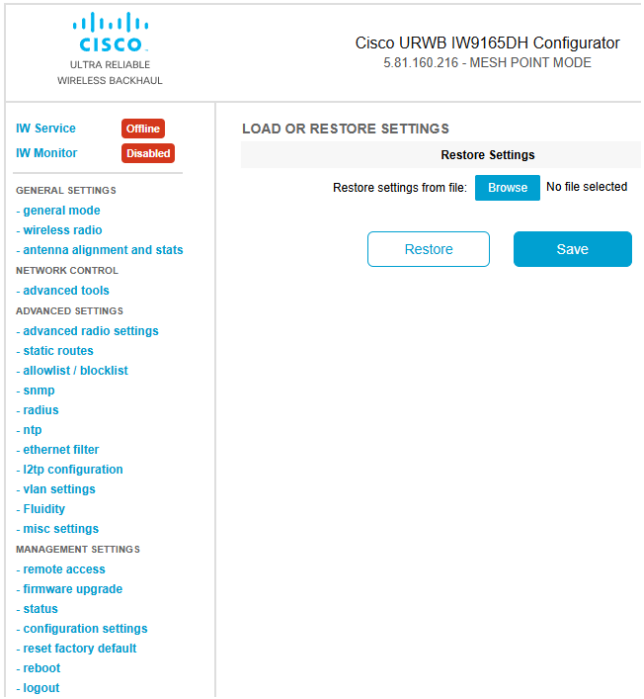
Note Device software configuration (*.conf) files are not interchangeable with IW Service configuration setup (*.iwconf) files.

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

Procedure

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

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



Step 2 To download the device's existing configuration SETTINGS to your computer, click **Save** to download the device configuration (*.conf).

Step 3 To upload a saved configuration file to the device, click **Browse** to upload the configuration (*.conf) file to the device.

Step 4 Click **RESTORE** to apply the configuration SETTINGS to the device.

Configure GENERAL SETTINGS

Configure the operational mode and LAN parameters to establish proper mesh network functionality and device connectivity.

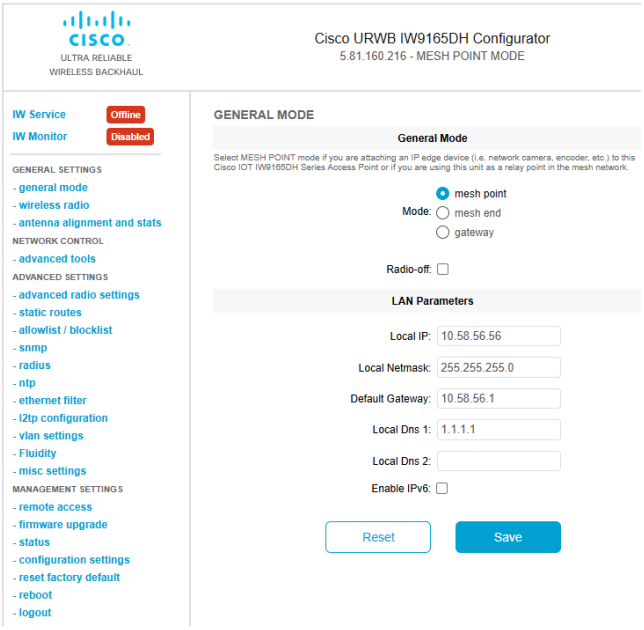
Devices capable of operating in a mesh radio network are shipped in mesh point mode. The GENERAL Mode has operational mode controls that determine how the device functions within the network.

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 General Mode settings, follow these steps:

Procedure

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



Step 2 Select the device's operational mode from the following options:

- **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.

Step 3 Change the LAN parameters by entering the local primary DNS address in the **DNS 1** field, and enter the local secondary DNS address in the **DNS 2** field if needed.

The **Local IP** and **Local Netmask** LAN parameters are shown with factory-set default values when the GENERAL Mode window is opened for the first time.

Step 4 Click **Save** to save the LAN SETTINGS.

To clear the SETTINGS, click **Reset**.

Step 5 Alternatively, configure GENERAL SETTINGS using CLI commands.

Example:

```
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
```

Step 6 Configure LAN parameters using CLI commands.

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

Configure the access point locally without connecting to a wired LAN by establishing a console connection and accessing the command-line interface.

This task enables local configuration of the access point when network connectivity is not available or when initial setup is required.

Before you begin

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. Then, open the CLI by connecting to the access point's console port.

Procedure

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.

Step 2 Set up a terminal emulator to communicate with the access point.

In the terminal emulator, use these settings:

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

Step 3 Log in using the default credentials and access the appropriate command-prompt mode.

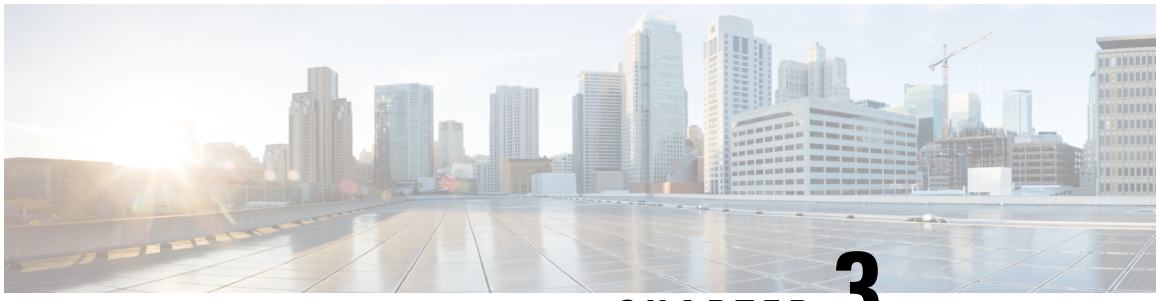
There are two available command-prompt modes: standard command prompt (>) and privileged command prompt (#). When you log in for the first time, the system directs you to standard command prompt (>) mode, where you can execute unprivileged commands.

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

Use these default credentials to log in:

- Username: Cisco
- Password: Cisco

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



CHAPTER 3

SSH and Web UI Access

- Enable SSH access, on page 17
- Disable SSH access, on page 17
- Enable web UI access, on page 18
- Disable web UI access, on page 18

Enable SSH access

Procedure

Step 1 Use the **configure ssh enable** command to enable access to the SSH.

Example:

```
Device# configure ssh enable
```

Step 2 Use the **show ssh** command to verify whether SSH is enabled by entering the following command:

Example:

```
Device# show ssh
 SSH: enabled
```

Disable SSH access

Procedure

Step 1 Use the **configure ssh disable** command to disable access to the SSH.

Example:

```
Device# configure ssh disable
```

Step 2 Use the **show ssh** command to verify that SSH is disabled by entering the following command:

Example:

```
Device# show ssh
 SSH: disabled
```

Enable web UI access

Enable Web UI access to allow graphical interface management of the device.

Web UI access provides a graphical interface for device management and configuration.

Procedure

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

```
Device# configure webui enable
```

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

```
Device# show webui config

Web-UI: enabled
```

Disable web UI access

This task disables Web UI access on the device.

Use this procedure when you need to disable web-based management access to the device.

Procedure

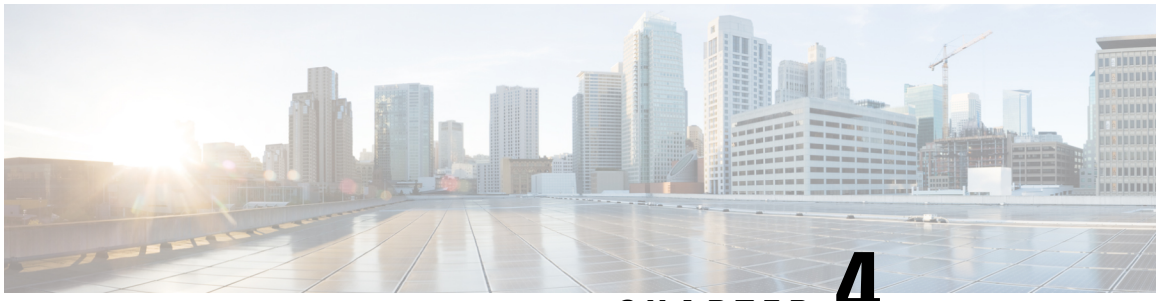
Step 1 To disable Web UI access, use the following command:

```
Device# configure webui disable
```

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

```
Device# show webui config

Web-UI: disabled
```



CHAPTER 4

Upgrade the Device using GUI

• Upgrade the device using GUI, on page 19

Upgrade the device using GUI

Procedure

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

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

Step 3 Click **Login** .

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

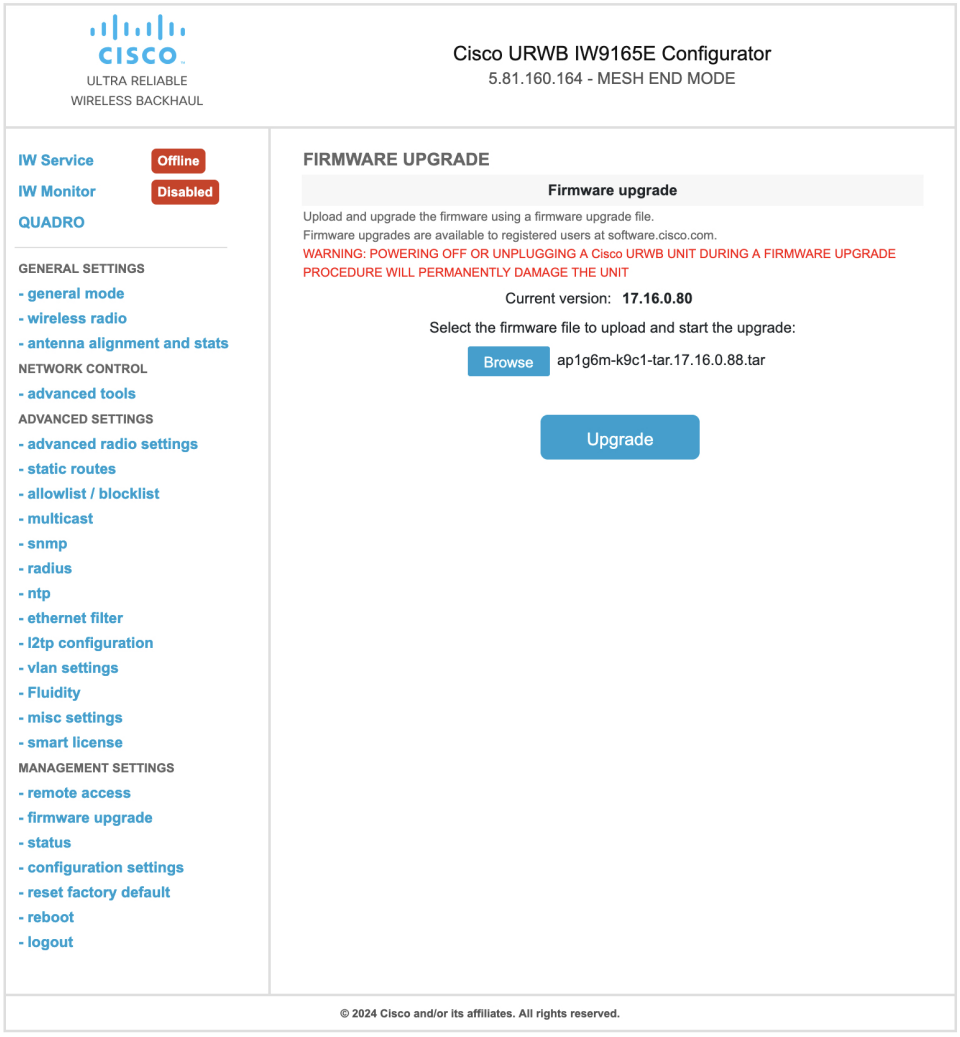
Step 4 In the **MANAGEMENT SETTINGS** , click the **firmware upgrade** link to open the **FIRMWARE UPGRADE** window.

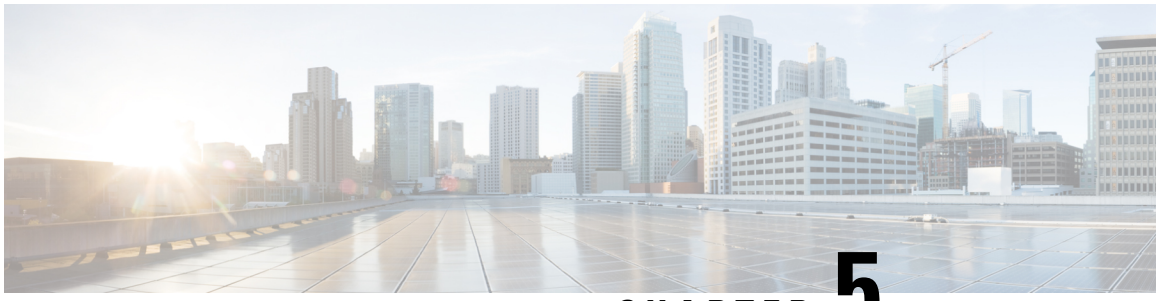
Step 5 Click the **Browse** button to locate and select the firmware upgrade file.

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

Step 7 Click **OK** to confirm uploading the firmware file to the device.

Once the firmware is successfully uploaded to the device, the AP verifies the image and then reboots.


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



CHAPTER 5

Upgrade the Device using TFTP

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

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

- Device Upgrade using TFTP, on page 21
- Automatic Device Upgrade using TFTP, on page 21
- Direct Device Upgrade using TFTP, on page 23
- TFTP Device Upgrade using CLI, on page 24

Device Upgrade using TFTP

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

Upgrade Methods

You can choose either of the following methods:

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

Automatic Device Upgrade using TFTP

Before you begin

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

Procedure

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

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

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

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

Configuring Manifest File on the TFTP Server

The manifest file is a configuration component that acts as a roadmap for the device upgrade process.

- Provides instructions for retrieving the device image from the TFTP server.
- Defines the conditions that must be satisfied before the upgrade begins.

Upgrade Process Workflow

1. The device retrieves the manifest file from the TFTP server.
2. The device parses the manifest file to locate the device image.
3. The device retrieves the image from the TFTP server.
4. The device verifies the required conditions and initiates the upgrade.

Manifest File Format

The manifest file contains the device image filename, MD5 checksum, and device image version required for the device upgrade process.

The manifest file includes the following information:

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

Table 1: Manifest file names by device model

Device Type	Manifest File Name
IW9167EH	IW9167EH.manifest

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

Example Manifest File Format

```
image_name=ap1g6m-k9c1-tar.202307110910

image_md5=376e15acd4e82a49a81d42add904f5b0

image_version=8.8.1.101
```

Direct Device Upgrade using TFTP

Direct device upgrade using TFTP is a configuration method where the device retrieves a specified image file directly from a remote TFTP server to perform a system update.

- Requires a reachable TFTP server with the target image file.
- Uses specific CLI commands to define the server address and file path.
- Initiates the upgrade process immediately upon command execution.

TFTP Upgrade Configuration Commands

Table 2: TFTP Upgrade Configuration

Purpose	Command or Action
To configure the TFTP server with IP address	`Device#configure tftp server A.B.C.D` A.B.C.D: IP address of the TFTP server
To configure the TFTP upgrade image	`Device#configure tftp upgrade <image file>` Configure TFTP upgrade image <image file bin>



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

TFTP Device Upgrade using CLI

Procedure

Step 1 Use the **configure tftp server** *ip-address* command to configure the TFTP server IP address.

Example:

```
Device# configure tftp server A.B.C.D
```

ip-address :IP address of the TFTP server.

Step 2 Enable or disable automatic TFTP device upgrades.

- Use the **configure tftp upgrade automatic disable**command to disable automatic TFTP device upgrades.

  ```
  Device# configure tftp upgrade automatic disable
  ```

- Use the **configure tftp upgrade automatic enable**command to enable automatic TFTP device upgrades.

  ```
  Device#configure tftp upgrade automatic enable
  ```

Step 3 Use the **configure tftp upgrade check period** *period*command to configure the check period for TFTP device upgrades.

Example:

```
Device# configure tftp upgrade check period 3
```

Note
The check period must be specified in the hours format.

Step 4 Use the **configure tftp upgrade check now** command to check for the manifest file immediately.

Example:

```
Device# configure tftp upgrade check now
```

Step 5 Use the **show tftp config** command to verify the TFTP configuration.

Example:

```
Device# show tftp config
```

The device upgrade procedure fails to start under the following conditions:

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

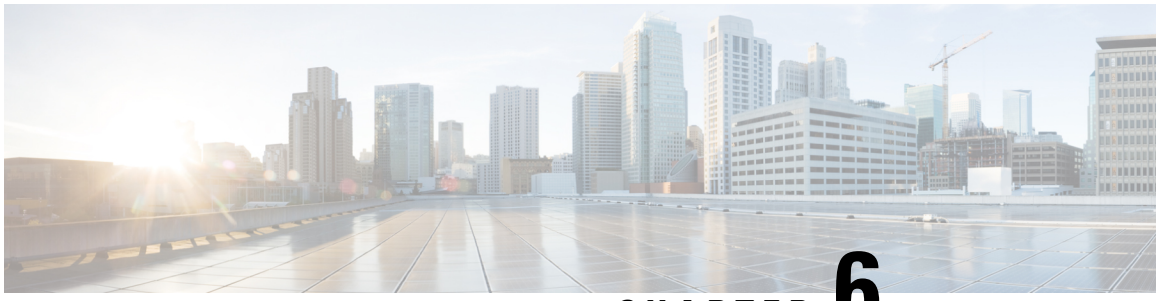
Example of show TFTP configuration:

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

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

Example of automatic TFTP upgrade:

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



CHAPTER 6

Smart Licensing

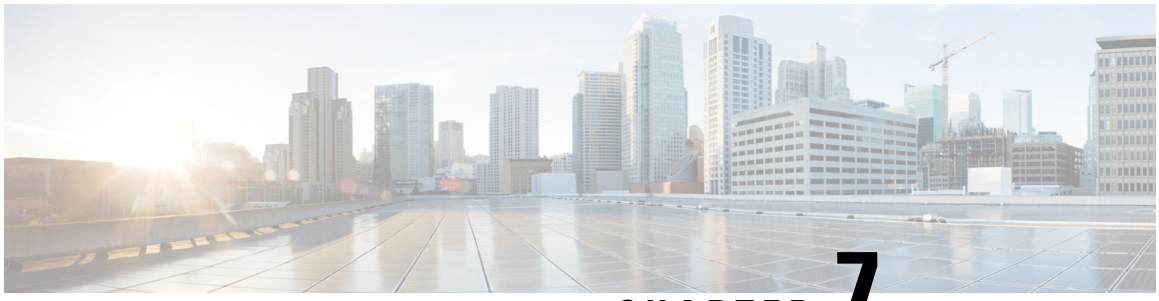
- Smart licensing support, on page 27

Smart licensing support

Smart licensing support is a licensing feature that provides updated information related to Smart licensing for access points running in URWB mode through a dedicated standalone guide.

Smart licensing guide replacement

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



CHAPTER 7

Fixed domains and country codes (ROW)

• Fixed domains and country codes for Catalyst APs (ROW), on page 29

Fixed domains and country codes for Catalyst APs (ROW)

Fixed domains and country codes for Catalyst APs (ROW) is a regulatory management system that simplifies the management of country codes for regions that do not have a specific domain mapped, with fixed domain and country code support for the Catalyst IW9167E, IW9165E, and IW9165D APs.

Regulatory approval verification

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

Supported fixed domains for Catalyst IW9167E

This table provides a summary of supported fixed domains for the Catalyst IW9167E, detailing indoor deployment capabilities for each domain.

Table 3: Supported fixed domains for Catalyst IW9167E

Domain	Indoor deployment support
A	No
B [1]	N/A
E	Yes
F	No
Q	No
Z	No

[1] Outdoor and indoor frequencies are same for the B domain.

Supported country codes for Catalyst IW9167E

This table provides the complete list of supported country codes for the Catalyst IW9167E access point, including indoor deployment support status and initial software release information.

Country code	Indoor deployment support	Initial support
Algeria (DZ)	No	17.16.1
Argentina (AR)	No	17.13.1
Bahamas (BS)	No	17.16.1
Brazil (BR)	No	17.13.1
Brunei (BN)	No	17.16.1
Cameroon (CM)	No	17.16.1
Chile (CL)	No	17.13.1
China (CN)	No	17.13.1
Colombia (CO)	No	17.13.1
Costa Rica (CR)	No	17.16.1
Ecuador (EC)	No	17.13.1
Egypt (EG)	No	17.15.1
El Salvador (SV)	No	17.16.1
Ghana (GH)	No	17.16.1
Great Britain (GB)	Yes	17.11.1
Hong Kong (HK)	No	17.13.1
Iceland (IS)[2]	Yes	—
India (IN)	No	17.12.1
Iraq (IQ)	No	17.13.1
Kenya (KE)	No	17.16.1
Korea (KR)	No	17.12.1
Kuwait (KW)	No	17.16.1
Macau (MO)	No	17.16.1
Malaysia (MY)	No	17.15.1
Mexico (MX)	No	17.13.1

Country code	Indoor deployment support	Initial support
Monaco (MC)[3]	Yes	—
Mongolia (MN)	No	17.15.1
Nigeria (NG)	No	17.16.1
Pakistan (PK)	No	17.13.1
Panama (PA)	No	17.16.1
Paraguay (PY)	No	17.16.1
Peru (PE)	No	17.12.1
Philippines (PH)	No	17.12.1
Puerto Rico (PR)[4]	No	17.15.1
Qatar (QA)	No	17.13.1
Saudi Arabia (SA)	No	17.13.1
Singapore (SG)	No	17.13.1
South Africa (ZA)	No	17.13.1
Taiwan, Republic of China (TW)	No	17.13.1
Thailand (TH)	No	17.13.1
Trinidad (TI)	No	17.18.1
United Arab Emirates (AE)	No	17.13.1
Uruguay (UY)	No	17.13.1
Vietnam (VN)	N/A	17.11.1

[2] Supported using -E domain.
[3] Supported using -E domain
[4] Supported using -B domain.

Note You can select the listed country codes using CLI or GUI. For ROW domain, select the country code for the device to work. This task IS common to all the three Catalyst APs: IW9167E, IW9165E, and IW9165DH.

Supported fixed domains for Catalyst IW9165E

This table provides a list of supported fixed domains for the Catalyst IW9165E access point and indicates their support status for indoor deployment.

Domain	Indoor deployment support
A	Yes
B [5]	N/A
E	Yes
F	Yes
Q	Yes
Z	Yes

[5] Outdoor and indoor frequencies are same for the B domain.

Supported country codes for Catalyst IW9165E

This table provides a comprehensive list of country codes supported by the Catalyst IW9165E access point, including indoor deployment capabilities and the initial software version that introduced support for each country.

Country code	Indoor deployment support	Initial support
Algeria (DZ)	Yes	17.16.1
Argentina (AR)	Yes	17.15.1
Bahrain (BH)	Yes	17.16.1
Bolivia (BO)	Yes	17.16.1
Brazil (BR)	Yes	17.13.1
Cameroon (CM)	Yes	17.18.1
Chile (CL)	Yes	17.13.1
China (CN)	Yes	17.15.1
Colombia (CO)	Yes	17.15.1
Costa Rica (CR)	Yes	17.16.1
Dominican Republic (DO)	Yes	17.16.1
Ecuador (EC)	Yes	17.15.1
Egypt (EG)	Yes	17.15.1
Ghana (GH)	Yes	17.18.1
Great Britain (GB)	Yes	17.12.1
Hong Kong (HK)	Yes	17.15.1

Country code	Indoor deployment support	Initial support
India (IN)	Yes	17.13.1
Iraq (IQ)	Yes	17.15.1
Kazakhstan (KZ)	Yes	17.16.1
Kenya (KE)	Yes	17.16.1
Korea (KR)	Yes	17.13.1
Kuwait (KW)	Yes	17.18.1
Malaysia (MY)	Yes	17.15.1
Mexico (MX)	Yes	17.13.1
Mongolia (MN)	Yes	17.15.1
Pakistan (PK)	Yes	17.15.1
Panama (PA)	Yes	17.16.1
Paraguay (PY)	Yes	17.16.1
Peru (PE)	Yes	17.13.1
Philippines (PH)	Yes	17.13.1
Qatar (QA)	Yes	17.13.1
Saudi Arabia (SA)	Yes	17.13.1
Singapore (SG)	Yes	17.13.1
South Africa (ZA)	Yes	17.13.1
Sri Lanka (LK)	Yes	17.13.1
Taiwan, Republic of China (TW)	Yes	17.14.1
Thailand (TH)	Yes	17.13.1
UAE (AE)	Yes	17.13.1
Vietnam (VN)	Yes	17.13.1

Supported fixed domains for Catalyst IW9165DH

This table provides the indoor deployment support status for various regulatory domains applicable to the Catalyst IW9165DH access point.

Domain	Indoor deployment support
A	No
B [6]	N/A
E	Yes
F	No
Q	No
Z	No

[6] Outdoor and indoor frequencies are same for the B domain.

Supported country codes for Catalyst IW9165DH

This table provides the supported country codes for the Catalyst IW9165DH access point, including indoor deployment availability and the initial software release that introduced support for each country.

Country code	Indoor deployment support	Initial support
Algeria (DZ)	No	17.16.1
Argentina (AR)	No	17.15.1
Bolivia (BO)	No	17.16.1
Brazil (BR)	No	17.13.1
Cameroon (CM)	No	17.16.1
Chile (CL)	No	17.13.1
China (CN)	No	17.15.1
Colombia (CO)	No	17.15.1
Costa Rica (CR)	No	17.16.1
Costa Rica (CR)	No	17.16.1
Dominican Republic (DO)	No	17.16.1
Ecuador (EC)	No	17.15.1
Egypt (EG)	No	17.15.1
Ghana (GH)	No	17.16.1
Great Britain (GB)	Yes	17.12.1
Hong Kong (HK)	No	17.15.1

Country code	Indoor deployment support	Initial support
India (IN)	No	17.13.1
Iraq (IQ)	No	17.15.1
Kazakhstan (KZ)	No	17.16.1
Kenya (KE)	No	17.16.1
Korea (KR)	No	17.13.1
Kuwait (KW)	No	17.16.1
Malaysia (MY)	No	17.15.1
Mexico (MX)	No	17.13.1
Mongolia (MN)	No	17.15.1
Pakistan (PK)	No	17.15.1
Panama (PA)	No	17.16.1
Paraguay (PY)	No	17.16.1
Peru (PE)	No	17.13.1
Philippines (PH)	No	17.13.1
Qatar (QA)	No	17.13.1
Saudi Arabia (SA)	No	17.13.1
Singapore (SG)	No	17.13.1
South Africa (ZA)	No	17.13.1
Sri Lanka (LK)	No	17.13.1
Taiwan, Republic of China (TW)	No	17.14.1
Thailand (TH)	No	17.13.1
UAE (AE)	No	17.13.1
Vietnam (VN)	No	17.13.1

Configure and verify country code using CLI

This task configures the country code for Rest of the World (ROW) domain access points to ensure proper wireless interface operation and regulatory compliance.

Country code configuration is required for ROW domain access points to enable correct wireless operation. The country code must be included in the ROW domain for successful configuration.

Before you begin

Follow these steps to configure and verify country code using CLI:

Procedure

Step 1 Use the **configure countrycode** *countrycode* command to configure the country code for the ROW domain.

Example:

```
Device# configure countrycode BR
```

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

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

Step 2 Use the **show version | in Product** command to verify the product model and ROW domain status.

Example:

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

Step 3 Use the **show dot11Radio** *interface* **config**command to verify the ROW country code configuration status.

Example:

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

Configure country code using GUI

Configure the country code to ensure wireless interfaces function properly and establish wireless connections between devices.

Wireless interfaces fail to work if country code is not configured. The country code setting ensures proper regulatory compliance and enables wireless functionality for your devices.

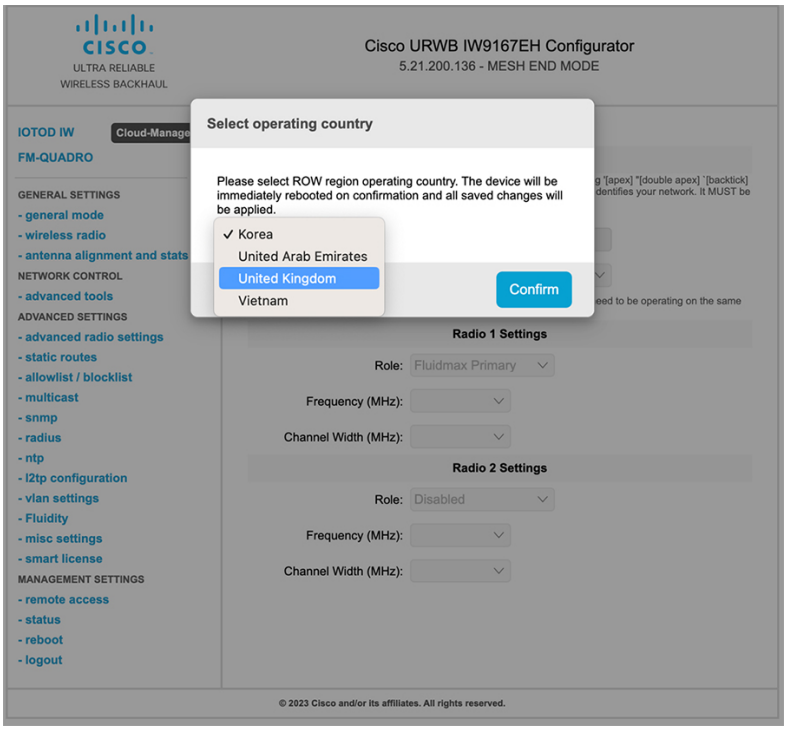
Before you begin

Follow these steps to configure the country code:

Procedure

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

Step 2 For ROW domain, if the country code is not selected, the following pop-up appears:



Step 3 To select a country code, click the pop-up in the above image then it redirects to the **Wireless SETTINGS** section.

In the **Wireless SETTINGS** section, choose country from the drop-down list.

A confirmation pop-up appears.

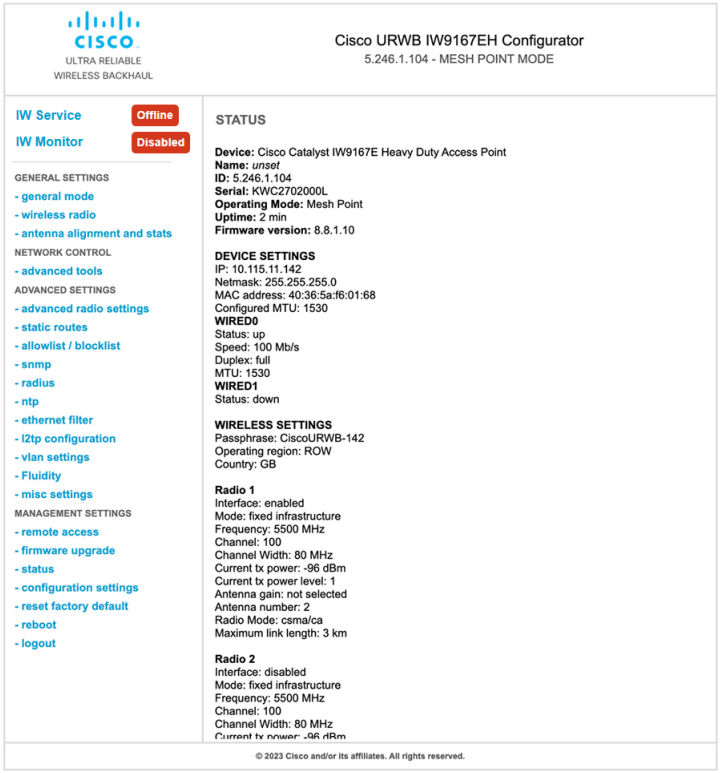
Step 4 Click **Confirm**.

A reboot confirmation screen appears.

Step 5 Click **Yes**.

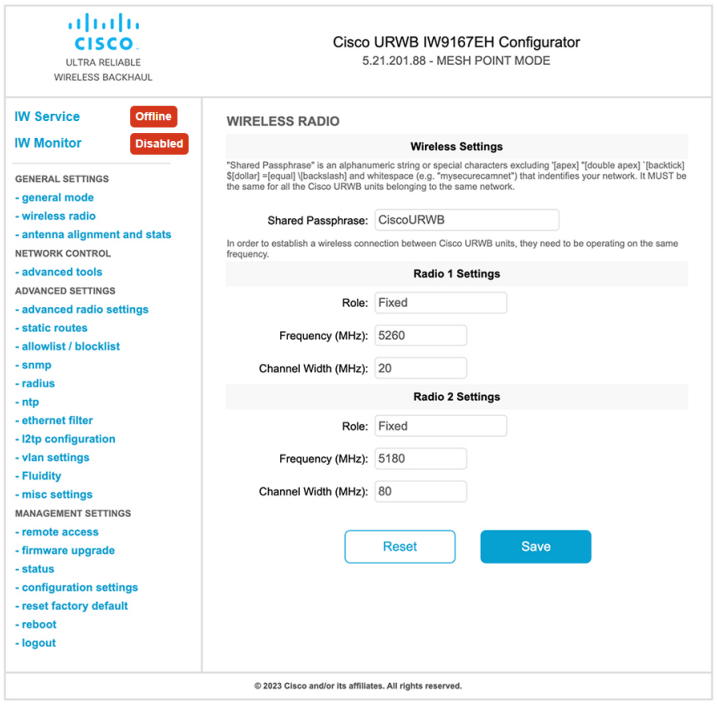
Step 6 In the **MANAGEMENT SETTINGS**, click **STATUS**.

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

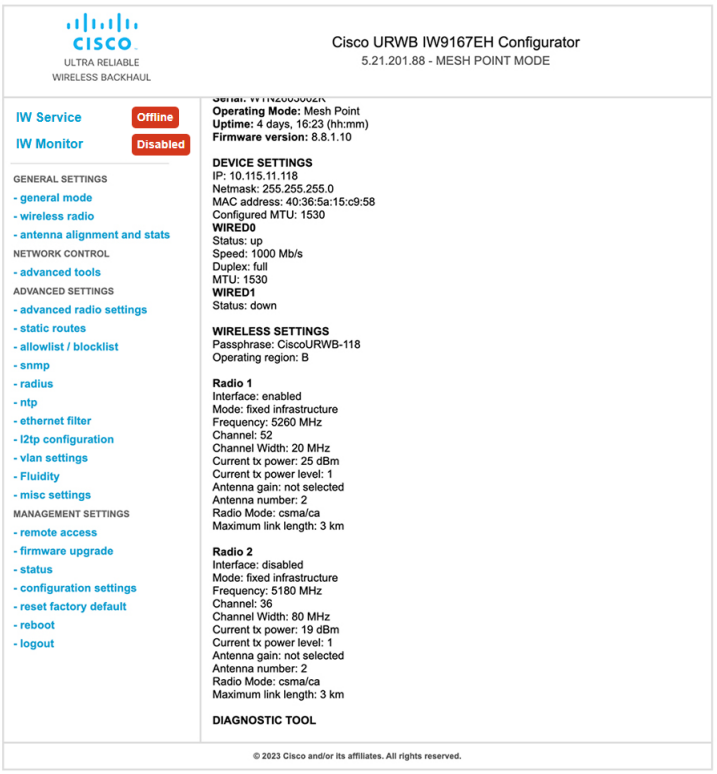


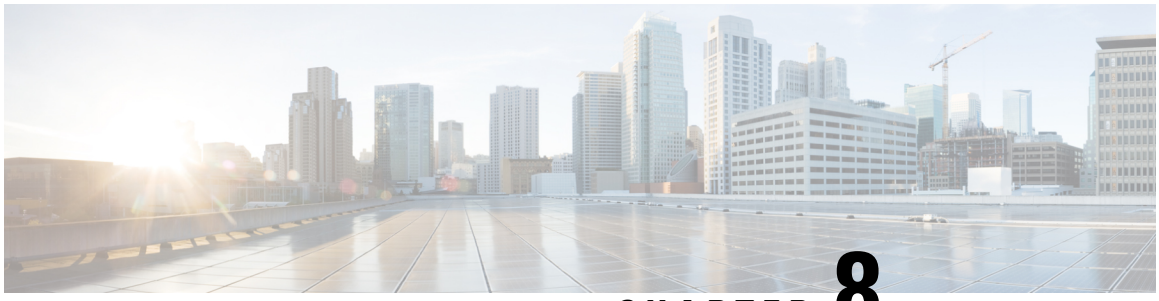
Step 7 To establish a wireless connection between devices, set the same operating frequency in radio devices.

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



Following image shows the configuration of country code using GUI:





CHAPTER 8

Indoor Deployment

• Configuring Guard Interval for HE, on page 41

Configuring Guard Interval for HE

Configures the guard interval for HE to improve link reliability in long-range outdoor deployments.

Procedure

Step 1 Use the **configure dot11Radio** *interface* **guard-interval** [*gi*] command to configure the guard interval.

Example:

```
Device# configure dot11Radio 1 guard-interval 1600
```

Guard interval values include:

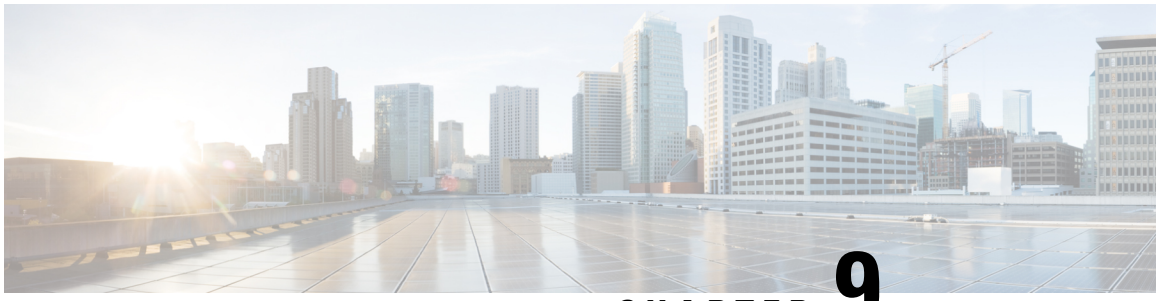
- 3200: Configures 3200 ns guard interval (supported only in HE mode).
- 1600: Configures 1600 ns guard interval (supported only in HE mode).
- 800: Configures 800 ns guard interval (default guard interval mode and disable mode in HT, VHT, and HE).
- 400: Configures 400 ns guard interval (supported in HT and VHT modes).

Step 2 Use the **show dot11Radio** *interface* **show** command to verify the configuration.

Example:

```
Device# show dot11Radio 1 show

Maximum tx mcs: 9
High-efficiency : enabled
Maximum tx nss : 2
RTS protection : disabled
guard-interval : 1600 ns
```



CHAPTER 9

LED Pattern for Catalysts IW9167 and IW9165

- LED pattern for Catalyst IW9167, on page 43
- LED pattern for Catalyst IW9165, on page 44

LED pattern for Catalyst IW9167

The Catalyst IW9167E follows specific LED patterns during the booting process and operational states to indicate system status and signal quality.

Table 4: Definition of booting LED pattern

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

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

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

Table 5: 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 the patterns to indicate URWB states:

Table 6: LED pattern for URWB states

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

RSSI LED

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

Table 7: 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

This table shows the LED functionalities for the Catalyst IW9165E:

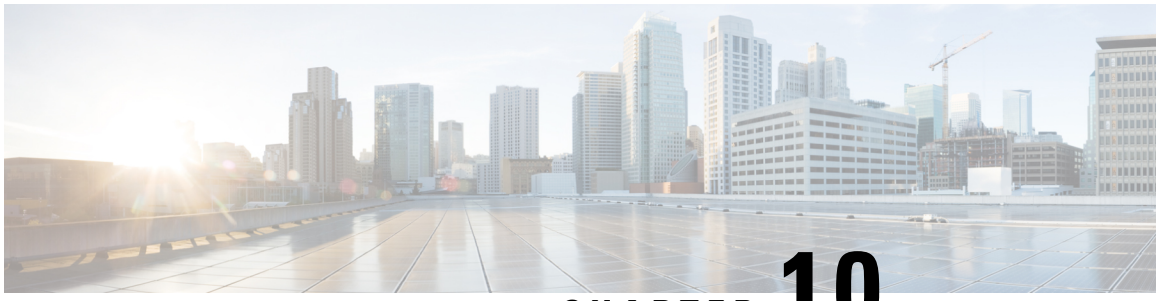
Table 8: URWB LED function for the Catalyst IW9165E

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

This table shows the LED functionalities for the Catalyst IW9165D:

Table 9: URWB LED function for the Catalyst IW9165D

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



CHAPTER 10

IPv6 Support

- IPv6 Support, on page 47
- IPv6 address types, on page 47
- IPv6 limitations on the AP, on page 48
- Enable or disable IPv6 using CLI, on page 48
- Enable or disable IPv6 RA autoconfig using CLI, on page 48
- Configure static IPv6 address with eui-64, gateway, and DNS server address, on page 49
- Verify static IPv6 address with eui-64, gateway, and DNS server address, on page 49
- Configure static IPv6 address without eui-64, gateway, and DNS server address, on page 50
- Verify static IPv6 address without eui-64, gateway, and DNS server address, on page 50
- Configure static IPv6 address with EUI-64, on page 50
- Verify static IPv6 address with eui-64, on page 51
- Configure static IPv6 address without eui-64, on page 51
- Verify static IPv6 address without eui-64, on page 51
- Clear the IPv6 gateway and DNS servers configuration, on page 51
- Verify the cleared IPv6 gateway and DNS servers configuration, on page 52
- Enable and configure static IPv6 using GUI, on page 52
- Verify static IPv6 using GUI, on page 54

IPv6 Support

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

IPv6 address types

You can configure the AP with these IPv6 address types:

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

- **Unique-Local**: Can be routed within a private organization, but not through the public internet. It is not expected to be routable on the global Internet. However, it is routable inside a limited area, such as a site, and it may route between a limited set of sites.
- **Global Unicast**: A routable address in the IPv6 Internet, similar to the public IPv4 address space.

IPv6 limitations on the AP

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

Enable or disable IPv6 using CLI

This task enables or disables IPv6 support on the access point (AP) to control IPv6 addressing functionality.

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

Procedure

Use the **configure ipv6** {**enable** | **disable**} command to enable or disable the IPv6 address on the AP.

Example:

```
Device# configure ipv6 enable
```

Enable or disable IPv6 RA autoconfig using CLI

This task enables or disables IPv6 Router Advertisement (RA) autoconfiguration on the access point to control automatic IPv6 address assignment from router advertisements.

IPv6 RA autoconfig allows access points to automatically configure IPv6 addresses based on router advertisements received from the network. You may need to enable or disable this feature depending on your network's IPv6 configuration requirements.

Follow these steps to enable or disable IPv6 RA autoconfig on the access point:

Procedure

Use the **configure ipv6 enable autoconfig-ra** {**enable** | **disable**} command to enable or disable the IPv6 RA Autoconfig on the AP.

Example:

```
Device# configure ipv6 enable autoconfig-ra enable
```

Note

- Enable: Enables the autoconfiguration from router advertisement.
- Disable: Disables the autoconfiguration from router advertisement.

Configure static IPv6 address with eui-64, gateway, and DNS server address

Configure a static IPv6 address with eui-64, gateway, and DNS server address on the AP.

Static IPv6 configuration allows you to manually assign network parameters to an access point, providing predictable addressing while using EUI-64 for automatic interface identifier generation.

Procedure

Configure the static IPv6 address with eui-64, gateway, and DNS server address on the AP.

Example:

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

Verify static IPv6 address with eui-64, gateway, and DNS server address

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

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

Configure static IPv6 address without eui-64, gateway, and DNS server address

This task configures a static IPv6 address without eui-64, gateway, and DNS server address on the access point.

Use this configuration when you need to manually assign IPv6 network settings to an access point without using the eui-64 interface identifier format.

Procedure

Use the **configure ap address ipv6 static** *ip* command to configure the static IPv6 address without eui-64, gateway, and DNS server address on the AP.

Example:

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

Verify static IPv6 address without eui-64, gateway, and DNS server address

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

```
Device#show ipv6
IPv6: Enabled
Router Advertisment auto-configuration: Disabled
Static IPv6 config:
Address: fc00::1234:5678:xxxx:def/64
Gateway: fc00::1
DNS1: 2001:4860:4860::xxxx
DNS2: 2001:4860:4860::xxxx
Currently assigned addresses:
fc00::1234:5678:xxxx:def/64 global
fe80::4236:5aff:xxxx:168/64 link
```

Configure static IPv6 address with EUI-64

Configure the static IPv6 address with EUI-64 on the access point.

Procedure

Use the **configure ap address ipv6 static** *ip* command to configure the static IPv6 address with eui-64 on the AP.

Example:

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

Verify static IPv6 address with eui-64

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

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

Configure static IPv6 address without eui-64

Configure the static IPv6 address on the access point.

Procedure

Use the **configure ap address ipv6 static** *ip* command to configure the static IPv6 address without eui-64 on the AP.

Example:

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

Verify static IPv6 address without eui-64

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

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

Clear the IPv6 gateway and DNS servers configuration

Clear the IPv6 gateway and DNS servers addresses configuration on the AP.

This task removes existing IPv6 gateway and DNS server configurations from an access point.

Procedure

Use the **configure ap address ipv6 static** *ip* command to clear the IPv6 gateway and DNS servers addresses configuration on the AP.

Example:

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

Verify the cleared IPv6 gateway and DNS servers configuration

Verify the cleared IPv6 gateway and DNS server addresses configuration on the AP using the show command.

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

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

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

Enable and configure static IPv6 using GUI

Enable and configure static IPv6 addressing to provide manual control over the device's IPv6 network configuration instead of relying on automatic configuration methods.

Static IPv6 configuration allows you to manually set the device's IPv6 address, gateway, and DNS servers. This is useful when you need specific network SETTINGS that differ from automatically assigned addresses.

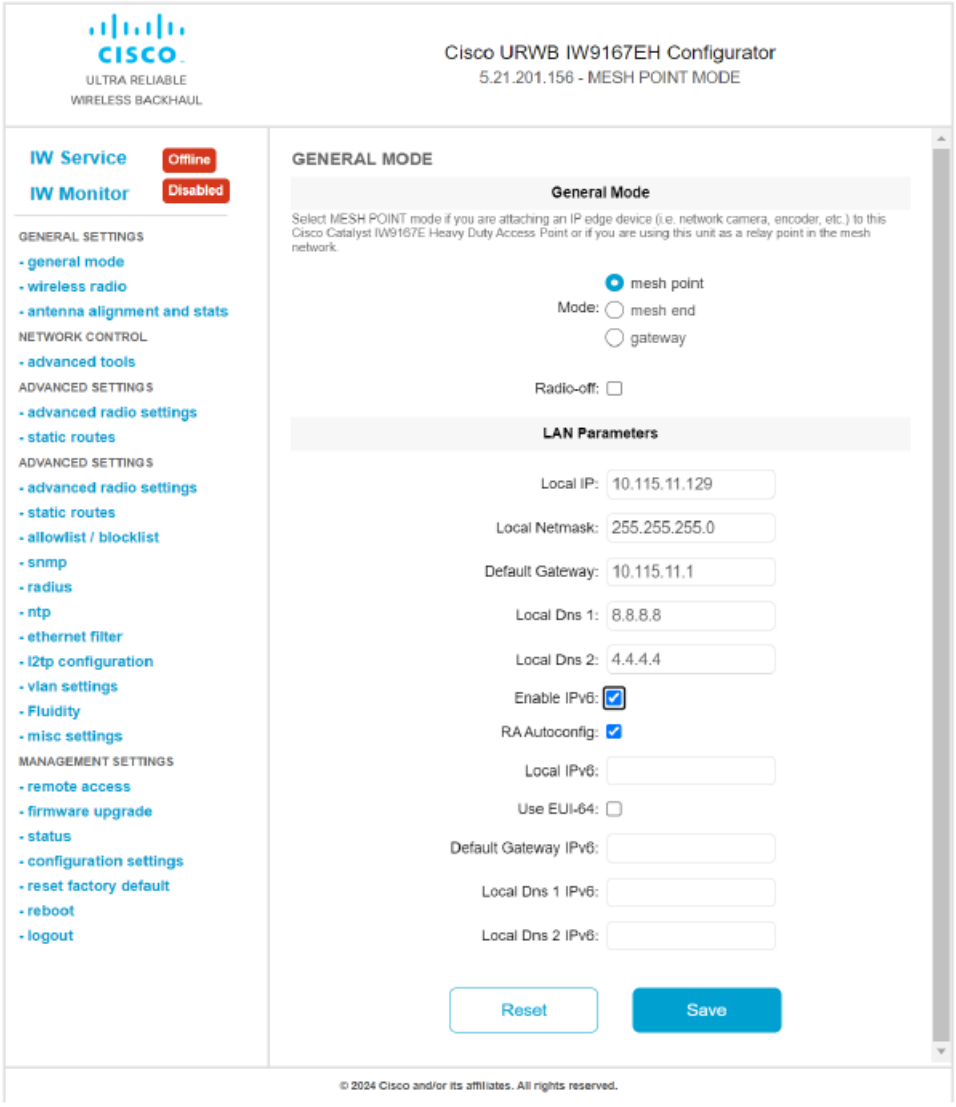
Before you begin

Follow these steps to enable and configure static IPv6 using the GUI:

Procedure

Step 1 Log in to the configurator by entering your credentials on the web login page.
Once you successfully log into the GUI, the URWB configurator displays.

Step 2 In the **GENERAL SETTINGS**, click **GENERAL mode** to open the **GENERAL Mode** window.



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

Step 3 Check the **Enable IPv6** check box.
The system automatically enables the **RA Autoconfig**.

Step 4 Enter IPv6 address in the **Local IPv6** field.

Step 5 (Optional) Check the **Use EUI-64** check box.

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

Step 6 (Optional) Enter the gateway IP address in the **Default Gateway IPv6** field.

Step 7 (Optional) Enter the DNS server 1 IP address in the **Local DNS 1 IPv6** field.

Step 8 (Optional) Enter the DNS server 2 IP address in the **Local DNS 2 IPv6** field.

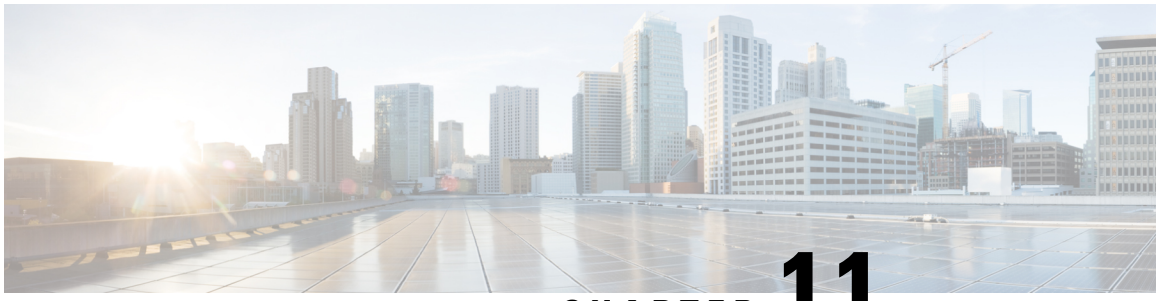
Step 9 Click **Save**.

Verify static IPv6 using GUI

Procedure

Step 1 In the **MANAGEMENT SETTINGS** , click **STATUS** .

Step 2 On the **STATUS** page, in the **DEVICE SETTINGS** section, view the IPv6 details.



CHAPTER 11

FIPS Certification

- FIPS certification, on page 55
- Enable or disable FIPS mode, on page 55
- Verify FIPS mode using CLI, on page 56

FIPS certification

FIPS certification is a compliance mode that ensures SSH and GUI functionalities comply with FIPS140-3 security standards from NIST. When enabled, it also ensures that the AP configuration meets FIPS requirements.

Note FIPS certification does not support SNMP.

Enable or disable FIPS mode

This task configures FIPS mode on an access point.

Procedure

Use the **configure fips** { **enable** | **disable** } command to enable or disable FIPS mode on AP.

Example:

```
Device# configure fips enable
```

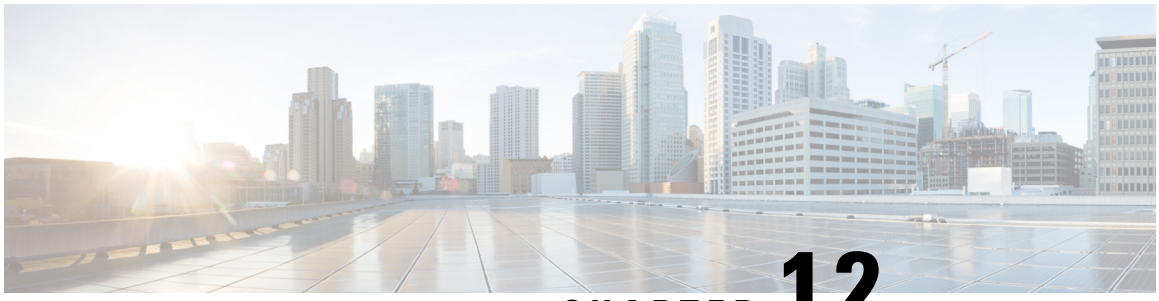
Verify FIPS mode using CLI

Procedure

Use the **show fips** command to verify FIPS mode on the AP.

Example:

```
Device# show fips
FIPS: enabled
```



CHAPTER 12

URWB Operation Mode

- URWB operation mode, on page 57
- Identify Software Images from CLI, on page 57
- Reset button settings, on page 58
- Configure image conversion, on page 58
- Access the GUI, on page 59
- Verify URWB Catalyst IW9167E configuration using GUI, on page 60
- Commit CLI configuration, on page 60
- Configure IW Service Cloud-Managed and Offline Mode using CLI, on page 61
- Configure password after first login using CLI, on page 62
- Configure IW Service using GUI , on page 64

URWB operation mode

URWB operation mode is a wireless technology configuration that enables Catalyst Industrial Wireless access points to operate in Ultra-Reliable Wireless Backhaul mode.

URWB operation mode characteristics

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.

Identify Software Images from CLI

The access point OS supports two different software images: Catalyst Wi-Fi (AP) and UIW. Use CLI commands to determine which software is running and verify the operating mode.

Use the **show version** 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** command 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 this CLI command:

```
Device#show iw-service 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

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.

Configure image conversion

Configure image conversion to change the operational mode of a Catalyst IW9167E access point to meet different network requirements.

Use image conversion when you need to change the operational mode of a Catalyst IW9167E access point between Wi-Fi mode (CAPWAP AP), URWB mode, and WGB/uWGB mode based on your network deployment needs.

Procedure

Step 1 To convert from CAPWAP to URWB mode or from WGB/uWGB to URWB mode, use this CLI command:

Example:

```
Device# configure boot mode urwb
```

The access point reboots and starts up in URWB mode.

Step 2 To convert from URWB to CAPWAP mode or from WGB/uWGB to CAPWAP mode, use this CLI command:

Example:

```
Device# configure boot mode capwap
```

The access point reboots and starts up in CAPWAP mode.

Step 3 To convert from CAPWAP to WGB/uWGB mode or from URWB to WGB/uWGB mode, use this CLI command:

Example:

```
Device# configure boot mode wgb
```

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

Access the GUI

This task allows you to access the Web UI configuration interface for your device.

Use this procedure when you need to configure or manage your IW9167E or IW9165 device through the web-based interface.

Procedure

Step 1 Open the web browser and enter the following URL: https://<IP address of unit>/

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

Step 2 Enter the credentials using the **Username** and **Enable password**.

Step 3 Log into the GUI.

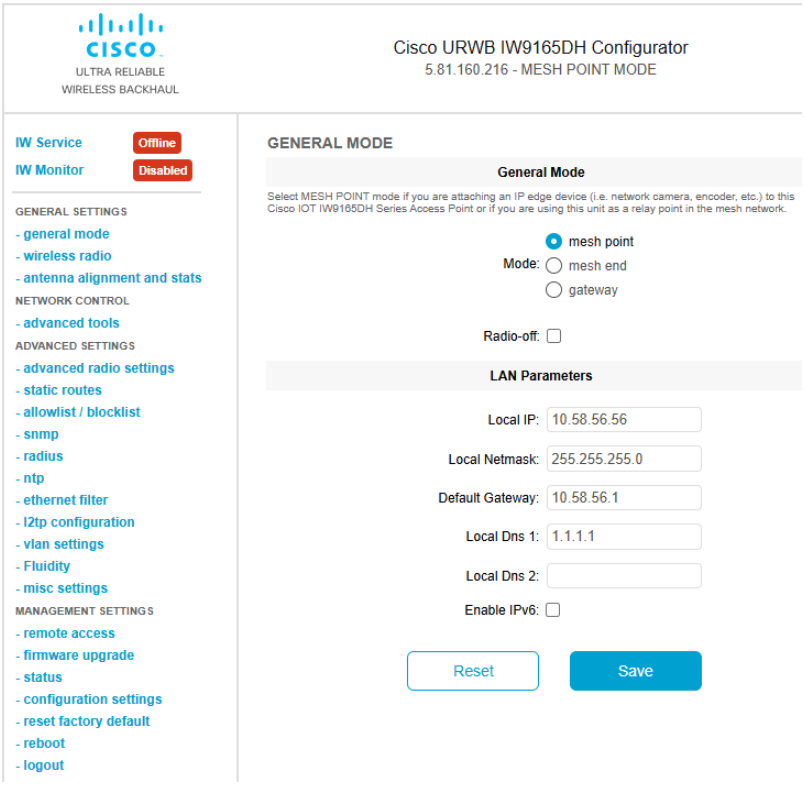
Once you successfully log into the GUI, the URWB configurator displays:



Verify URWB Catalyst IW9167E configuration using GUI

This figure displays the graphical user interface configuration for the Catalyst IW9167E access point to ensure correct URWB setup.

Figure 6: Catalyst IW9167E configurator



Commit CLI configuration

Save the current or running configuration settings to local storage or memory and make the configuration effective on the device.

The modified configuration values are stored in the cache configuration file. After entering the `write` command, you must reboot the device for the current configuration to take effect.

Procedure

Step 1 Save the current configuration settings to memory.

Example:

```
Device# write
```

You can also use the abbreviated command:

```
Device# wr
```

The `write` or `wr` command commits the current configuration settings to memory.

Step 2 Reload the device.

Example:

```
Device# reload
```

The `reload` command reloads the device.

The configuration settings are saved to memory and the device reloads with the new configuration settings in effect.

Example:

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

Proceed with reload? [confirm]

(enter to confirm)

Configure IW Service Cloud-Managed and Offline Mode using CLI

This task sets up the device management mode to either connect to cloud services for centralized management or configure it locally for offline operation.

IW Service is the cloud management portal, and the device is connected to the Cloud-Managed 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 IW Service cloud service and select the configuration file exported from IW Service and upload the configuration file using upload configuration button at the end of IW Service management page.

Procedure

To activate or deactivate IW Service configuration capability, use this CLI command:

Example:

```
Device#configure iw-service {offline | cloud-managed}
```

Cloud-Managed - To set up IW Service mode to Cloud-Managed. The device can be managed from IW Service cloud server (if it is connected to the network).

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

Configure password after first login using CLI

Set up new login credentials after the device switches to offline mode to ensure secure access to the device.

Once the device switches to offline mode after the initial login, you need to set up new login credentials. The login credentials must follow specific criteria for security purposes.

Before you begin

Ensure the login credentials meet 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

Before you begin

Follow these steps to configure password after first login using CLI:

Procedure

Step 1 Switch the device to offline mode.

Example:

```
Device#configure iw-service offline

Switching to IW Service  Offline mode...

Will switch from Provisioning Mode to IW Service  offline Mode, device need to reboot:Y/N?
Y
```

The device reboots and switches to offline mode.

Step 2 Log in using the default credentials.

Example:

```
User Access Verification:

Username: Cisco

Password: Cisco
```

Default credentials:

```
username: Cisco

password: Cisco

enable password: Cisco
```

Step 3 Reset the credentials when prompted after first login.

Example:

```
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
```

Sample new credentials:

```
username: demouser

password: DemoP@ssw0rd

enable password: DemoE^aP@ssw0rd
```

Step 4 Re-login using the new credentials.

Example:

```
User access verification

Username: demouser

Password: DemoP@ssw0rd

Device> enable

Password:DemoE^aP@ssw0rd

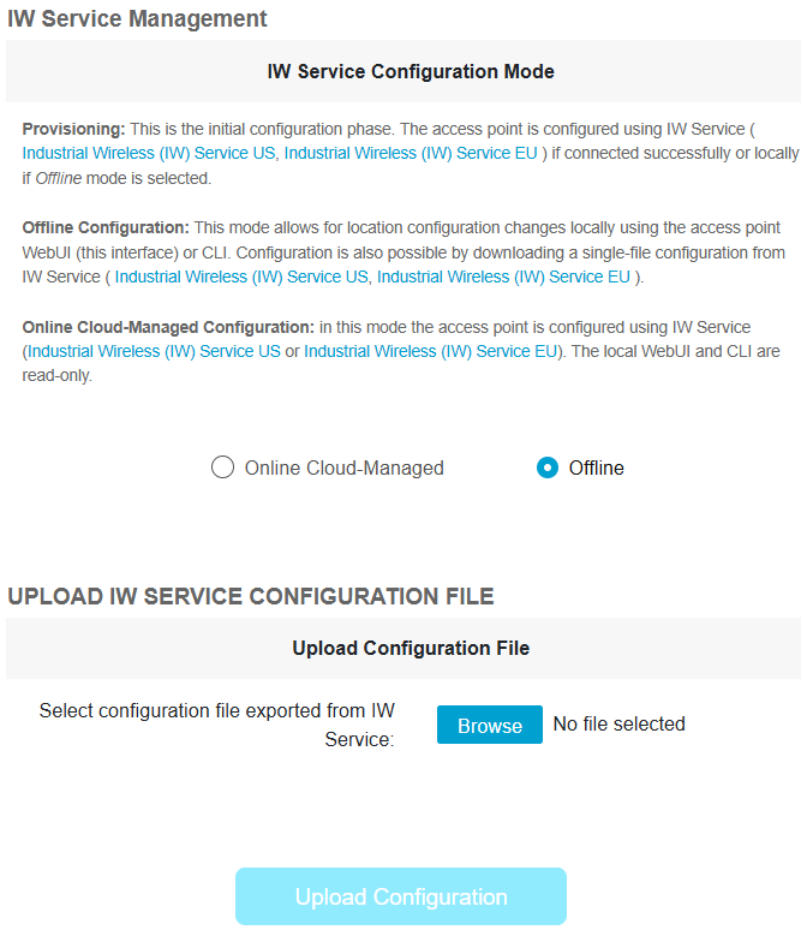
Device#
```

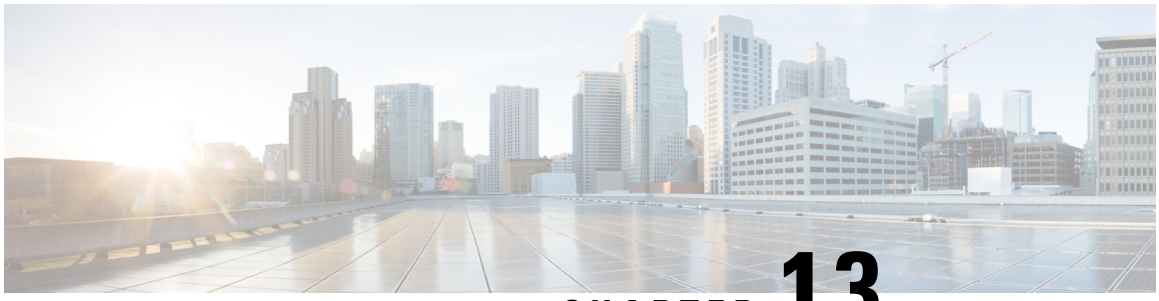
Note

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 IW Service using GUI

This topic provides the visual configuration steps for IW Service using the GUI.





CHAPTER 13

URWB Radio Mode

- Configure URWB radio mode, on page 65
- Configure radio-off mode from CLI, on page 66
- Configure radio mode for URWB from CLI, on page 67
- Configure AMPDU using CLI, on page 68
- Configure frequency from CLI, on page 69
- Configure maximum modulation coding scheme index from CLI, on page 69
- Configure maximum number of spatial streams index from CLI, on page 70
- Configure Rx-SOP threshold from CLI, on page 70
- Configure RTS mode from CLI, on page 71
- Configure WMM mode from CLI, on page 71
- Configure NTP from CLI, on page 72
- Configure NTP using GUI, on page 73
- Validate radio mode for URWB, on page 74
- Configure radio-off mode using GUI, on page 74
- Configure Radio mode using GUI, on page 75

Configure 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.

Table 10: 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

Table 11: Operating mode of radio interface

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

Table 12: 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)

Configure radio-off mode from CLI

This task allows you to configure radio-off mode to disable all wireless interfaces on the device when both Fluidity and fixed radios need to be turned off.

Radio-off mode is used when you need to disable wireless functionality on mesh devices. When you specify radio-off, the device disables all the wireless interfaces. This configuration is performed through CLI commands that set the device's operating mode and radio settings.

Before you begin

Follow these steps to configure radio-off mode from CLI:

Procedure

Step 1 Set the device's current operating mode.

Mode could be mesh end, mesh point or global gateway (L3).

Example:

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

Step 2 Set the device's selected Multi-Protocol Label Switching (MPLS) OSI layer.

The possible value of layer is 2 (OSI Layer-2) or 3 (OSI Layer-3).

Example:

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

Step 3 Set the radio-off mode.

Example:

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

Step 4 End the current configuration and save it.

Example:

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

Device# write
```

Example:

```
Configure modeconfig mode meshend radio-off fluidity

Configure modeconfig mode meshend radio-off fixed
```

Configure radio mode for URWB from CLI

Configure the radio mode for URWB to set the operating function of wireless interfaces and enable mixed Fluidity and fixed infrastructure combinations for different interfaces.

The device allows mixed Fluidity and fixed infrastructure combinations for different interfaces. 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.

Before you begin

Follow these steps to configure radio mode for URWB from CLI:

Procedure

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

Example:

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

Step 2 Configure an operating mode for the specified interface.

Example:

```
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.

Step 3 Set Fluidmax role for Fluidmax interface mode.

Example:

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

Primary - set Fluidmax role to primary

Secondary - set Fluidmax role to secondary

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

Example:

```
Device# end
```

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.

Configure AMPDU using CLI

This task allows you to configure AMPDU length and priority settings to optimize wireless network performance and transmission efficiency.

AMPDU (Aggregated MAC Protocol Data Unit) configuration enables you to adjust transmission parameters for wireless interfaces to improve network throughput and manage traffic prioritization.

Before you begin

Follow these steps to configure AMPDU using CLI:

Procedure

Step 1 Configure the AMPDU length using the following command:

Example:

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

length: <0-255> integer number – microseconds

Step 2 Configure AMPDU priority enable or disable setting:

Example:

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

enable: enable AMPDU tx priority

disable: disble AMPDU tx priority

Step 3 Configure AMPDU priority for specific indexes:

Example:

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

0: AMPDU tx priority for index 0

1: AMPDU tx priority for index 1

2: AMPDU tx priority for index 2

3: AMPDU tx priority for index 3

4: AMPDU tx priority for index 4

5: AMPDU tx priority for index 5

6: AMPDU tx priority for index 6

7: AMPDU tx priority for index 7

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

Configure frequency from CLI

Configure an operating frequency for a dot11radio interface using CLI commands.

Use the CLI to set the operating frequency for wireless radio interfaces.

Procedure

Configure the operating frequency.

Example:

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

Valid range for operating frequency is 0-7125 in MHz.

Configure maximum modulation coding scheme index from CLI

Configure the maximum MCS index to optimize wireless performance and data transmission rates.

The maximum MCS index determines the highest modulation and coding scheme that can be used for wireless transmission. You can set this value manually or allow automatic configuration.

Procedure

Configure the maximum MCS index using the following CLI command:

Example:

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

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

Valid values are from 0 to 11 or AUTO.

Note
If High Efficiency mode is disabled, set the MCS index value ranging from 0 to 9. If High Efficiency mode is enabled, set the MCS index value as 10 or 11.

Configure maximum number of spatial streams index from CLI

Configure the maximum number of spatial streams (NSS) index to optimize wireless performance based on device capabilities and antenna configuration.

The NSS index determines the maximum number of spatial streams that can be used for wireless communication. This setting can be configured manually with specific values or set to AUTO for automatic configuration.

Procedure

Configure the maximum number of spatial streams index using the following command:

Example:

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

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

Valid values range from 1 to 4 or 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.

Configure Rx-SOP threshold from CLI

Configure the receiver start of packet (Rx-SOP) threshold to control signal detection sensitivity on the wireless interface.

The Rx-SOP threshold setting determines the minimum signal level required for the receiver to detect the start of a packet.

Procedure

Configure the Rx-SOP threshold using the following CLI command:

Example:

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

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

Configure RTS mode from CLI

Configure RTS mode to control ready to send protection on wireless interfaces, either by disabling RTS protection or enabling it with a specific threshold value.

RTS mode configuration allows you to manage wireless transmission protection mechanisms on dot11radio interfaces.

Procedure

Step 1 To disable ready to send (RTS) mode, use the following CLI command:

Example:

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

Step 2 To enable RTS with threshold value, use the following CLI command:

Example:

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

The threshold range is from 0 to 2346.

Configure WMM mode from CLI

This task allows you to configure wireless multimedia (WMM) mode and manage wireless statistics counters.

WMM mode configuration is essential for managing different types of network traffic through class-of-service (CoS) parameters. This configuration helps prioritize voice, video, best-effort, and background traffic appropriately.

Procedure

Step 1 Configure wireless multimedia (WMM) mode using the appropriate class-of-service parameter.

Example:

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

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

- be: Best-effort traffic queue (CS0 and CS3).
- bk: Background traffic queue (CS1 and CS2).

- vi: Video traffic queue (CS4 and CS5).
- vo: Voice traffic queue (CS6 and CS7).

Step 2 Clear wireless statistics counters if needed.

Example:

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

Configure NTP from CLI

Configure Network Time Protocol (NTP) settings to ensure accurate time synchronization on the device.

NTP configuration includes setting up server addresses, authentication methods, timezone settings. Proper NTP configuration ensures time synchronization across network devices.

Procedure

Step 1 Use the **configure ntp server** *string* command to configure the NTP server address.

Example:

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

String - IP address or domain name.

Step 2 Use the **configure ntp authentication** command to configure NTP authentication.

Example:

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

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

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

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

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

- \ [backslash]
- # [number sign]
- whitespace

Example:

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

Step 3 Use the **configure ntp** {**enable** | **disable**} command to enable or disable the NTP service.

Example:

```
Device# configure ntp enable
```

Step 4 Use the **configure ntp timezone** *string* command to configure the NTP timezone.

Example:

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

Step 5 Use the **show ntp config** command to validate the NTP configuration and status.

Example:

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

Step 6 Use the **show ntp** command to check if device can sync up time with NTP server.

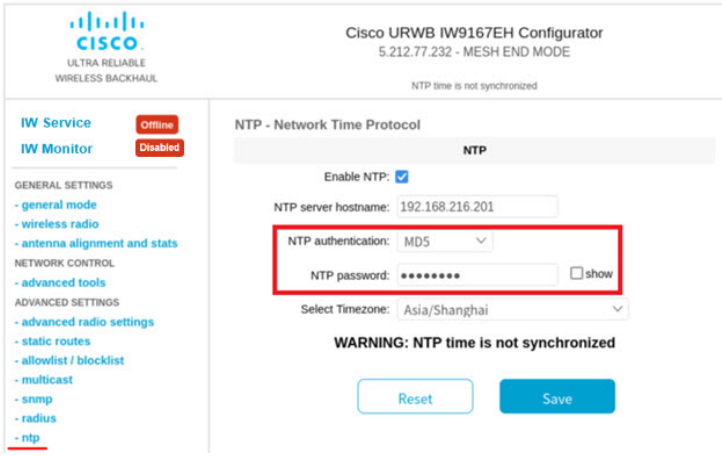
Example:

```
Device# #show ntp
Stratum Version Last Received  Delay    Offset  Jitter    NTP server
1          4      9sec ago    1.840ms -0.845ms 0.124ms 192.168.216.201
```

Configure NTP using GUI

This topic provides the graphical interface configuration steps for synchronizing device clocks with network time servers.

Figure 7: NTP GUI



Validate radio mode for URWB

To validate Radio mode, use the show commands described here.

```
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
```

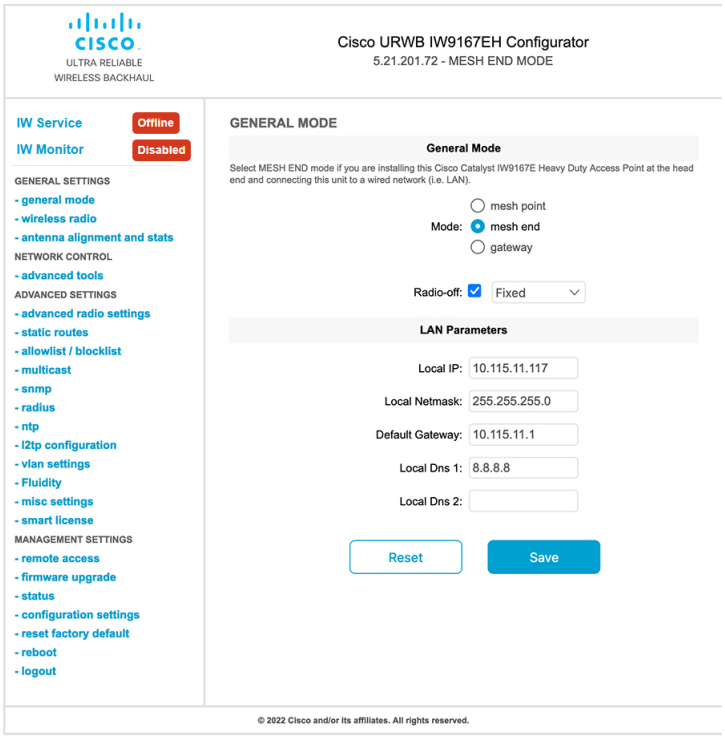
Configure radio-off mode using GUI

This task configures Radio-off mode to optimize wireless network performance.

Use this procedure when setting up Catalyst IW9167E access points at the head end that will be connected to a wired network such as LAN.

Procedure

Step 1 Choose either **Fixed** or **Fluidity** mode for **Radio-off** configuration.



Step 2 Select mode as **mesh end** when installing the Catalyst IW9167E access point at the head end and connecting this device to a wired network such as LAN.

Configure Radio mode using GUI

Configure the Radio mode using the GUI to set the operating frequency and enable wireless connections between devices.

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

Before you begin

Follow these steps to configure a Radio mode using GUI:

Procedure

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



Step 2 In the **WIRELESS RADIO** section, choose Radio 1 Role as **Fluidmax Primary** with FluidMAX Cluster ID.

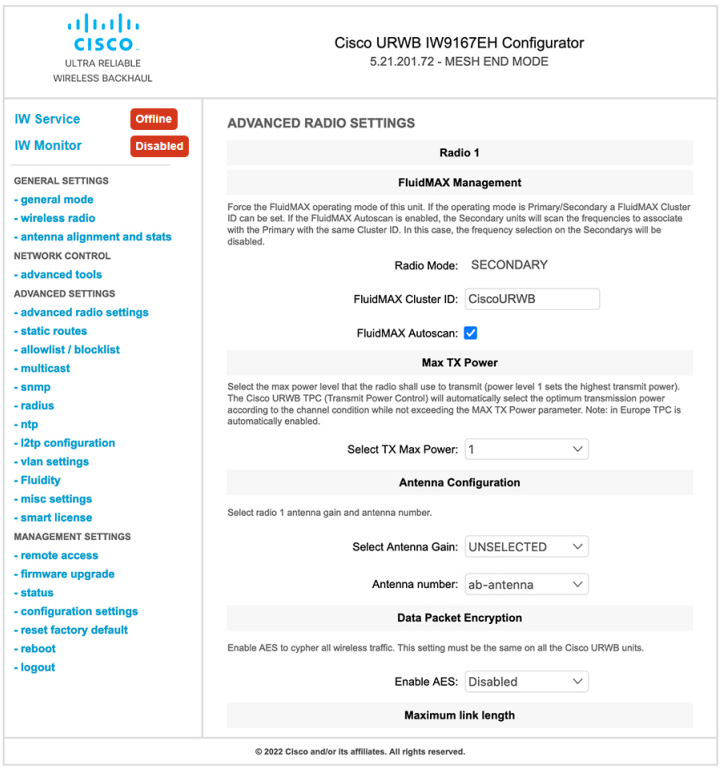
In this scenario, the frequency selection for the Primary is enabled and Secondary is disabled. In the **ADVANCED RADIO SETTINGS** window, go to **Max TX Power** section, and choose power level as 1 from the **Select TX Max Power** drop-down list and URWB transmission power control (TPC) automatically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



Note
In Europe TPC is automatically enabled.

Step 3 In the **WIRELESS RADIO** section, choose Radio 1 Role as **Fluidmax Secondary** with FluidMAX Cluster ID.

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



Note
In Europe TPC is automatically enabled.

Step 4 In the **Fluidity SETTINGS** section, choose **Unit Role** as **Infrastructure** from the drop-down list.

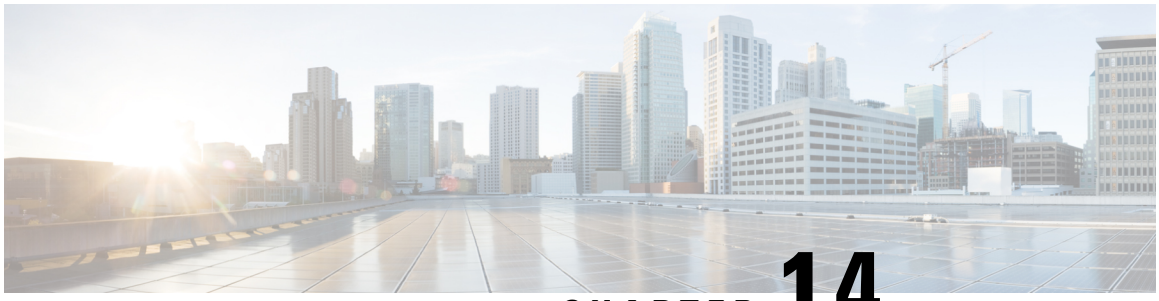
When the device acts as the entry point of the infrastructure for the mobile vehicles or choose unit role as **Infrastructure (WIRELESS relay)** only when it used as a wireless relay agent to other infrastructure unit or choose unit role as a **Vehicle** when it is mobile.

Step 5 Choose network type based on the general network architecture.

- Choose **Flat** mode from **Network Type** drop-down list, if the network belongs to single layer-2 broadcast domain.
- Choose **Multiple subnets** if the network belongs to single layer-3 broadcast domain.


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


Cisco URWB IW9167EH Configurator
5.21.201.72 - MESH END MODE
ULTRA RELIABLE WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
FLUIDITY
Fluidity Settings
The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.
Unit Role: Infrastructure
Network Type: Multiple subnets
The following advanced settings allow to fine-tune the performance of the system depending on the specific environment. Please do not alter this settings unless you have read the manual first and you know what you are doing.
The Handoff Logic controls the algorithm used by a mobile radio to select the best infrastructure point to connect to. In Normal mode, the point providing the strongest signal is selected. In Load Balancing mode, the mobile radio prefers the point which provides the best balance between signal strength and amount of traffic carried.
Handoff Logic: Standard
Reset
Save
© 2022 Cisco and/or its affiliates. All rights reserved.



CHAPTER 14

IW Service Cluster

- IW Service cluster, on page 81
- Configure IW Service Cluster from CLI, on page 81
- Verify IW Service Cluster , on page 82

IW Service cluster

A IW Service cluster is a cloud-based IoT services platform that

- monitors and manages IoT devices and networks
- provides different cluster options for access based on geolocation or manual configuration, and
- supports Auto, EU, or US cluster configurations from Cisco UIW Release 17.15.1.

IW Service cluster configuration by release

The cluster configuration options vary depending on the Cisco UIW release version.

For more information about the IW Service, see Introduction to Industrial Wireless.

Table 13: Cluster configuration by release

Release	Configuration options	Default behavior
Before Release 17.15.1	Auto only	Redirects users to US or EU cluster based on geolocation
Release 17.15.1 and later	Auto, EU, or US	Manual configuration available

Configure IW Service Cluster from CLI

This task allows you to configure the cluster settings for IW Service to optimize service connectivity based on geographical region.

You can configure the cluster setting to automatically select the optimal cluster or manually specify a regional cluster (US or EU) for your access point deployment.

Procedure

To configure the IW Service cluster in an AP, run the following command:

Device#**iw-cluster** {**auto** | **US** | **EU**}

Note
By default, the auto option is enabled.

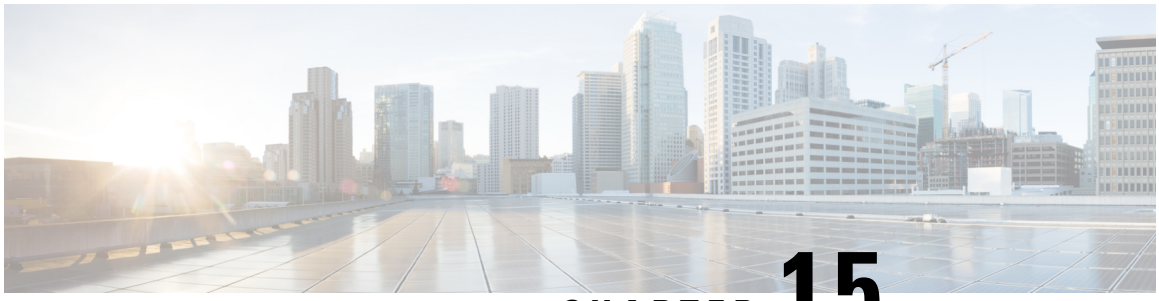
After you configure the AP with the required cluster, use the following URL to access the IW Service.

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

Verify IW Service Cluster

To verify the IW Service cluster configuration, run the show iotod-iw iw-service cluster configuration command on the device.

```
Device#show iw-servicecluster configuration IW ServiceEU Cluster
```



CHAPTER 15

Wired Interface

- Enable or disable wired interfaces, on page 83
- Configure maximum transmission unit settings, on page 84

Enable or disable wired interfaces

This task allows you to manage wired interface states by enabling or disabling specific interfaces as needed for your network configuration.

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

Before you begin

Follow these steps to enable or disable wired interfaces:

Procedure

Step 1 Configure the desired state for a specific wired interface using the CLI command.

Example:

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

Step 2 Apply the configuration to the interfaces.

Example:

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

Note that you cannot disable both interfaces simultaneously. The following error will occur if you attempt to disable both interfaces:

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

Step 3 Verify the configuration state of the wired interfaces.

Example:

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

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

Configure maximum transmission unit settings

Configure the maximum transmission unit (MTU) settings to control the maximum frame size that can be transported across the URWB network.

This setting must be configured on every access point in the URWB network to ensure consistent frame size handling across the entire network.

Procedure

Step 1 Configure the MTU value for wired interfaces.

Example:

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

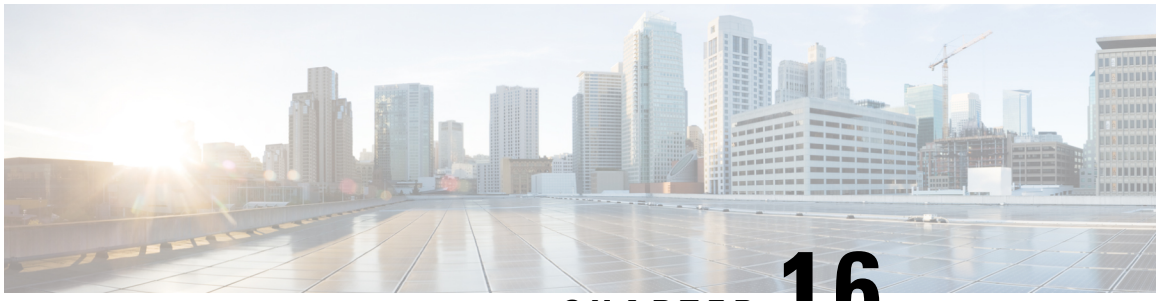
Example:

```
Device# configure wired mtu 1600
```

Step 2 Verify the MTU value for wired interfaces.

Example:

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



CHAPTER 16

Radio Antenna Settings

- Radio antenna settings, on page 85
- Validate URWB individual antenna RSSI values, on page 87

Radio antenna settings

Radio antenna settings are configuration parameters that

- manage antenna port assignments and gain values for wireless access point radios
- support multiple antenna options including self-identifying antennas (SIA), and
- enable CLI commands to control antenna port and gain management for different radio modes.

Antenna configuration details

The antenna configuration varies by Catalyst model:

- **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.
- **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.
- **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.

For more information on antennas, see Antennas and Radios.

The following sections allow you to manage antenna port and gain on each antenna for different Radio mode.

Configure antenna gain

This task sets the maximum antenna gain value to optimize wireless performance on the dot11radio interface.

You can configure antenna gain using either an integer value (1-19 dBi) or by setting it to UNSELECTED for automatic configuration. When set to UNSELECTED, the background process automatically configures the minimum supported antenna gain.

Procedure

Configure the antenna gain on the dot11radio interface.

Example:

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

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

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

Configure transmit and receive antennas

This task configures antenna transmission chains to optimize wireless communication performance and signal coverage.

Antenna configuration is essential for establishing proper wireless communication links. Different antenna chain configurations provide varying levels of signal strength and coverage patterns.

Procedure

Configure the antenna transmission chain using the following CLI command format:

Example:

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

Note
Catalyst IW9165 does not support abcd-antenna mode.

Configure transmission power

Set the maximum transmission power level on a wireless interface to control signal strength and coverage.

You can configure transmission power manually by specifying a level from 1-8, or use AUTO to let the background process automatically configure the maximum allowed power level.

Before you begin

Follow these steps to configure transmission power:

Procedure

Set the maximum transmission power level.

Example:

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

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

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

Validate URWB individual antenna RSSI values

This task allows you to view the RSSI value measured for each antenna separately on the Catalyst IW9167E, IW9165E, and IW9165D access points. Multiple RSSI values enable you to monitor the signal strength received separately by each antenna on their radio interface. This information helps identify possible issues with individual antennas or cables.

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

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

Table 14: Radio chain to antenna port mapping

Access Point	Radio Interface	Radio Chain	Antenna Port
IW9167EH	1	[A,B,C,D]	[4, 3,2,1]
	2	[A,B,C,D]	[5,6,7,8]
IW9165E	1	[A,B]	[1,2]
	2	[A,B]	[3,4]

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

Procedure

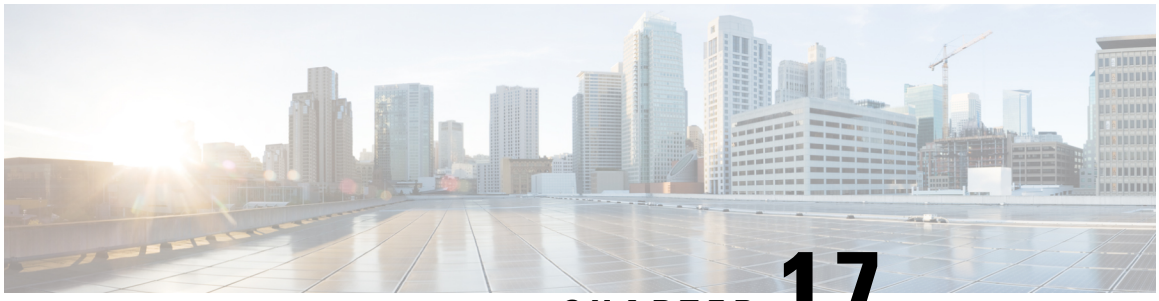
To validate the RSSI of individual antenna on an AP, use this command:

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

Replace <n> with the appropriate radio number

Example:

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



CHAPTER 17

Radio Channel and Bandwidth

- 4900-4990 MHz frequency support for US and canada with license enforcement, on page 89
- 5855-5935 MHz frequency support, on page 90
- Enabling 5855-5935 MHz frequency bands, on page 91
- Configure operating channel and bandwidth using CLI, on page 92
- Validate operating channel and bandwidth using CLI, on page 94
- Configure operating channel and bandwidth using GUI, on page 95
- UNII-3 band with DFS support, on page 95
- Configure operating channel using CLI, on page 97
- Configure channel bandwidth from CLI, on page 98
- Validate operating channel and bandwidth from CLI, on page 99
- Configure radio channel and bandwidth from GUI, on page 99
- Configure VLAN SETTINGS, on page 101
- Rules for packet management, on page 102
- Configure Fluidity using GUI, on page 103
- Configure fluidity using CLI, on page 107
- Configure fluidity coloring, on page 108

4900-4990 MHz frequency support for US and canada with license enforcement

From UIW Release 17.16.1, the Cisco Catalyst IW9167E, IW9165D, and IW9165E APs introduces additional support 4.9 GHz frequency band in URWB mode for Canada (-A) and -B (United States) domains.

When operating in the 4.9 GHz frequency bands for -A and -B domains, devices use 10 MHz and 20 MHz channel bandwidths with 5 MHz channel spacing.

The 4.9 GHz frequency bands are available on both the radio slot 1 and slot 2 and is disabled by default.

Note The -A and -B domains do not support IEEE 802.11ax rates when operating in 4.9 GHz.

Table 15: 4.9 GHz frequency bands supported for the 10 MHz and 20 MHz channel bandwidth

Channel	Channel bandwidth (10 MHz)	Channel bandwidth (20 MHz)
11	4945	NA
19	4985	NA
20	4950	4950
21	4955	4955
22	4960	4960
23	4965	4965
24	4970	4970
25	4975	4975
26	4980	4980

Enable 4900-4990 MHz frequency bands

Use this task to enable the 4.9 GHz frequency bands on the AP.

The IW Service sends the 4.9 GHz frequency band enablement configuration to the AP.

Procedure

Step 1 Configure the 4.9 GHz frequency band enablement using IW Service Cloud-Managed or offline deployment mode.

For more information on how to configure the 4.9 GHz band enablement from IW Service, see the Introduction to Industrial Wireless.

Step 2 Use the **configure dot11Radio** *interface* **4.9G high-throughput enable** command to enable 802.11an/ac rates. When enabled, the radios are allowed to operate at higher rates, limiting the power profile.

```
Device# configure dot11Radio 1 4.9G high-throughput enable
```

Note
You can use the **configure dot11Radio** *interface* **4.9G high-throughput disable** command to disable high-throughput. When disabled, the radio interface operates only at 802.11a rates, unlocking high-power profile.

5855-5935 MHz frequency support

The Intelligent Transport Systems (ITS) frequency band is a radio spectrum allocation that

- spans 5875–5935 MHz and is subdivided for specific applications

- designates 5875–5915 MHz for Road ITS applications
- allocates 5915–5935 MHz for Urban Rail Systems, such as automatic train control systems Communications-Based Train Control (CBTC), and
- requires license approval from the relevant national regulatory authority.

Channel allocation and power table specifications

From UIW Release 17.18.1, the Cisco Catalyst IW9167E, IW9165D, and IW9165E APs support the ITS frequency band within the European regulatory domain (-E PID).

A new power table is introduced for the -E domain. This allows for various frequencies from 5860 MHz to 5930 MHz at 10 MHz intervals.

Table 16: 10 MHz channel allocation in the 5.9 GHz band

Channel width	Frequency (MHz)	Channel number
10 MHz	5860	172
10 MHz	5870	174
10 MHz	5880	176
10 MHz	5890	178
10 MHz	5900	180
10 MHz	5910	182
10 MHz	5920	184
10 MHz	5930	186

Restrictions for wireless frequency configuration

Here are some unsupported scenarios:

- The 5 MHz channel width option is not supported.
- Using frequencies from 5860 MHz to 5930 MHz is allowed only for customers who have obtained local regulatory approval.
- 5930 MHz is not supported in the IW9165E AP in 17.18.1 release.

Enabling 5855-5935 MHz frequency bands

Summary

The key components involved in enabling 5855-5935 MHz frequency bands are:

- IW Service: Sends the 5.9 GHz frequency band enablement configuration to the access point and manages the deployment mode selection
- Access Point (AP): Receives the configuration and initiates the frequency band activation process
- Deployment Modes: Cloud-Managed Mode and Offline Deployment Mode provide different configuration approaches

Workflow

These stages describe the process to configure the 5.9 GHz frequency band using the IW service.

1. Choose one of the two available deployment modes for the IW Service
   - Cloud-Managed Mode
   - Offline Deployment Mode
2. Use the IW Service to enable the 5.9 GHz frequency band based on your selected deployment mode
3. The IW Service transmits the 5.9 GHz enablement configuration to the target AP.

Configure operating channel and bandwidth using CLI

This task configures the operating channel and bandwidth settings for a dot11Radio interface to optimize wireless network performance.

Use this procedure when you need to set specific channel and bandwidth parameters for wireless radio interfaces in your network configuration.

Procedure

Step 1 Use the **configure dot11Radio** *interface* **channel** *channel-id* command to set the operating channel.

Example:

```
Device# configure dot11Radio 1 channel 172
```

Valid *channel-id* range is from 1 to 256.

Step 2 Use the **configure dot11Radio** *interface* **band-width** *bandwidth* command to set the bandwidth.

Example:

```
Device# configure dot11Radio 1 band-width 10
```

Valid *bandwidth* is 10 MHz.

Step 3 Use the **configure dot11Radio** *interface* **maximum-link-length distance***distance* {**km**| **miles**} command to set the maximum wireless link distance the radio assumes for the dot11 radio interface.

Example:

```
Device# configure dot11Radio 1 maximum-link-length distance 70 km
```

Valid *distance* is 1-99.

The radio does not actually measure the peer's distance. Instead, it operates on timing assumptions tailored for links up to the configured distance.

Use Cases

- Fixed outdoor URWB links
- Point-to-point links
- Point-to-multipoint fixed infrastructure links
- Longer-distance outdoor wireless paths

Impact on Radio Timing and MAC Behavior

The configured maximum-link-length affects timing-sensitive MAC behaviors, including:

- ACK timing
- Block ACK timing
- AMPDU behavior
- Long-distance propagation tolerance
- Rate-control interpretation of retries and loss

Consequences of Misconfiguration

When the configured distance is set shorter than the physical distance, the radio's timing windows (slots) close before the signal has physical time to travel the distance and return. This causes the radio to prematurely assume the packet was lost, leading to:

- Excessive retries
- MCS fallback
- Lower effective transmit rates
- Rate-control getting stuck at a low rate

Example

If the maximum-link-length is configured as 3000 meters, the radio assumes timing suitable for links up to 3000 meters, not that it has measured the peer at 3000 meters.

Proper configuration of this parameter is critical for optimal wireless performance, especially in fixed outdoor point-to-point or point-to-multipoint deployments.

Step 4 Use the **end** command to return to privileged EXEC mode.

Example:

```
Device# end
```

Validate operating channel and bandwidth using CLI

To validate radio channel and bandwidth, use the **show** command to display configuration parameters and verify operational status.

```
Device# show dot11Radio 1 config

Interface:              enabled

Mode:                   fixed infrastructure

Frequency:              5860 MHz
Channel:                172
Channel width:          10 MHz
Antenna number:         2
TX power level:         8
TX power:               2 dBm
Antenna gain:           unselected
Maximum tx mcs:         9
High-efficiency:        disabled
Maximum tx nss:         2
RTS protection:         disabled
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

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:             33322f268bd38d6307fb52ffec9f515fe15303ac62ed375b397716bd810d511c
AES encryption:         disabled
AES key-control:        disabled
Key rotation:           disabled
Key rotation timeout:   0(second)

DFS region:             E
DFS radar role:         auto
Radar detected:         0
Indoor deployment:      disable
Rx-SOP Threshold:       0 dBm(AUTO)
Max packet retries:     32
```

Configure operating channel and bandwidth using GUI

This task allows you to set the frequency range and channel width for wireless radio operations to ensure optimal network performance.

Use this procedure when you need to configure wireless radio SETTINGS for your network device. This configuration affects the radio's operating parameters and bandwidth allocation.

Procedure

Step 1 Choose **GENERAL SETTINGS > wireless radio** and go to Radio 1 Settings:

Step 2 From the **Role** drop-down list, select Fixed or Fluidity.

Step 3 From the **Frequency (MHz)** drop-down list, select the frequency range. See Table 1 for a list of valid frequencies.

Step 4 From the **Channel Width (MHz)** drop-down list, select 10 MHz.

Step 5 Click **Save**.

Step 6 (Optional) Choose **MANAGEMENT SETTINGS > status**. This page displays the status of radio channel, bandwidth configuration, and specific information of each wireless interface.

UNII-3 band with DFS support

Dynamic Frequency Selection (DFS) is a wireless communication feature that scans for radar signals in real-time, automatically adjusts the frequency on a DFS-enabled radio to avoid interference with radar systems, and ensures coexistence with radar systems, especially in the 5 GHz frequency band. DFS is a regulatory requirement for devices operating in the 5 GHz band to prevent interference with critical radar systems, such as weather or military radars.

The Unlicensed National Information Infrastructure (UNII-3) frequency band is part of the radio frequency spectrum ranging from 5725 MHz to 5825 MHz, as defined by the US Federal Communications Commission (FCC).

UNII-3 frequency band support in Great Britain

From Cisco UIW Release 17.18.1, the Cisco Catalyst IW9165D and IW9167EH APs support the UNII-3 band with DFS channels. These channels range from channel 149 (5745 MHz) to channel 165 (5825 MHz) under the country code GB in the Rest of the World (ROW) regulatory domain (-ROW PID).

Table 17: UNII-3 band support on Cisco Catalyst IW9165 and 9167 APs (Great Britain)

Cisco UIW Release	Access Points	Regulatory Domain	Country Code	Frequency Range
17.18.1	IW9165D IW9167EH	-ROW	GB	5745 to 5825 MHz

Table 18: Supported UNII-3 band channels (Great Britain)

Channel Number	Center Frequency (MHz)
149	5745
153	5765
157	5785
161	5805
165	5825

How DFS works

Workflow

These stages describe how the DFS process works:

1. Radar signal scanning: DFS-enabled radios continuously monitor the operating frequency band for radar signals to ensure compliance with regulatory requirements.
2. Radar signal detection: If a radar signal is detected, the device identifies the specific frequency being used by the radar.
3. Frequency avoidance: The radio dynamically selects and prepares to switch to a new frequency within the allowed spectrum to avoid interference with the radar.
4. Channel availability check: Before switching, the device performs a channel availability check to confirm that the new frequency is clear of radar signals or other interference.
5. Seamless communication: Once the new frequency is validated, the device switches to it and resumes normal communication without disrupting network operations.

Benefits

APs operating in the UNII-3 band provide enhanced wireless connectivity and performance advantages in radar environments.

APs operating in the UNII-3 band

- operates within the 5.8 GHz frequency range of 5745 MHz to 5825 MHz
- helps to avoid radar interference by switching frequencies, and
- improves wireless connectivity and performance in radar environments.

Restrictions for UNII-3 band with DFS support

These are the restriction for the UNII-3 band with DFS support.

- Supports 10 MHz and 160 MHz channel width only.

- Use of 5.8 GHz frequencies from 5745 MHz to 5825 MHz is permitted only for customers with local regulatory approval.

Configure DFS channel

Configure the DFS (Dynamic Frequency Selection) channel to enable wireless operation on specific regulatory frequencies.

Use this procedure to configure the DFS channel. DFS channels allow wireless devices to operate on specific frequencies while avoiding interference with radar systems.

Before you begin

Ensure that the device's regulatory domain is ROW.

Follow these steps to configure DFS channel:

Procedure

Step 1 Use the **configure countrycode** *country-code* command to set the country code.

Example:

```
Device# configure countrycode GB
```

Step 2 (Optional) Use the **show controllers dot11Radio** *radio* **frequency** command to verify the UNII-3 band with DFS support channels.

Example:

```
Device# show controllers dot11Radio 1 frequency
wifi1     Link encap:Ethernet  HWaddr 8C:84:42:92:EA:C0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:2699
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

Configured Frequency: 5745Mhz Channel: 149 20MHz (DFS enabled)
Serving Frequency: 5745Mhz Channel: 149 20MHz
Allowed Frequency: * Dynamic Frequency Selection (DFS) only
  *5500MHz(100) *5520MHz(104) *5540MHz(108) *5560MHz(112) *5580MHz(116) *5600MHz(120) *5620MHz(124)
 *5640MHz(128)
  *5660MHz(132) *5680MHz(136) *5700MHz(140) *5745MHz(149) *5765MHz(153) *5785MHz(157) *5805MHz(161)
 *5825MHz(165)
```

Configure operating channel using CLI

Configure the operating channel for wireless devices to operate in the 4.9 GHz frequency band with URWB mode support.

From UIW Release 17.15.1, the Cisco Catalyst IW9167E, IW9165D, and IW9165E AP supports 4.9 GHz frequency band in URWB mode for -Q domain (Japan). When operating at 4.9 GHz frequency band, the device supports only 20 MHz channel bandwidth.

The -Q domain supports 802.11ax rates when operating in 4.9 GHz.

Table 19: Supported channels and frequencies for the 4.9 GHz band

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

Procedure

Step 1 Use the **configure dot11Radio** *interface* command to configure the wireless device with radio interface number.

Example:

```
Device# configure dot11Radio 1
```

The valid values are 1 and 2.

Step 2 Use the **configure dot11Radio** *interface* **channel** *channel-id* command to set the operating channel id.

Example:

```
Device# configure dot11Radio 1 channel 192
```

The valid range for the channel is 1 to 256.

Step 3 Use the **end** command to return to privileged EXEC mode.

Example:

```
Device# end
```

Configure channel bandwidth from CLI

This task configures the channel bandwidth for radio interfaces to optimize wireless network performance and manage spectrum usage.

Channel bandwidth configuration is performed on radio interfaces to set the appropriate bandwidth for wireless communication. Different radio interfaces support different bandwidth options depending on their capabilities.

Procedure

Step 1 Use the **configure dot11Radio** *interface* command to configure the radio interface number.

Example:

```
Device# configure dot11Radio 1
```

The valid values are 1 and 2.

Step 2 Use the **configure dot11Radio** *interface* **band-width** *bandwidth* command to set channel bandwidth.

Example:

```
Device# configure dot11Radio 1 band-width 20
```

- Radio 1 supports 20, 40, and 80 MHz bandwidths.
- Radio 2 supports 20, 40, 80, and 160 MHz bandwidths.

Step 3 Use the **end** command to return to privileged EXEC mode.

Example:

```
Device# end
```

Validate operating channel and bandwidth from CLI

To validate radio channel and bandwidth, use the show command shown in the 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

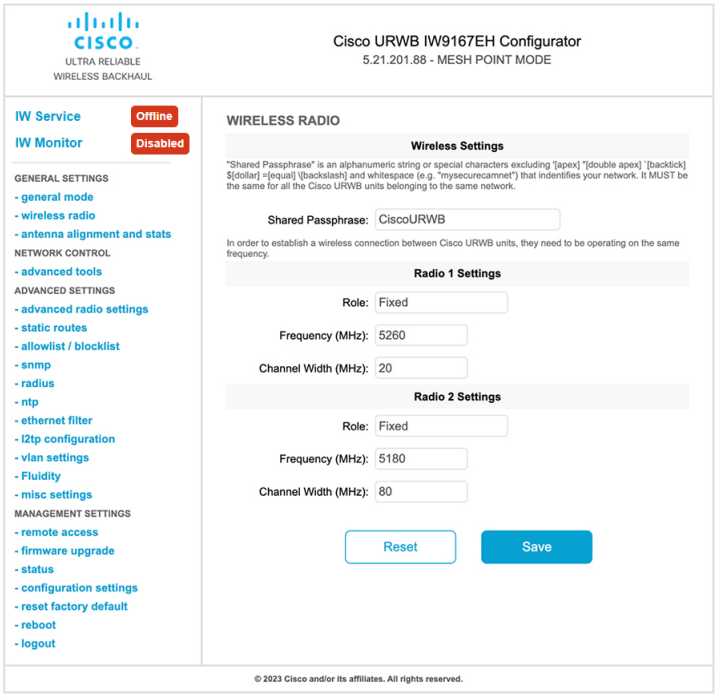
Configure Radio channel and bandwidth to set the operating channel ID, Radio mode as Fluidity or fixed infrastructure and set the Radio frequency range and bandwidth.

Use this configuration to optimize wireless network performance by properly setting radio parameters for your environment.

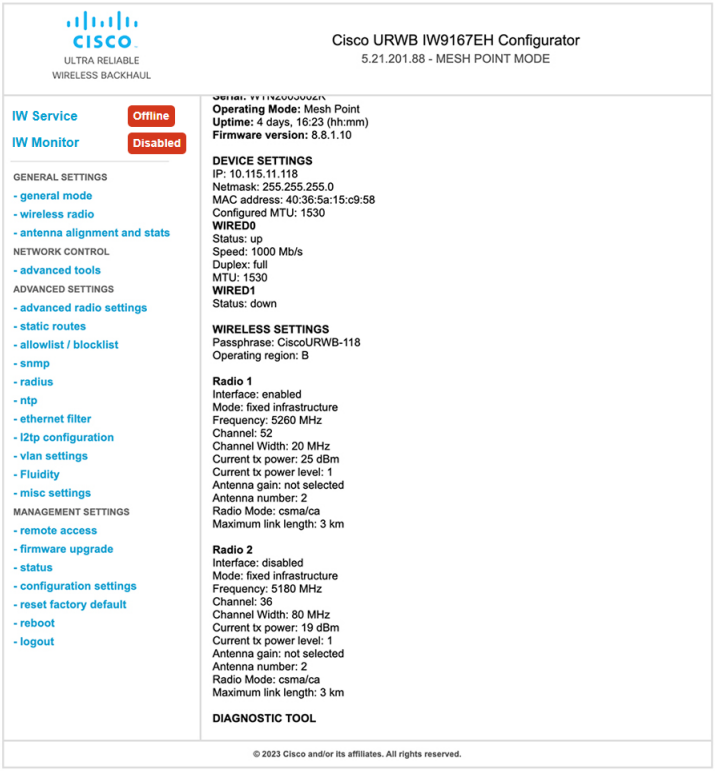
Procedure

Step 1 Configure Radio channel and bandwidth to set the operating channel ID, Radio mode as Fluidity or fixed infrastructure and set the Radio frequency range and bandwidth.

The following image shows the configuration of Radio channel and bandwidth:



Step 2 Following image shows the status of Radio channel and bandwidth configuration and specific information of each wireless interface.



Configure VLAN SETTINGS

Configure VLAN SETTINGS to enable the access point to connect to VLANs within the local wireless network using specific management and native VLAN identifiers.

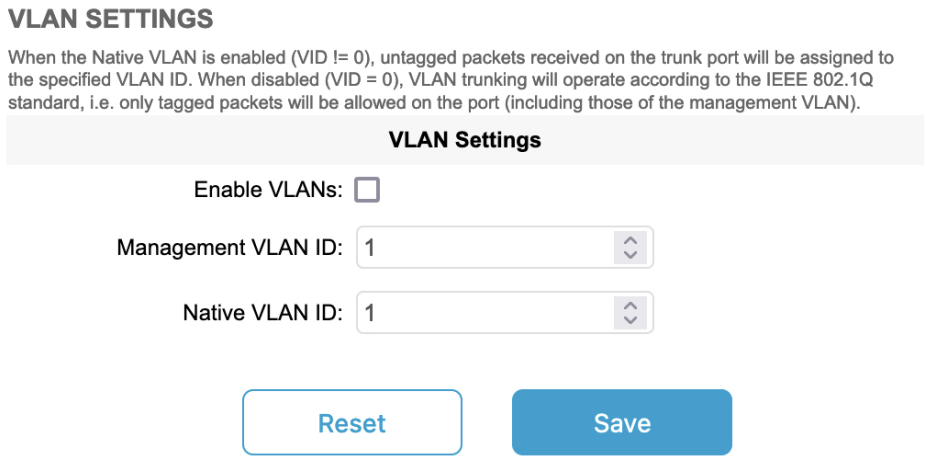
Default VLAN configuration parameters for the access point are:

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

Procedure

Step 1 In the **ADVANCED SETTINGS**, click **VLAN SETTINGS**.

The **VLAN SETTINGS** window appears.



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

Step 3 Enter the management identification number of the VLAN in the **Management VLAN ID** field.

For detailed info about VLAN SETTINGS and packet management, see Rules for Packet Management.

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

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

Step 5 Click **Save**.

Rules for packet management

This topic provides the rules for packet management in traffic management scenarios, including classification parameters for incoming and outgoing data packets.

Traffic management

The incoming data packets are classified based on these parameter values:

Table 20: Access port rules management for incoming packets with an access point in smart mode

Untagged packet	If native VLAN is ON, then the packet is allowed (tagged with NVID) If native VLAN is OFF, then the packet is dropped
Tagged packet (any VID without any check)	Packet allowed with original tag

Table 21: Access port rules management for outgoing packets with an access point in smart mode

Packets from the access points (for example: IW Service interface)	Packet tagged with MVID

Signaling traffic	Packet tagged with MVID
Tagged with valid VID (1–4094), but not with NVID	Packet allowed (tagged)
Tagged with null VID (0) or NVID	Packet allowed (untagged)

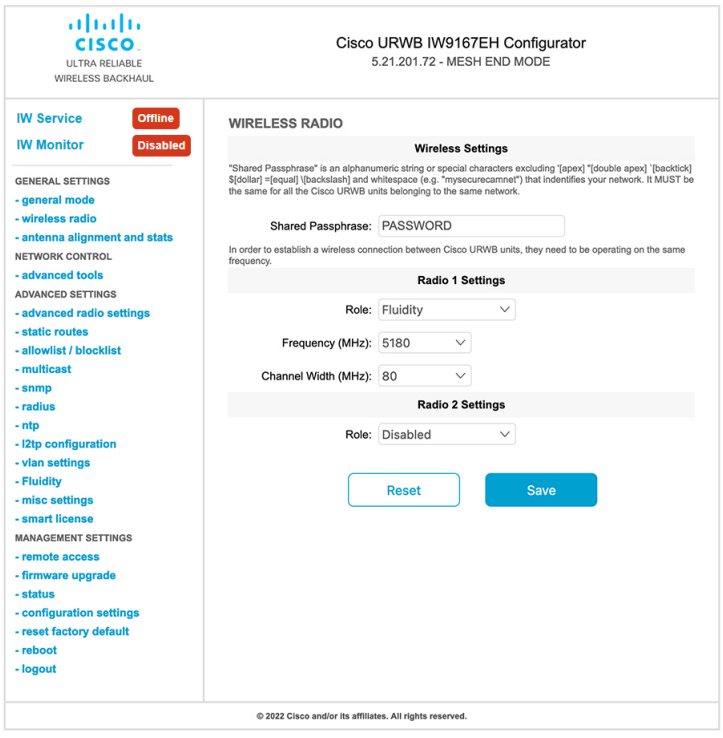
Note The packets transmitted through the Cisco VIC SFP+ interface is always tagged with a VLAN header. The interface transmits outgoing packets are classified as untagged with an IEEE 802.1p header with a VLAN ID tag of 0.

Configure Fluidity using GUI

Procedure

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

The **WIRELESS RADIO** window appears.



Step 2 Choose **Fluidity** from the **Role** drop-down list.

Step 3 In the **ADVACED SETTINGS** , click **Fluidity** .

The **FLUIDITY** window appears.

Step 4 In the **Fluidity Settings** , choose a **Unit Role** from the drop-down list:

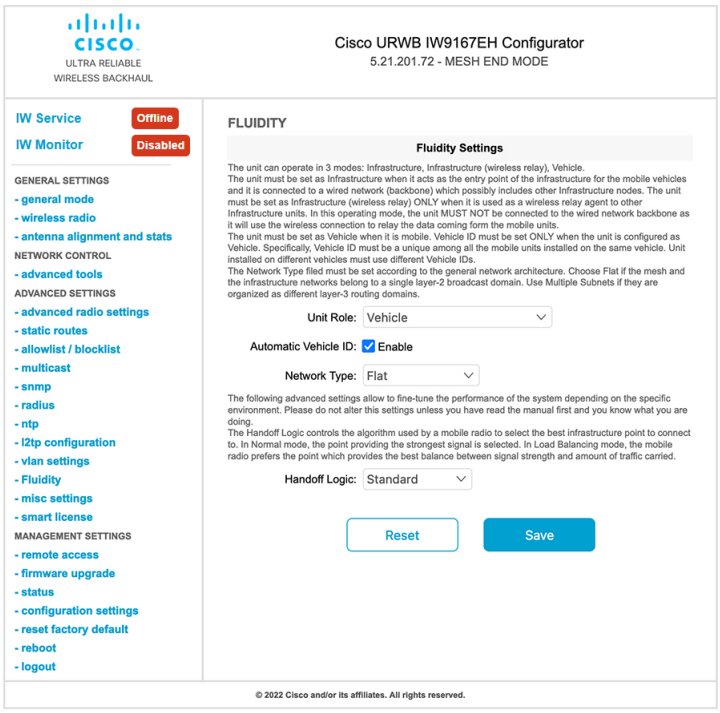
- Infrastructure
- Infrastructure (wireless relay)
- Vehicle

Note

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

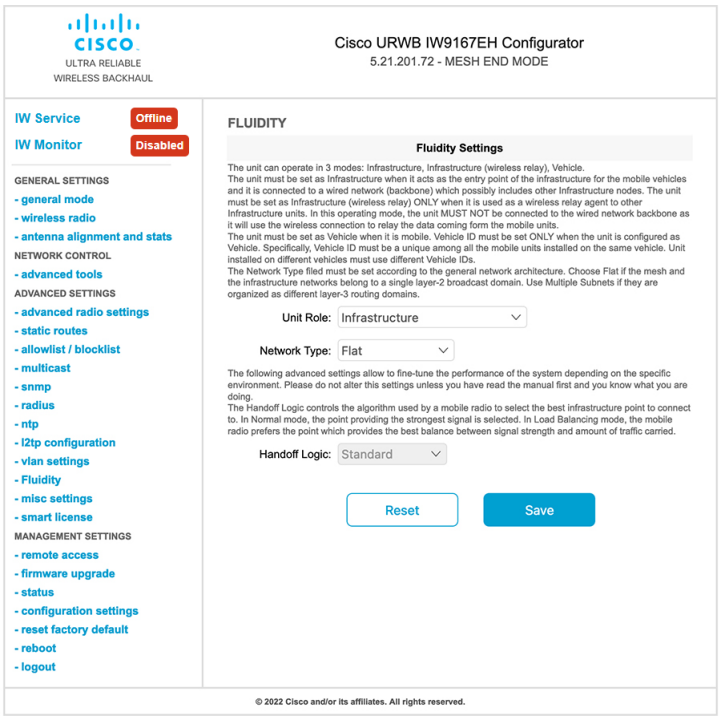
Step 5 Check the **Automatic Vehicle ID** check box to automatically set the Vehicle ID for mobile units.



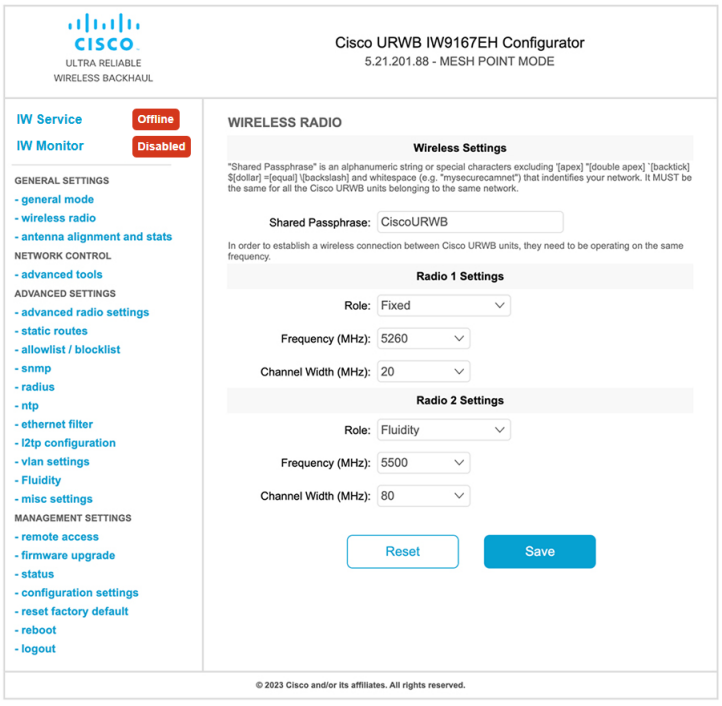


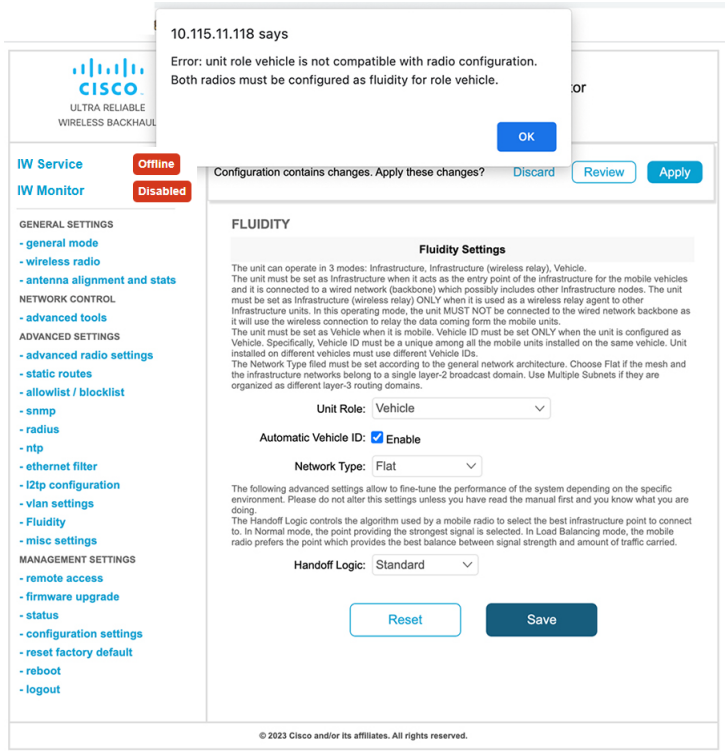
The Fluidity configuration is applied. The following images illustrate the wireless interface configured in infrastructure mode and the requirement that both radios must be configured as Fluidity when the role is set to Vehicle.





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





Configure fluidity using CLI

Configure Fluidity mode on radio interfaces to enable enhanced wireless connectivity and performance for vehicle communications.

Fluidity mode is configured on radio interfaces to support specific communication roles.

Before you begin

Follow these steps to configure fluidity using CLI:

Procedure

Step 1 Use the **configure dot11Radio** *interface* **mode fluidity** command to configure Fluidity mode on the desired radio interface:

Example:

```
configure dot11Radio 1 mode fluidity
```

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

Step 2 For Vehicle role, configure both radios in Fluidity mode:

Example:

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

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

Configure fluidity role using CLI

Configure the Fluidity role to establish whether the device operates in infrastructure mode, vehicle mode, or as a wireless relay.

The Fluidity role determines how the device functions within the network topology. Infrastructure mode provides fixed network services, while vehicle modes support mobile connectivity with automatic or manual ID selection.

Procedure

Step 1 Use the **configure fluidity id** command to configure the Fluidity role (infrastructure or mobile).

Example:

```
Device# configure fluidity id
```

Step 2 Use the **configure fluidity id** [**vehicle-auto** | **infrastructure**| **vehicle-id**| **wireless-relay**] command to configure Fluidity id mode.

Example:

```
Device# configure fluidity id wireless-relay
```

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

Step 3 Use the **end** command to return to privileged EXEC mode.

Example:

```
Device# end
```

Step 4 Use the **write** command to save the configuration.

Example:

```
Device# write
```

Configure fluidity coloring

Fluidity coloring enables wayside or outside devices (Fluidity infrastructure devices) to be given specific color codes to enhance or drive the handoff process. With the standard configuration handoff decision is made based on received signal strength indication (RSSI).

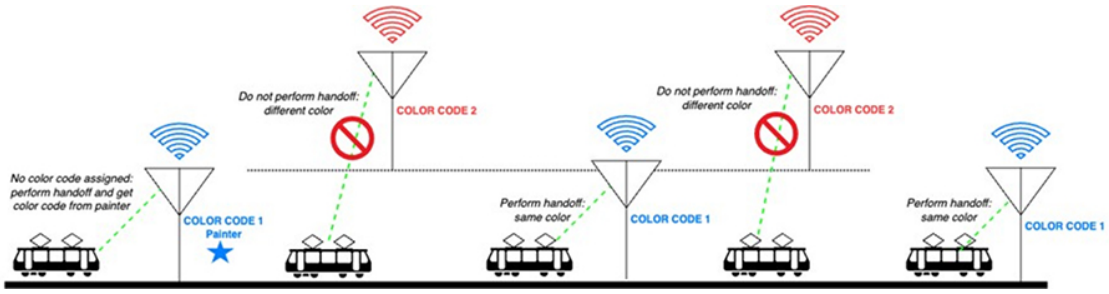
Typical use case: When a train is travelling on one side of the track in one direction (metro line with single tunnel for both track directions) and does not need to connect to the access point located on the opposite side

of the tunnel, so mark the access point on each side with a different color to prevent occasional handovers to infrastructure devices on the opposite track.

Fluidity Coloring is introduced from UIW Release 17.12.1. The painter is a key role for wayside or outside device (Fluidity infrastructure device).

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

Figure 8: Fluidity coloring



The process of Fluidity coloring as follows:

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

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

Table 22: Fluidity coloring role

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

Procedure

Step 1 Use the **configure fluidity color mode** {**disabled** | **enabled**} command to configure the Fluidity color mode.

Example:

```
Device# configure fluidity color mode enabled
```

Step 2 Use the **configure fluidity color value** command to configure the Fluidity color value.

Example:

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

Example (painter):

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

Example (non-painter):

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

Example (clear):

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

Step 3 Use the **show fluidity config** command to verify the Fluidity color configuration.

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
```

Step 4 Use the **configure fluidity color rssi-threshold** *threshold* command to configure fluidity coloring RSSI threshold.

Example:

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

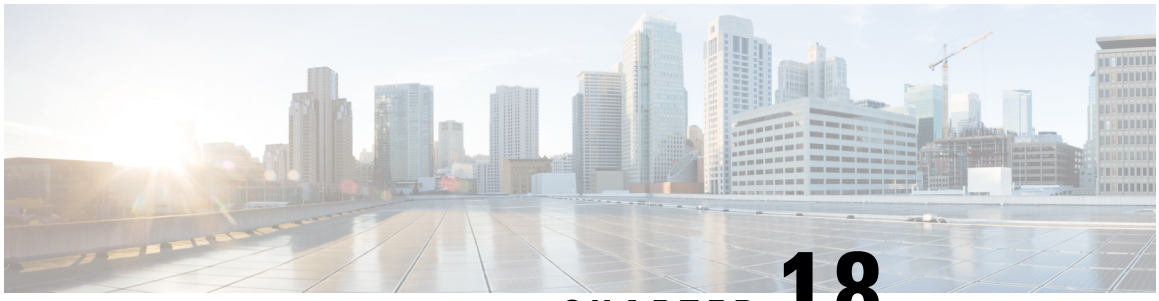
Device# configure fluidity color rssi-threshold 55
```

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

Step 5 Use the **show fluidity config** command to verify the fluidity coloring RSSI threshold configuration.

Example:

```
Device# show fluidity config
.
.
.
Color: enabled, current: 0
Color min RSSI threshold: 55
```



CHAPTER 18

High Efficiency (802.11 ax)

- Configure and validate high efficiency, on page 113
- Configure global gateway using GUI, on page 114
- Configuring Guard Interval for HE, on page 116

Configure and validate high efficiency

This task enables or disables 802.11ax High Efficiency (HE) mode on URWB devices and validates the configuration.

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

Procedure

Step 1 Use the **configure dot11Radio** {**1** | **2**} **high-efficiency** {**enable** | **disable**} command to enable or disable HE mode.

Example:

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

Step 2 Use the **configure dot11Radio** {**1** | **2**} **mcs maxmcs** *mcs-index* command to configure maxmcs.

Example:

```
Device# configure dot11Radio 1 mcs maxmcs 11
```

Note
The default maxmcs is 9.

Step 3 Use the **show dot11Radio** {**1** | **2**} **config** command to validate HE mode.

Example:

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

Step 4 Use the **show eng-stats** command to view engineering statistics:

Example:

```
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
```

Configure global gateway using GUI

Configure global gateway MODE to automatically enforce MPLS Layer 3 functionality on your device.

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

Procedure

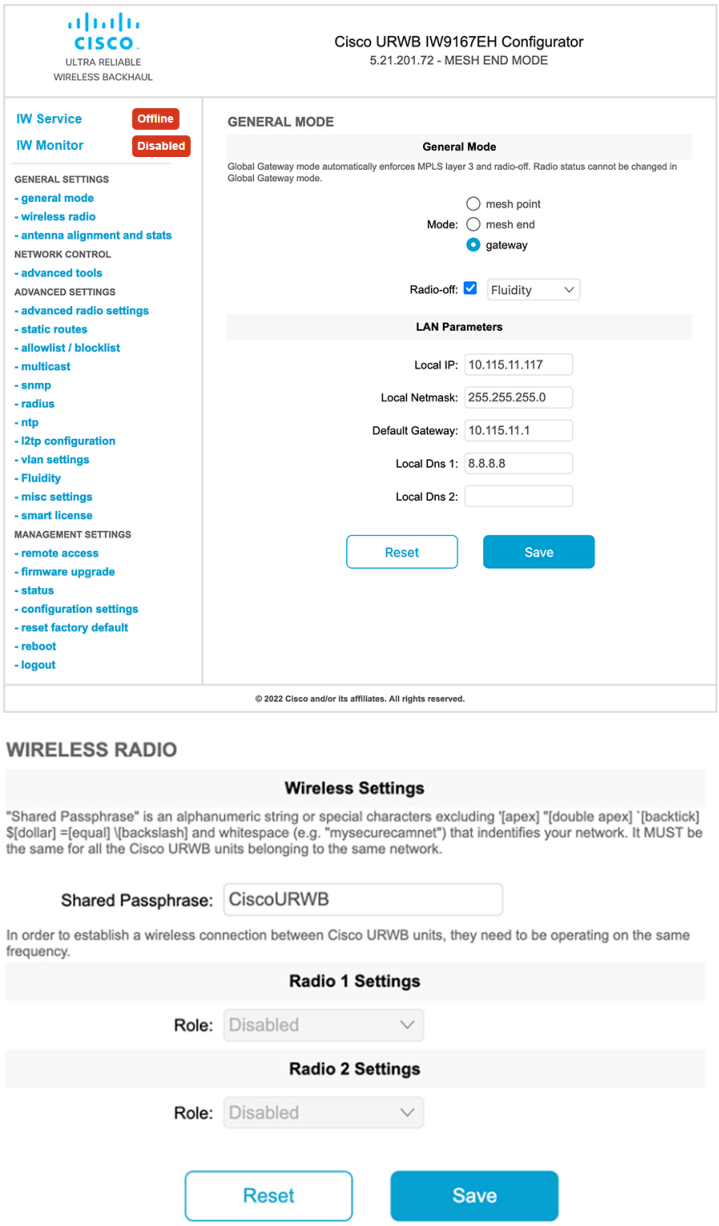
Step 1 In the **GENERAL SETTINGS**, click **GENERAL MODE**.

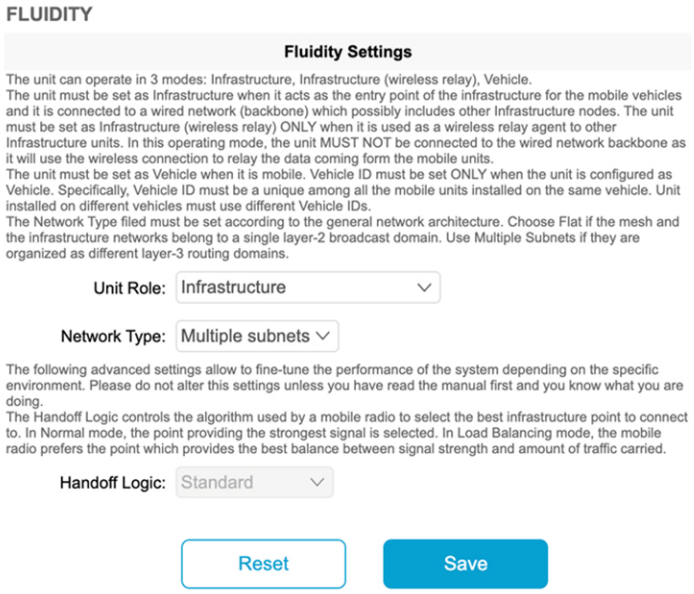
The **GENERAL MODE** window appears.

Step 2 Click **gateway** from **MODE**.

Following images shows the GUI configuration of global gateway mode:

Figure 9: Global gateway mode





Configuring Guard Interval for HE

Configures the guard interval for HE to improve link reliability in long-range outdoor deployments.

Procedure

Step 1 Use the **configure dot11Radio** *interface* **guard-interval** [*gi*] command to configure the guard interval.

Example:

```
Device# configure dot11Radio 1 guard-interval 1600
```

Guard interval values include:

- 3200: Configures 3200 ns guard interval (supported only in HE mode).
- 1600: Configures 1600 ns guard interval (supported only in HE mode).
- 800: Configures 800 ns guard interval (default guard interval mode and disable mode in HT, VHT, and HE).
- 400: Configures 400 ns guard interval (supported in HT and VHT modes).

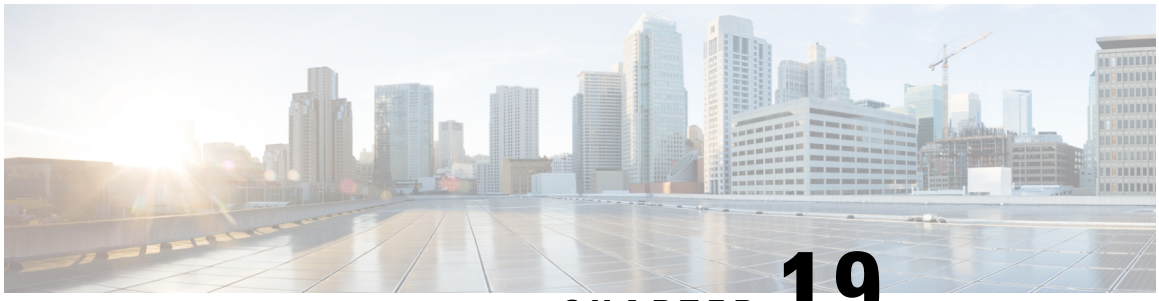
Step 2 Use the **show dot11Radio** *interface* **show** command to verify the configuration.

Example:

```
Device# show dot11Radio 1 show

Maximum tx mcs: 9
High-efficiency : enabled
Maximum tx nss : 2
```

```
RTS protection : disabled
guard-interval : 1600 ns
```



CHAPTER 19

Roaming Parameters

- Packet retries limitation, on page 119
- Configure maximum retry limit for packet retransmissions using CLI, on page 119
- Verify maximum retry limit for packet retransmissions using CLI, on page 120

Packet retries limitation

Starting from UIW Release 17.15.1, you can set the limit for the packet retransmissions of unicast packets. This includes both aggregate and non-aggregate packets.

The maximum retry limit for packet retransmission is 32.

Configure maximum retry limit for packet retransmissions using CLI

This task configures the maximum retry limit for packet retransmissions on the access point, which helps control network reliability and performance.

Configuring the maximum retry limit for packet retransmissions allows you to control how many times the access point attempts to retransmit packets before giving up, which can help optimize network performance and reliability.

Procedure

Use the **configure dot11Radio** *interface* **packet retries** *retry-count* command to onfigure the maximum retry limit for packet retransmissions on the access point.

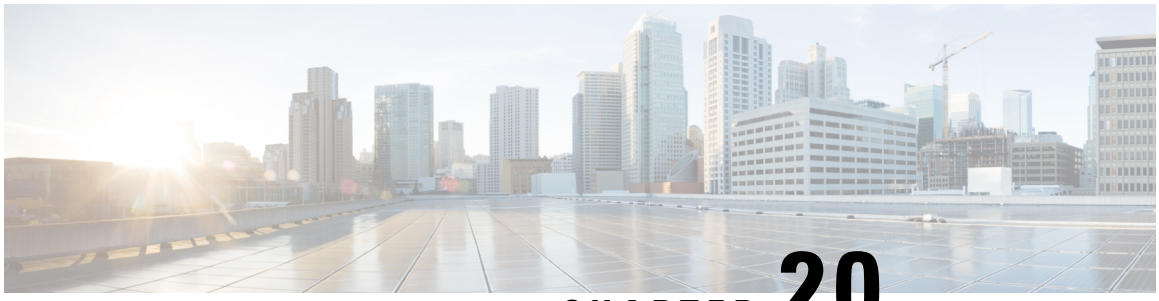
Example:

```
Device# configure dot11Radio 1 packet retries 32
```

Verify maximum retry limit for packet retransmissions using CLI

View the current maximum retry limit configuration for packet retransmissions on the radio interface.

```
Device# show dot11Radio 1 config
.
.
.
DFS region:             Q
DFS radar role:         auto
Radar detected:         0
Indoor deployment:      disable
Rx-SOP Threshold:       0 dBm(AUTO)
Max packet retries:     32
```



CHAPTER 20

Key Controller (Wireless Security)

- Key controller wireless security, on page 121

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.

A key controller is a wireless security protocol that

- implements a key rotation strategy for Catalyst IW9167E to support wireless security to standard Wi-Fi Protected Access (WPA) protocols
- involves a packet exchange between two devices with different stages corresponding to different states of each device, and
- uses algorithm flow controlled by a set of timers scheduled periodically to generate new Pairwise Transient Key/Group Transient Key for packet encryption.

Security benefits

The more frequently keys are updated, the lesser amount of information is leaked in the event of an attack.

Configure key controller from CLI

Configure a key controller to enable Advanced Encryption Standard (AES) encryption, key control, and key rotation functionality on radio interfaces to enhance wireless security.

Key controller configuration is necessary when you need to implement advanced encryption and key management for wireless radio interfaces in your network infrastructure.

Procedure

Step 1 Use the **configure dot11Radio** *interface* **crypto aes enable** command to enable Advanced Encryption Standard (AES) on Radio.

Example:

```
Device# configure dot11Radio 1 crypto aes enable
```

Step 2 Use the **configure dot11Radio** *interface* **crypto key-control enable** command to enable key controller.

Example:

```
Device# configure dot11Radio 1 crypto key-control enable
```

Step 3 Use the **configure dot11Radio** *interface* **crypto key-control key-rotation enable** command to enable key rotation.

Example:

```
Device# configure dot11Radio 1 crypto key-control key-rotation enable
```

Step 4 Use the **configure dot11Radio** *interface* **crypto key-control key-rotation** *value* command to set key rotation timer.

Example:

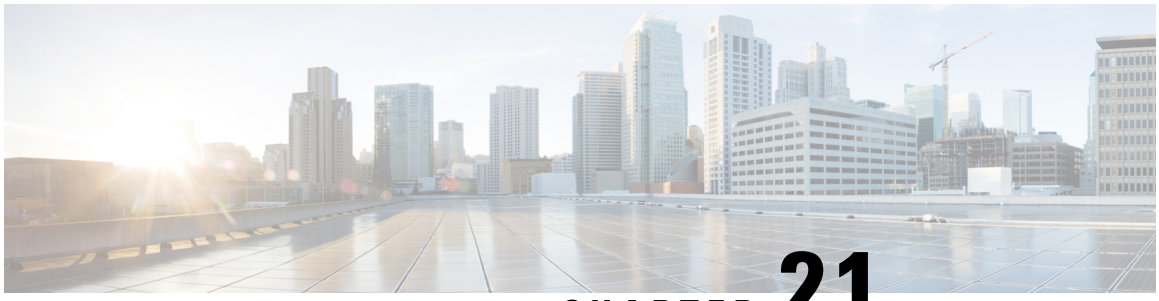
```
Device# configure dot11Radio 1 crypto key-control key-rotation 3600
```

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

Validate key controller from CLI

To validate a key controller, use this **show** command:

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



CHAPTER 21

SNMP

• Simple network management protocol, on page 123

Simple network management protocol

Simple network management protocol (SNMP) is a network protocol that enables network management functionalities in URWB software.

SNMP communication process

The SNMP communication process involves the following steps:

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

Figure 10: SNMP process



Configure SNMP from CLI

Configure SNMP to enable monitoring and management of network devices through network management systems.

SNMP configuration allows network management systems to monitor device status and receive trap notifications. Configure all parameters before enabling SNMP.

Note

- Before enabling the SNMP feature using CLI, you must configure all SNMP parameters.
- Disabling the SNMP feature automatically removes all related configurations.

Before you begin

Follow these steps to configure SNMP from CLI:

Procedure

Step 1 Use the **configure snmp** {**v2c**| **v3**} command to configure the SNMP protocol version.

Example:

```
Device# configure snmp version v2c
```

Step 2 Configure version-specific parameters.

a) Use the **configure snmp v2c community-id** *length* command to configure the community ID for SNMP v2c.

Example:

```
Device# configure snmp v2c community-id 64
```

Valid values for *length* ranges from 1 to 64.

b) Use the **configure snmp v3 username** *length* command to configure the username for SNMP v3.

Example:

```
Device# configure snmp v3 username 32
```

Valid values for *length* ranges from 1 to 32.

c) Use the **configure snmp v3 password** *length* command to configure the user password for SNMP v3.

Example:

```
Device# configure snmp v3 password 8
```

Valid values for *length* ranges from 8 to 64.

d) Use the **configure snmp auth-method** {**md5**| **sha**} command to configure the authentication protocol for SNMP v3.

Example:

```
Device# configure snmp v3 password 8
```

Valid values for *length* ranges from 8 to 64.

e) Use the **configure snmp encryption** {**des**| **aes**| **none**} command to configure the encryption protocol for SNMP v3.

Example:

```
Device# configure snmp encryption aes
```

f) Use the **configure snmp secret** *length* command to configure the encryption passphrase for SNMP v3.

Example:

```
Device# configure snmp v3 password 8
```

Valid values for *length* ranges from 8 to 64.

Step 3 Use the **configure snmp nms-hostname**{*hostname*| *ip-address*} command to configure the SNMP hostname or IP address.

Example:

```
Device# configure snmp nms-hostname cisco.com
```

Step 4 Configure trap settings.

a) Use the **configure snmp periodic-trap** {**enable**| **disable**} command to configure the periodic trap settings.

Example:

```
Device#configure snmp periodic-trap enable
```

b) Use the **configure snmp trap-period** *period* command to configure the notification trap period for periodic SNMP traps.

Example:

```
Device#configure snmp trap-period 2147483647
```

Valid values for *period* is from 1-2147483647.

Notification value trap period measured in minutes.

c) Use the **configure snmp event-trap** {**enable**| **disable**} command to configure event traps.

Example:

```
Device# configure snmp event-trap enable
```

Step 5 Use the **configure snmp enable** command to enable SNMP functionality.

Example:

```
Device# configure snmp enable
```

What to do next

Example configurations:

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
```

To disable SNMP configuration:

```
Device#configure snmp disabled
```

Disabling SNMP clears all sensitive information, including credentials. To enable SNMP again, specify all required values

Validate SNMP from CLI

Use the **show snmp** command to validate the SNMP.

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

Configure SNMP version v2c using GUI

This task enables SNMP version v2c on access points to allow network monitoring and management through SNMP operations and trap notifications.

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

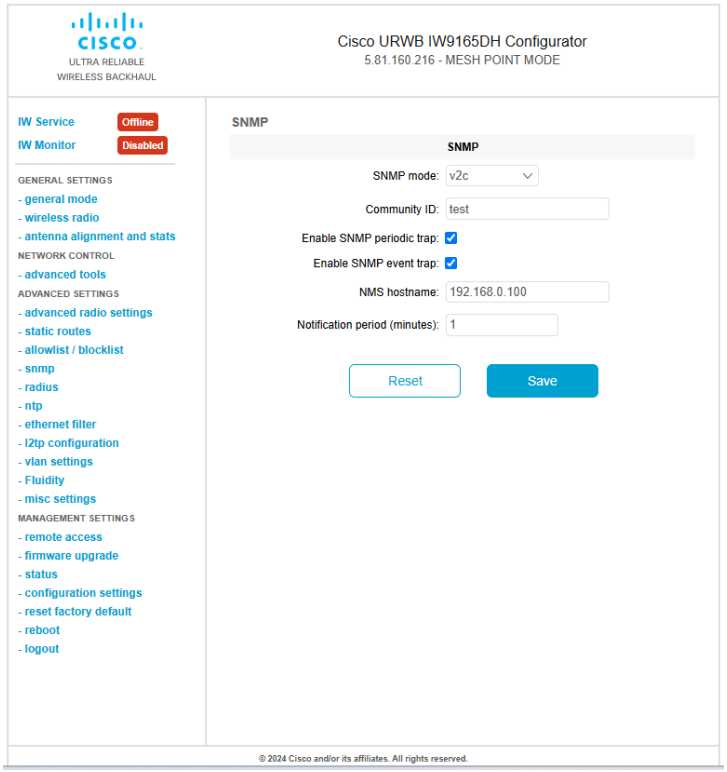
Before you begin

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

Procedure

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

The **SNMP** window appears.



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

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

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

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

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

Step 5 Click **Save**.

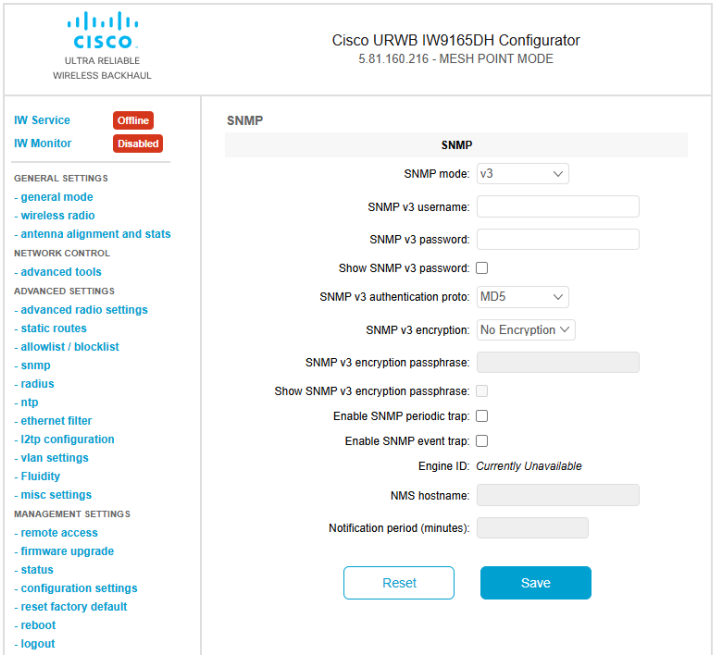
Configure SNMP version v3 using GUI

Configure SNMP version v3 to enable secure network monitoring and management of access points.

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

Procedure

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



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

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

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

Step 4 Choose the authentication type from the **SNMP v3 authentication proto** drop-down list.

The available options are:

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

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

Step 5 Choose the appropriate encryption protocol from the **SNMP v3 encryption** drop-down list.

The available options are:

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

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

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

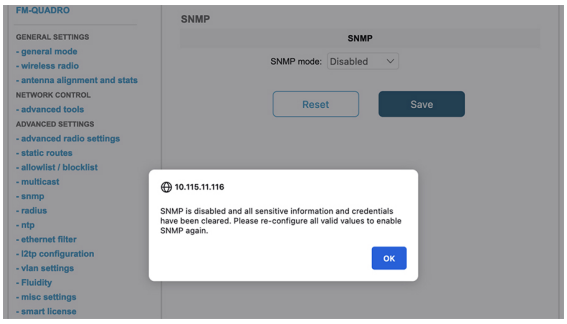
Step 7 Check the **Enable SNMP periodic trap** check box to enable the periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.

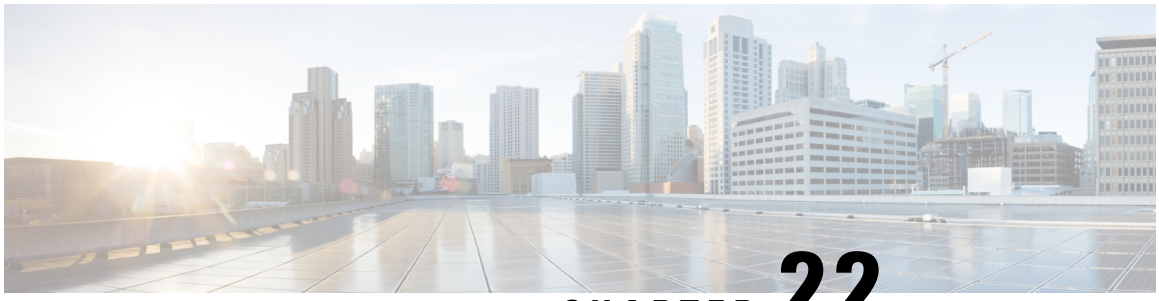
Step 8 Check the **Enable SNMP event trap** check box to enable the SNMP event traps for significant system-related events and then enter the host name of NMS in the **NMS hostname** field.

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

Step 9 Click **Save**.

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





CHAPTER 22

URWB Telemetry Protocol

- URWB telemetry protocol, on page 131
- Configure URWB Telemetry Protocol using CLI, on page 131
- Live Configuration of URWB Telemetry Protocol using CLI, on page 132
- Configure GNSS Telemetry Protocol using CLI, on page 133

URWB telemetry protocol

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

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

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

The telemetry UDP packet contains the following information:

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

Configure URWB Telemetry Protocol using CLI

The URWB telemetry protocol transmits raw UDP data to a specified receiver.

Before you begin

By default, the telemetry data is disabled.

Procedure

Step 1 Use the **configure telemetry server** *dest-ip port* command to set the IP address and UDP port of the receiver.

Example:

```
Device# configure telemetry server 10.115.11.56 1234
```

Multicast addresses are supported.

Step 2 Use the **configure telemetry export** { **enable** | **disable** } command to enable raw UDP telemetry transmission to the configured server.

Example:

```
Device# configure telemetry export enable
```

Note

- Ensure the IP address is configured before you rune the **configure telemetry export enable** 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 **configure telemetry export disable** command.

Step 3 Use the **show telemetry config** command to verify telemetry configuration.

Example:

```
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

Configure live telemetry settings using the live modifier for immediate effect.

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

Procedure

Step 1 Use the **configure telemetry live server** *ip-address port* command to configure live telemetry settings using the live modifier for immediate effect.

Example:

```
Device# configure telemetry live server 10.115.11.56 1234
```

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

Step 2 Use the **configure telemetry live export enable** command to enable live telemetry export.

Example:

```
Device# configure telemetry live export enable
```

Step 3 Use the **show telemetry config** command to view the telemetry information.

Example:

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

Configure GNSS Telemetry Protocol using CLI

Enables the GNSS telemetry protocol on the device.

Procedure

Step 1 Use the **configure gnss telemetry enable** command to enable GNSS telemetry.

Example:

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

Step 2 Use the **configure gnss telemetry disable** command to disable GNSS telemetry when needed.

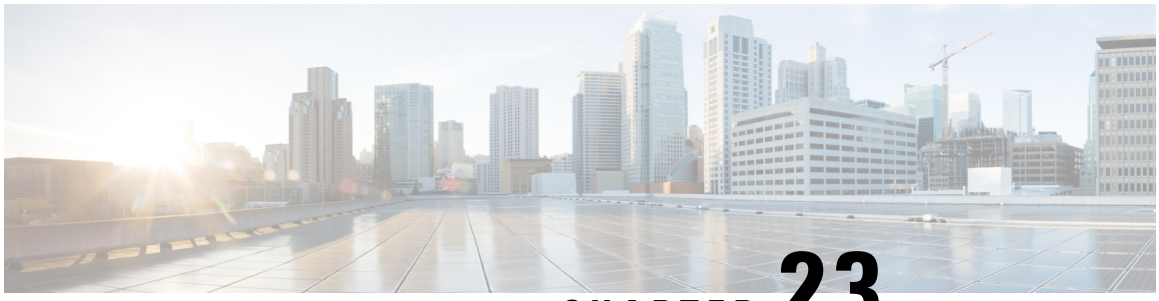
Example:

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

Step 3 Use the **show gnss telemetry** command to view GNSS telemetry status.

Example:

```
Device# show gnss telemetry
```



CHAPTER 23

IW Monitor Management

- IW MONITOR management, on page 135
- Configure IW MONITOR management using CLI, on page 136
- Configure IW MONITOR management using GUI, on page 136

IW MONITOR management

IW MONITOR is a standalone on-premise monitoring application that enables comprehensive network visibility and management.

- Dashboard monitoring and topology visualization
- Real-time performance monitoring and telemetry data processing
- Network events logging for authentication and configuration changes

IW MONITOR capabilities and features

The on-premises IW MONITOR supports these primary capabilities:

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

UIW Release 17.12.1 provides this support for IW MONITOR dashboard:

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

The following table outlines the IW MONITOR features supported from UIW release 17.12.1 onwards.

Table 23: IW MONITOR features support

Feature	Description
IW MONITOR log for RADIUS	RADIUS authentication attempts by mobile units are logged to IW MONITOR
IW MONITOR log CLI SSH access	SSH connections attempts are logged to IW MONITOR
IW MONITOR log GUI access	GUI logins are logged to IW MONITOR
IW MONITOR log ethernet link change	Physical link changes of LAN ports are buffered and logged to IW MONITOR
IW MONITOR log configuration change	Changes applied to the unit configuration through CLI or GUI are logged to MONITOR

Configure IW MONITOR management using CLI

Configure IW MONITOR management to enable network monitoring capabilities including dashboard monitoring, topology view, real-time performance monitoring, telemetry data processing, and network events logging.

IW MONITOR does not require any configuration, and access points are added to the IW MONITOR. Use the CLI to detach the device from the IW MONITOR server and troubleshoot the connection.

Procedure

Step 1 Use the **configure monitor detach** command to detach the device from the IW MONITOR server.

Example:

```
Device# configure monitor detach
```

Step 2 Use the **show monitor** command to verify the IW MONITOR management status.

Example:

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

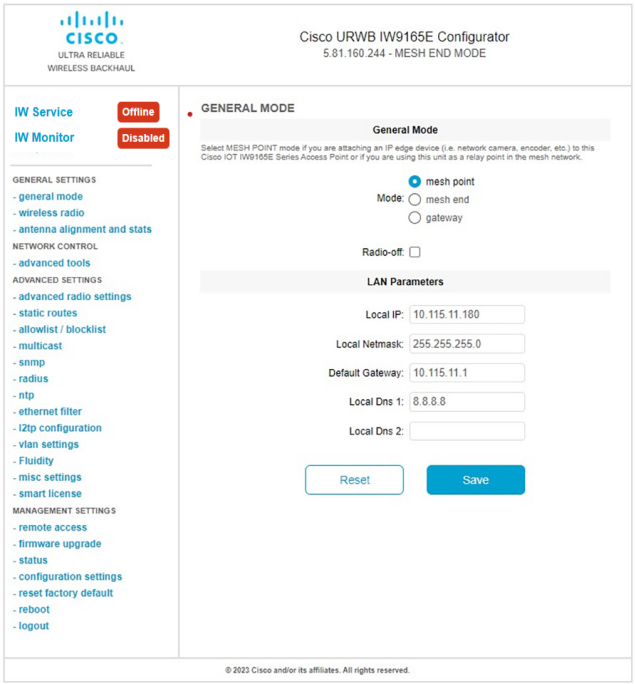
Configure IW MONITOR management using GUI

Enables IW MONITOR management to provide network monitoring capabilities.

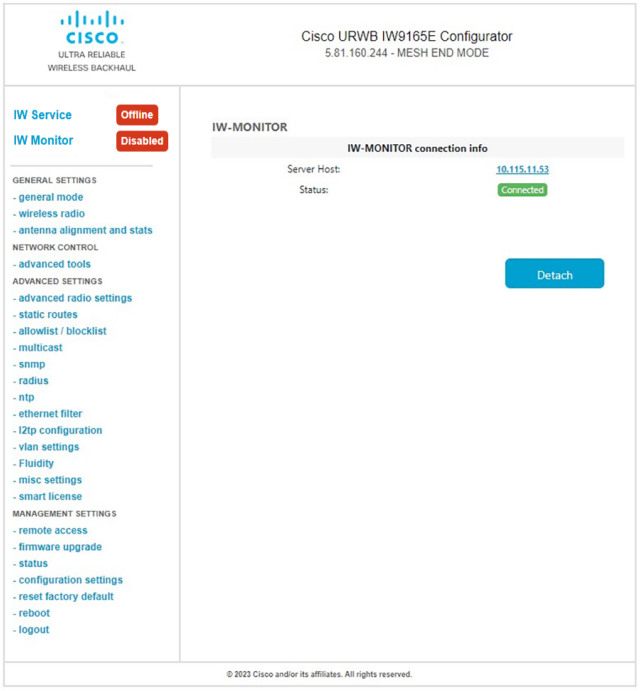
The UIW Release 17.12.1 introduces support for IW MONITOR, a standalone on-premise monitoring application supporting network monitoring features.

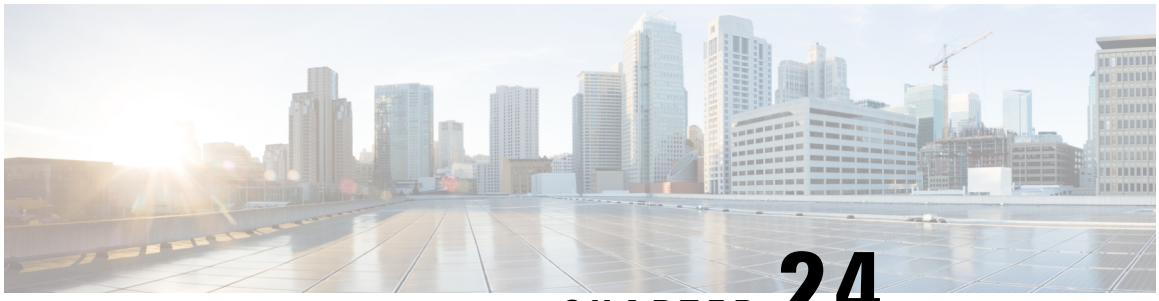
Procedure

Step 1 Enable the **IW MONITOR** option in the **Cisco URWB IW9165E or IW9167E Configurator** window.



Step 2 Verify that the **IW-MONITOR connection info** appears.


Cisco URWB IW9165E Configurator
5.81.160.244 - MESH END MODE
ULTRA RELIABLE
WIRELESS BACKHAUL
IW Service
Offline
IW Monitor
Disabled
GENERAL SETTINGS
- general mode
- wireless radio
- antenna alignment and stats
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- advanced radio settings
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- ethernet filter
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- firmware upgrade
- status
- configuration settings
- reset factory default
- reboot
- logout
IW-MONITOR
IW-MONITOR connection info
Server Host:
10.115.11.53
Status:
Connected
Detach
© 2023 Cisco and/or its affiliates. All rights reserved.



CHAPTER 24

Multicast

- Multicast, on page 139
- Configure Multicast using GUI, on page 140
- Configure multicast using CLI, on page 141
- Delete multicast using CLI, on page 142
- Verify multicast configuration using CLI, on page 142

Multicast

Multicast is a method of communication that

- sends data from one source to multiple destinations simultaneously
- supports Layer 2 and Layer 3 networks on AP
- enables point-to-multipoint or multipoint-to-multipoint transmissions.

Reserved IP address ranges for multicast protocols

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

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.

Table 24: Reserved multicast IP address ranges by protocol

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

Multicast configuration provides these advantages:

- 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. This helps to maintain consistent Quality of Service (QoS) for all recipient APs.

Configure Multicast using GUI

This task allows you to set up Multicast routing to efficiently distribute data across mesh networks by defining Multicast groups, netmasks, and destination addresses.

Multicast routing enables efficient data distribution in mesh networks by sending data to multiple destinations simultaneously. This configuration is essential for optimizing network traffic and bandwidth usage in mesh topologies.

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.

Follow these steps to configure Multicast using GUI:

Procedure

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

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

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

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

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

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

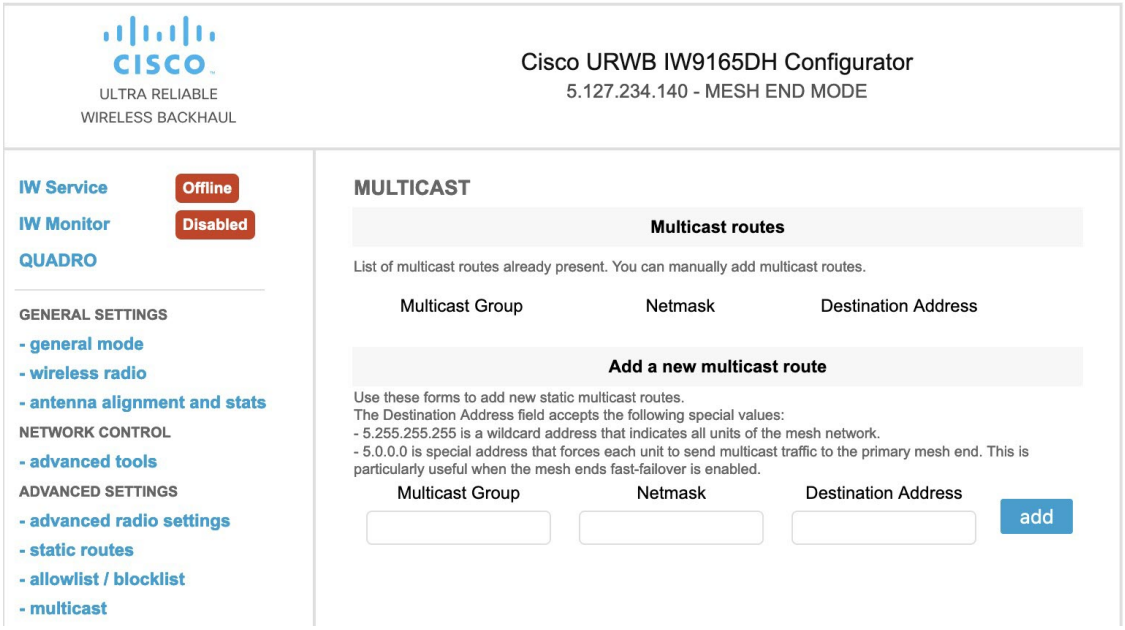
Note
The **Destination Address** field accepts the following special values:

- 5.255.255.255 IP address in the **Destination Address** field sends the data to all the mesh point devices over the mesh network. This is applicable only for the downstream data flow.

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

Tip
The netmask field allows you to specify a block of Multicast addresses. When you specify multiple Multicast groups, the Multicast IP address should represent the network address for each group.

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



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

Configure multicast using CLI

This task allows you to configure multicast groups to manage traffic flow in mesh networks, enabling proper data routing to mesh end devices and global gateways.

In Layer 3 mode, multicast rules must be configured on all mesh end devices and the global gateway. Different multicast IP addresses are used for upstream and downstream traffic to ensure proper data flow direction and failover capabilities.

Procedure

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

Example:

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

Note
This configuration takes effect only after the reboot.

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 especially useful when the mesh end's fast failover is enabled. This address applies only to the upstream data flow.
- 224.5.5.6/5.255.255.255: sends the data to all mesh point devices over the mesh network. This address applies only to the downstream data flow..

Delete multicast using CLI

This task removes a specific meshID IP address from a multicast group configuration using the command line interface.

Use this procedure when you need to remove a meshID IP address from an existing multicast group configuration. This is typically done during network reconfiguration or when decommissioning specific network segments.

Procedure

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

Example:

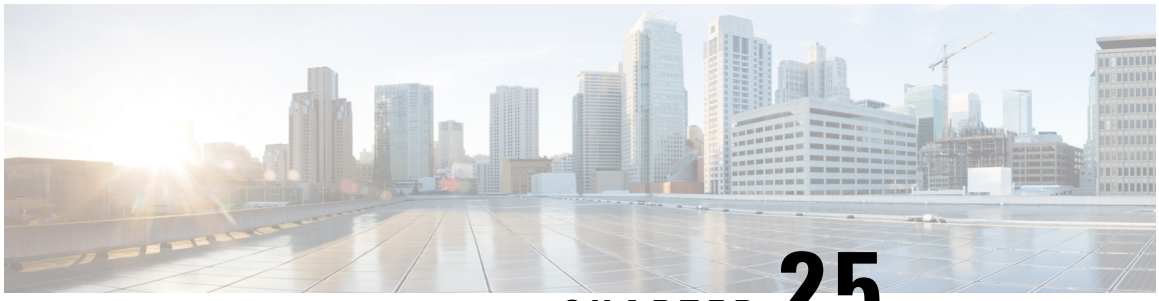
```
Device# configure multicast group delete 224.5.5.5 255.255.255.255 5.255.255.255
```

Note
This configuration takes effect only after the reboot.

Verify multicast configuration using CLI

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

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



CHAPTER 25

Quality of Service

- Quality of service, on page 143
- Configure QoS using CLI, on page 144
- Verify QoS configuration using CLI, on page 145
- Configure 802.1p VLAN priority preference using CLI, on page 145
- Verify 802.1p VLAN priority preference configuration using CLI, on page 146
- Configure CoS remapping using CLI, on page 146
- Verify CoS remapping using CLI, on page 147
- Configure QoS shaping using CLI, on page 147
- Verify QoS shaping using CLI, on page 148

Quality of service

Quality of Service (QoS) is a network management framework that

- prioritizes certain types of network traffic over others
- maintains the quality and performance of critical applications, safety protocols such as voice and video, which are sensitive to delays and packet loss, and
- 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

QoS provides these advantages:

- Prioritization: Manages traffic according to the QoS priority marked in the packet IP header.

- Bandwidth Management: Allocates network resources to ensure that high-priority applications have sufficient bandwidth.
- Latency Management: Minimizes delays in packet arrival time to maintain quality for time-sensitive applications.

QoS marking

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

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

802.1p

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

QoS shaping

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

Configure QoS using CLI

Enable or disable Quality of Service (QoS) processing on the device to control network traffic flow and prioritization.

By default, QoS feature is disabled on the device. You can enable or disable QoS processing as needed for your network configuration requirements.

Procedure

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

Example:

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

Note

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

Verify QoS configuration using CLI

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

QoS Enabled Output

```
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
```

QoS Disabled Output

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

Configure 802.1p VLAN priority preference using CLI

This task enables or disables 802.1p VLAN priority preference over DSCP for IP packets on URWB devices, controlling how the device processes QoS markings.

When configuring QoS on URWB devices, you can control whether the device prioritizes Layer 2 VLAN CoS markings over Layer 3 DSCP markings. This configuration affects how the device examines and processes Quality of Service markings in packet headers.

Procedure

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

Example:

```
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

Configure CoS remapping to adjust QoS priority marks according to the network administrator's design and to change priorities for one or more CoS values.

The URWB system allows remapping of the QoS priority marks based on a network administrator's design. This configuration helps in managing bandwidth and ensuring that higher priority traffic is delivered more efficiently.

Procedure

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

Example:

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

In the 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.

Important
The URWB system manages the remapping process without altering the original marking. The remapped QoS priorities are significant and valid only 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 QoS shaping to allocate and control bandwidth for different classes of service (CoS) on a network device, ensuring proper traffic management and bandwidth utilization.

QoS shaping allows you to manage network traffic by setting bandwidth limits for different CoS values, helping to prioritize critical traffic and control network congestion.

Procedure

Step 1 Use the **configure qos shaper-rates** *bandwidths* command to allocate bandwidth for different CoS on the device.

Example:

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

Note
All eight bandwidths cannot be with zero.

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).

Step 2 Use the **configure qos shaping enabled** command to enable QoS shaping.

Example:

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

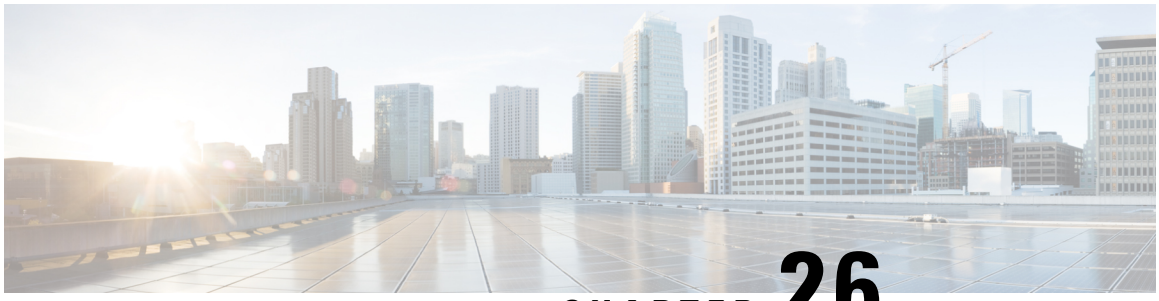
Note

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

Verify QoS shaping using CLI

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

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



CHAPTER 26

Frequency Scan

- Frequency scan, on page 149
- Fluidity frequency scan, on page 149
- Configure fluidity frequency scan using CLI, on page 150
- Verify fluidity frequency scan configuration using CLI, on page 152
- Fluidmax frequency scan, on page 152
- Verify fluidmax frequency scan status using GUI, on page 153
- Configure fluidmax frequency scan using CLI, on page 154
- Verify fluidmax frequency scan configuration using CLI, on page 154

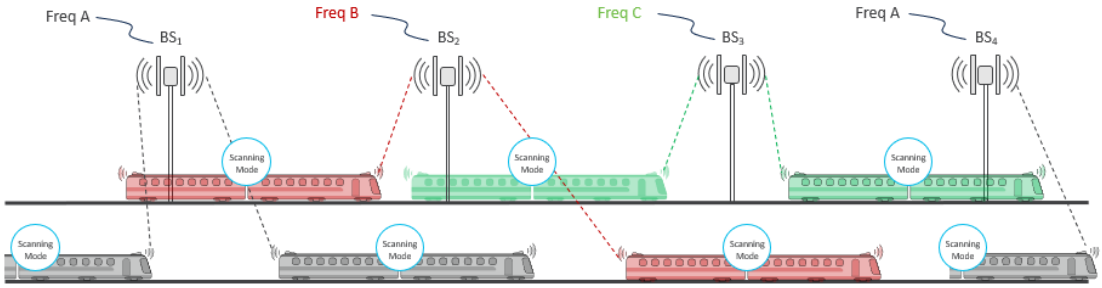
Frequency scan

A frequency scan is a diagnostic process used by URWB devices to identify and evaluate available wireless channels.

- Fluidity frequency scan
- Fluidmax frequency scan

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.



Fluidity frequency scan configurations

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

This task enables you to set up and manage Fluidity frequency scan functionality on the device to optimize wireless connectivity and performance.

Fluidity frequency scan allows the device to automatically monitor and switch between different wireless channels to maintain optimal connectivity. This functionality helps ensure consistent network performance by scanning for better connectivity options when signal strength falls below configured thresholds.

Procedure

Step 1 Use the **configure fluidity scan list clear** command to clear the Fluidity frequency scan list on the device.

Example:

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

Step 2 Use the **configure fluidity scan list** *channel-numbers bandwidth* command to configure the list of channels and their bandwidths for Fluidity frequency scan.

Example:

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

Step 3 Use the **configure fluidity scan isolation** *value* command to configure the isolation time for Fluidity frequency scan.

Example:

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

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

Step 4 Use the **configure fluidity scan rssi-threshold** *threshold* command to configure the SNR threshold for Fluidity frequency scan isolation mode.

Example:

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

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

Step 5 Use the **configure fluidity scan periodic** *scan-time* command to configure the periodic scan time on the device.

Example:

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

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

Step 6 Configure onboard radios Fluidity frequency allocation based on your requirements:

- **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
```

Fluidmax frequency scan

A Fluidmax frequency scan is a scanning mechanism that is typically used for devices in static or semi-static network environments where maintaining a consistent and interference-free connection is crucial.

Device environments and applications

Devices that benefit from Fluidmax frequency scan are often devices that require stable and reliable connections in fixed locations or areas where the network environment doesn't change frequently. These environments include:

- Industrial sites
- Remote monitoring stations
- Any setting where maintaining a consistent and interference-free connection is crucial

Verify fluidmax frequency scan status using GUI

This task verifies whether the Fluidmax frequency scan is enabled or disabled by checking the FluidMAX Autoscan checkbox status in the ADVANCED RADIO SETTINGS.

Use this procedure to check the current configuration status of Fluidmax frequency scanning on your URWB device through the web-based GUI interface.

Before you begin

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

Procedure

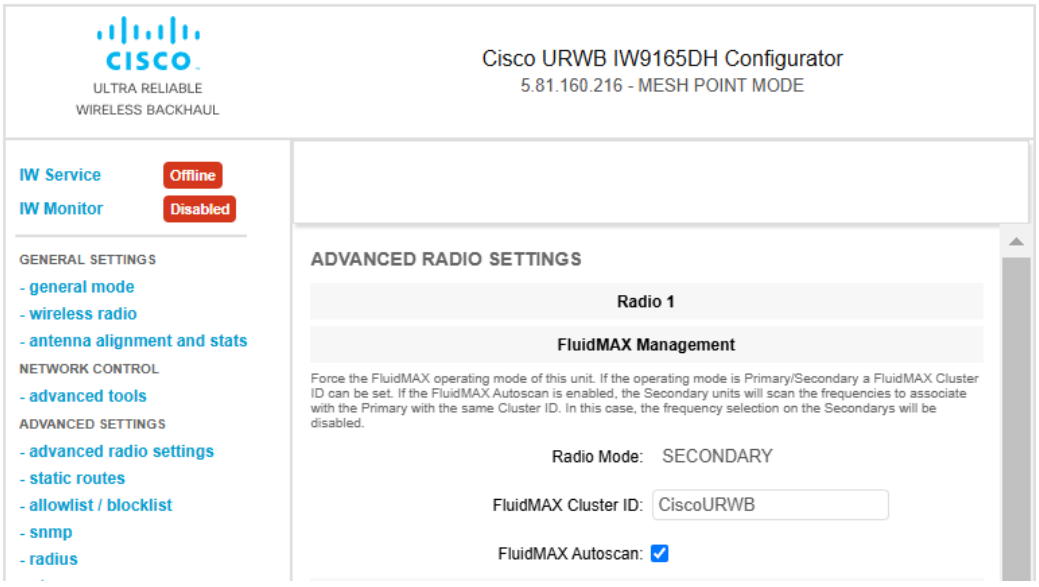
Step 1 Launch the computer's web browser and enter the URL to open the configurator login page.

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

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

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

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



Configure fluidmax frequency scan using CLI

Configure Fluidmax frequency scan settings to enable automatic frequency scanning and to set appropriate threshold values. This ensures optimal wireless performance.

Fluidmax frequency scan allows the device to automatically scan for better frequencies when the signal quality falls below a specified threshold. This feature helps maintain optimal wireless connectivity in dynamic environments.

Procedure

Step 1 Use the **configure dot11Radio** *slot number***mode fluidmax automatic-scan enable** command to enable the Fluidmax frequency on the radio.

Example:

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

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

Step 2 Use the **configure dot11Radio** *slot number***mode fluidmax** *threshold value* command to set the threshold value for Fluidmax frequency scan.

Example:

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

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

Verify fluidmax frequency scan configuration using CLI

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

```
Device #show dot11Radio 1 config

Interface: enabled

Mode: fluidmax secondary

Frequency: 5200 MHz
Channel: 40
Channel width: 20 MHz
Antenna number: 2
TX power level: 2
TX power: 14 dBm
Antenna gain: 15 dBi
Maximum tx mcs: 9
```

```
High-efficiency: disabled
Maximum tx nss: 2
RTS protection: 512
guard-interval: 800 ns
ampdu max length: 255
distance: 3000 m

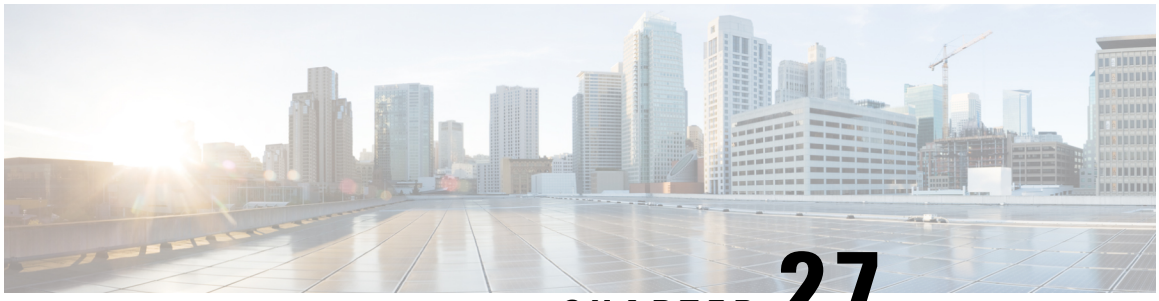
The ampdu Tx
priority 0: enabled
priority 1: enabled
priority 2: enabled
priority 3: enabled
priority 4: enabled
priority 5: enabled
priority 6: disabled
priority 7: disabled

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

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

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

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



CHAPTER 27

Network Address Translation

- Network address translation, on page 157
- Downstream data flow using NAPT for AGVs, on page 158
- Assign port numbers using NAPT for AGVs, on page 159
- NAPT rule on AP, on page 160
- Upstream data flow using SNAT for AGVs, on page 160
- Configure NAPT using CLI, on page 161
- NAPT configuration example, on page 162
- Configure SNAT using CLI, on page 162
- SNAT configuration example, on page 163
- Delete NAT rule using CLI, on page 163
- Delete all NAT rules, on page 164
- Verify NAT configuration using CLI, on page 164
- Verify NAT translations using CLI, on page 164

Network address translation

Network Address Translation (NAT) is a networking feature that ensures smooth and efficient roaming for Automated Guided Vehicles (AGVs) by using a single public IP address for AGVs to access the outside network and assigns port numbers to each application on the AGV, managing data flow for both downstream and upstream directions.

This feature is supported from UIW Release 17.16.1 only.

NAT functionalities

This feature supports the following functionalities:

- NAT with Port Translation (NAPT)
- Source NAT (SNAT)

NAT with Port Translation (NAPT) for downstream traffic manages and routes incoming data packets to the correct inside device. It uses an address table to find a specific application's inside private IP address and port number to forward the packet. For more information, see Downstream Data Flow using NAPT for AGVs.

Source NAT (SNAT) for upstream traffic modifies the source IP address and port numbers of the outgoing packets from inside network devices before sending them to an external network. For more information, see Upstream Data Flow using SNAT for AGVs.

Note

- NAT is supported only in the Layer 2 mode of the AP.
- The NAT/PAT feature supports rules configuration for TCP and UDP traffic only.

Advantage of NAT

A common IP address scheme for on-board vehicle systems reduces the complexity of uniquely identifying all vehicle equipment and facilitates access from external systems.

Downstream data flow using NAPT for AGVs

Downstream data flow using NAPT for AGVs is a network communication process that

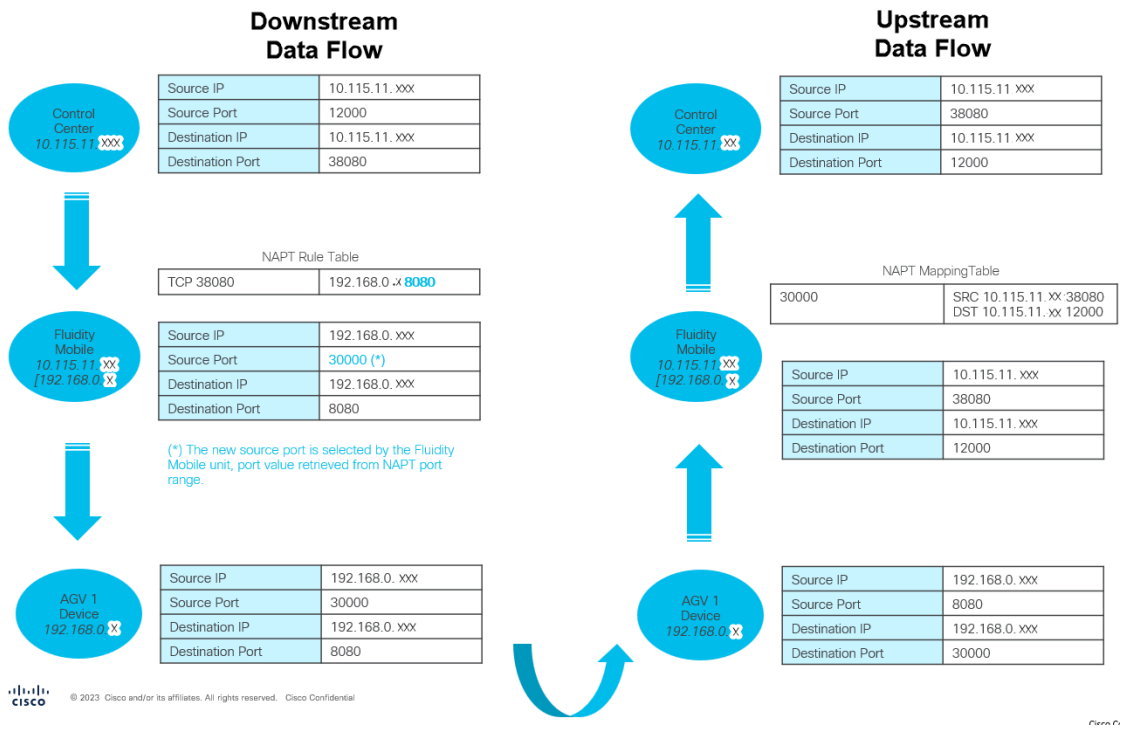
- enables data flow from the outside network to the AGV's inside network
- uses the AP as a gateway between the outside and inside networks
- employs NAPT address tables to find the inside private IP address and port number of specific applications to forward packets.

NAPT functionality for AGVs

By using NAPT:

- Devices from the outside network can connect to services on the AGVs' inside network.
- APs in the AGVs' inside network can direct data flow to specific ports.

Figure 11: Example of downstream data flow using NAPT:



Assign port numbers using NAPT for AGVs

NAPT assigns different port numbers to various services on an AGV. This ensures that responses from the outside network is sent to the correct service on the AGV.

Reserved outside port numbers for NAPT configuration

Protocol / Port Number	Service	Notes
TCP and UDP	—	Port numbers from 1 to 1023 are not allowed on both TCP and UDP protocols.
UDP/1812-1813	RADIUS	—
UDP/6600 UDP/6610	Industrial Wireless Monitor	On-Premises UDP and ping

Protocol / Port Number	Service	Notes
UDP/<telemetry port>	Industrial Wireless Telemetry	• Port number configured for Industrial Wireless Telemetry protocol varies. • The default value configured for Telemetry is 30000.

NAPT rule on AP

A NAPT rule is a network address and port translation rule that sends data flow to specific ports on inside hosts. A typical NAPT rule consists of `<Protocol, Global Destination Port, Translated Local Destination IP, Translated Local Destination Port>`, where the protocol can be either UDP or TCP.

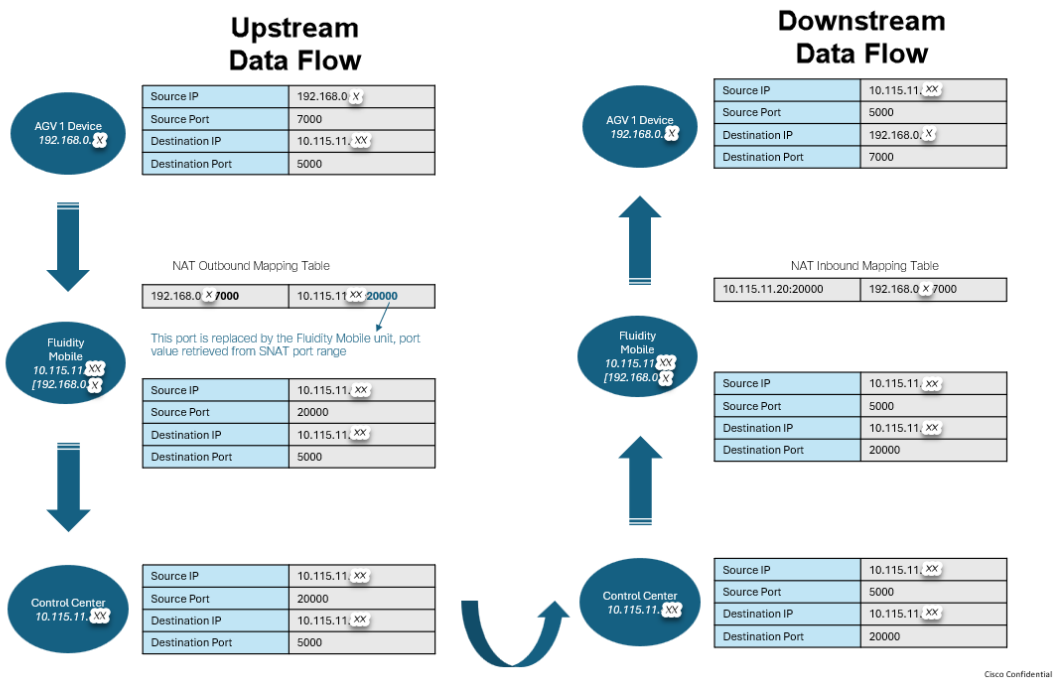
Upstream data flow using SNAT for AGVs

Upstream data flow using Source Network Address Translation (SNAT) for AGVs is a network process that transmits data from the inside network to the outside network through an access point gateway. SNAT modifies outgoing packet headers, changing the source IP address and source port in outgoing packets to match the public IP and port.

Network flow characteristics

The AP serves as a gateway between the inside and outside networks. The AP sends a packet from the inside network to the outside network. SNAT then changes the source IP address and source port in the outgoing packets to match the public IP and port.

Figure 12: Example of upstream data flow using SNAT:



Configure NAPT using CLI

Configure NAPT functionality to enable downstream data flow on the AP.

Perform this task to configure NAPT functionality to enable downstream data flow on the AP.

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the **configure ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat inside port range** *first-port-number second-port-number* command to configure inside port range on the NAT.

Example:

```
Device# configure ip nat inside port range 32000 33000
```

Inside port valid range is from 30000 to 35000. This range should not overlap the SNAT range.

Step 4 Use the **configure ip nat entry add proto** {**TCP** | **UDP**} **outside port** *outside-port-number* **inside ipv4** *inside-ipv4-address* **port** *inside-port-number* command to configure protocol, outside port value, inside IPv4 address, and inside port value on the NAT.

Example:

```
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2 port
8080
```

Step 5 Use the **write** command to save the current configuration.

Example:

```
Device#write
```

Step 6 Use the **reload** command to reload the device.

Example:

```
Device#reload
```

NAPT configuration example

This reference provides the configuration steps for Network Address Port Translation (NAPT) to enable address translation between inside and outside networks with port mapping capabilities.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat inside port range 32000 33000
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2
port 8080
Device# write
Device# reload
```

Configure SNAT using CLI

This task enables SNAT functionality to allow upstream data flow on the access point by configuring NAT rules, inside IPv4 addresses, outside port ranges, and saving the configuration.

Perform this task to configure SNAT functionality to enable upstream data flow on the AP.

Follow these steps to configure SNAT using CLI:

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the configure **ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat outside port range** *left-limit-port-number right-limit-port-number* command to configure outside port range on the NAT.

Example:

```
Device# configure ip nat outside port range 22000 23000
```

Outside port valid range is from 20000 to 25000. This range should not overlap the NAPT range.

Step 4 Use the **write** command to save the current configuration.

Example:

```
Device# write
```

Step 5 Use the **reload** command to reload the device.

Example:

```
Device# reload
```

SNAT configuration example

A sample configuration of SNAT to enable network address translation between inside and outside network parameters.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat outside port range 22000 23000
Device# write
Device# reload
```

Delete NAT rule using CLI

This task deletes a specific NAT rule on the AP.

Procedure

Use the **configure ip nat entry del** command to delete the specific NAT rule on the AP.

Example:

```
Device# configure ip nat entry del 0
```

Delete all NAT rules

This task deletes all NAT rules on the AP.

Procedure

Use the **configure ip nat entry del all** command to delete all the NAT rules on the AP.

Example:

```
Device#configure ip nat entry del all
```

Verify NAT configuration using CLI

The **show ip nat config** command displays the status of NAT configuration.

```
Device# show ip nat config
NAT: enabled
IP: 192.168.1.144
Netmask: 255.255.255.0
NAPT port range: 30000-35000
SNAT port range: 22000-23000
TCP timeout: 300
UDP timeout: 300
NAT max rules: 100
```

Verify NAT translations using CLI

The **show ip NAT translations** command displays all the NAT translations.

```
Device# show ip nat translations

NAT: enabled

Port NAT Translations
---------------------

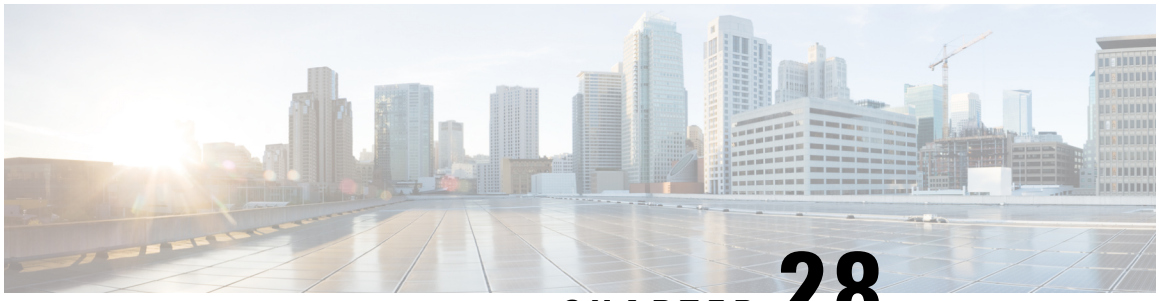
TCP Translations
(192.168.50.4, 4000, 192.168.50.1, 34200) => (10.115.11.157, 4443, 10.115.11.250, 51010)
(10.115.11.250, 51010, 10.115.11.157, 4443) => (192.168.50.1, 34200, 192.168.50.4, 4000)

UDP Translations
None

Source NAT Translations
-----------------------
```

```
TCP Translations
(192.168.50.4, 51178, 10.115.11.250, 4000) => (10.115.11.157, 20292, 10.115.11.250, 4000)
(10.115.11.250, 4000, 10.115.11.157, 20292) => (10.115.11.250, 4000, 192.168.50.4, 51178)

UDP Translations
(10.115.11.250, 3000, 10.115.11.157, 22068) => (10.115.11.250, 3000, 192.168.50.4, 38318)
(192.168.50.4, 38318, 10.115.11.250, 3000) => (10.115.11.157, 22068, 10.115.11.250, 3000)
```



CHAPTER 28

Layer 2 Mesh Transparency

- Layer 2 mesh transparency, on page 167
- Configure and verify Layer-2 protocols forwarding using CLI, on page 168
- Configure Layer-2 protocol forwarding using GUI, on page 169

Layer 2 mesh transparency

Layer 2 mesh transparency is a feature that allows selective forwarding of specific ether-types across URWB networks in MPLS Layer 2 mode.

Reserved ether-types

This list of reserved ether-types cannot be configured:

Table 25: List of reserved ether-types

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

These functionalities are supported using the URWB data plane mesh network when used in MPLS Layer 2 mode:

- Ether-types present in URWB network are detected and reported automatically.
- You can add and remove ether-types from the allowlist.

- You can configure full transparency to enable all Layer 2 protocols easily.
- The feature supports both CLI and GUI.

Configure and verify Layer-2 protocols forwarding using CLI

This task allows you to manage Layer 2 protocol forwarding by adding, deleting, or clearing ethernet types from allowlists and configuring Ethernet-I protocol behavior.

Use this procedure to control which ethernet types are allowed for Layer 2 protocol forwarding in your MPLS configuration. After you clear the detected ethernet types, the detection process operates in the background.

Procedure

Step 1 Use the **configure mpls ether-filter allow-list add** *ether-type-value* command to add an ethernet type to allowlist.

Example:

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

Step 2 (Optional) Use the **configure mpls ether-filter allow-list delete** *ether-type-value* command to delete an ethernet type from allowlist.

Example:

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

Step 3 (Optional) Use the **configure mpls ether-filter allow-list clear** command to clear all ethernet types from allowlist.

Example:

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

Step 4 (Optional) Use the **configure mpls ether-filter allow-list add all** command to add all ethernet types to allowlist.

Example:

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

Note
The **all** keyword sets the ether filter to all-pass mode by filling the allowlist with a single entry, 0x0000.

Step 5 (Optional) Use the **configure mpls ether-filter table clear** command to clear list of detected ether-types.

Example:

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

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

Step 6 (Optional) Use the **configure mpls ether-filter ethernet-I forward** command to configure Ethernet – I protocol to forward.

Example:

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

Step 7 (Optional) Use the **configure mpls ether-filter ethernet-I block** command to configure Ethernet – I protocol to block.

Example:

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

Step 8 (Optional) Use the **show mpls config** command to verify list of allowed ether-types.

Example:

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

Step 9 (Optional) Use the **show mpls ether-filter table** command to verify list of detected ether-types.

Example:

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

Configure Layer-2 protocol forwarding using GUI

This task allows you to manage ethernet filter configurations including adding specific and detected ether types to the allowlist, clearing ethernet types, and configuring ethernet protocol settings.

Use the ethernet filter functionality to control which ethernet types and protocols are permitted. This configuration helps manage network traffic filtering at the Layer-2 level.

Procedure

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

The **Ethernet Filter** window appears.

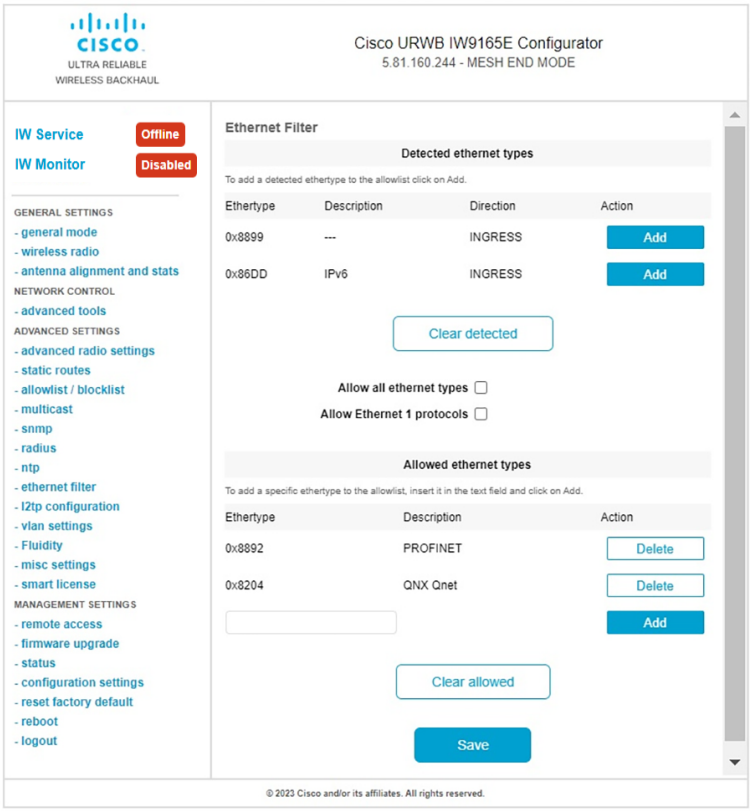
Step 2 Add an ether type to the allowlist.

a) Click **Add** in the **Detected ethernet types** section.

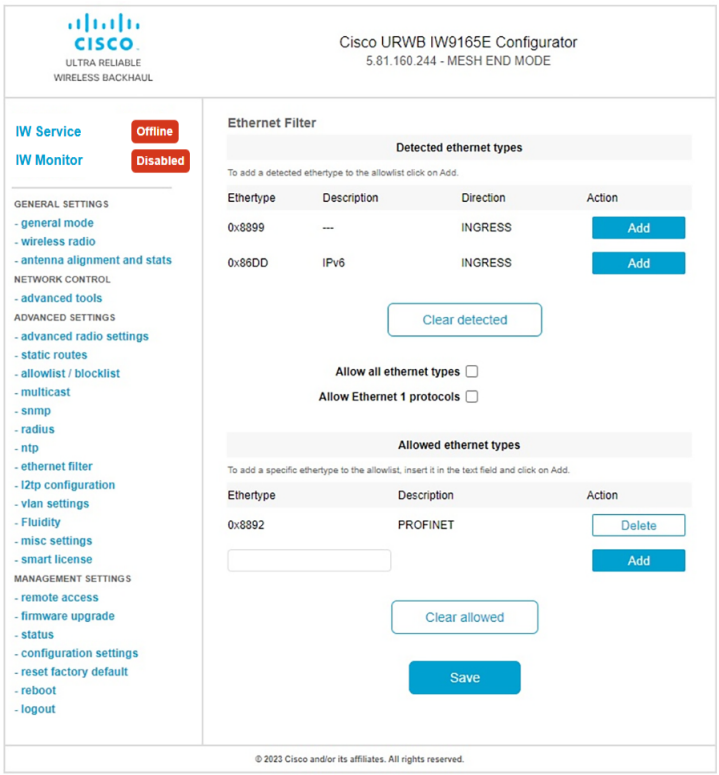
b) In the **Allowed ethernet types** section, enter the **Ethertype** name in the text box and click **Add**.

You can view the added ether types reflected in the **Allowed Ethernet type** section.

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


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

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


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

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

Step 3 Clear all allowed ethernet types from the allowlist.

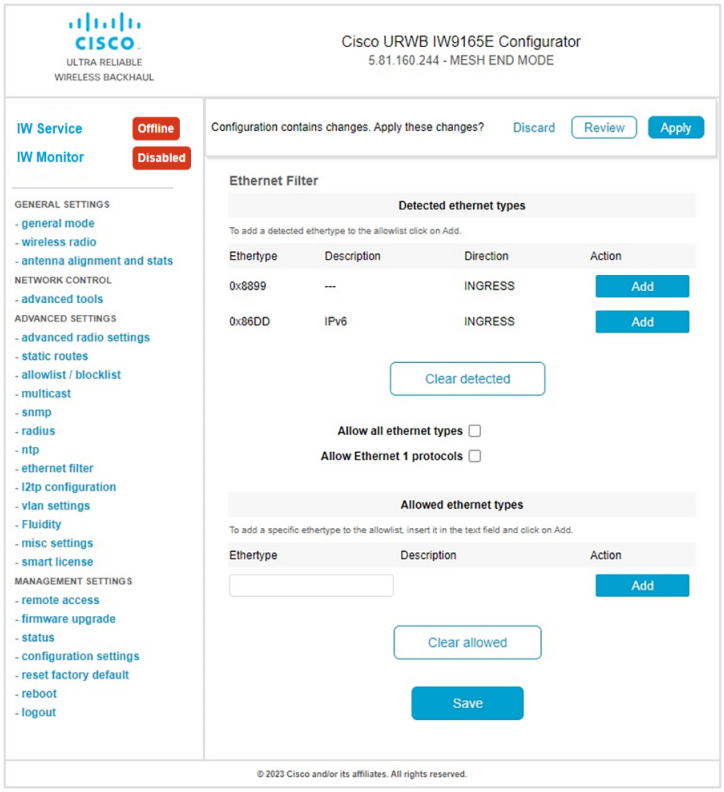
a) In the **ADVANCED SETTINGS**, click **ethernet filter**.

The **Ethernet Filter** window appears.

b) Click **Clear allowed** in the **Allowed ethernet types** section to remove all ethernet types from the allowlist.

All ethernet types are removed from the allowlist.

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



Step 4 Clear all detected ethernet types from the allowlist.

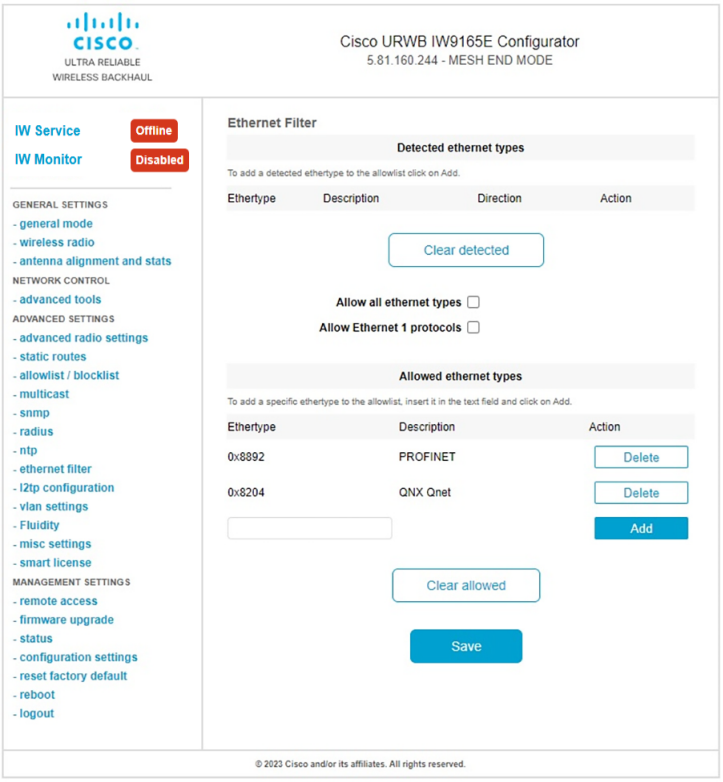
a) In the **ADVANCED SETTINGS**, click **ethernet filter**.

The **Ethernet Filter** window appears.

b) Click **Clear detected** in the **Detected ethernet types** section to remove the detected ethernet types from the allowlist.

All detected ethernet types are removed from the **Detected ethernet types** section.

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



c)

Step 5 Add or allow all ethernet types to the allowlist.

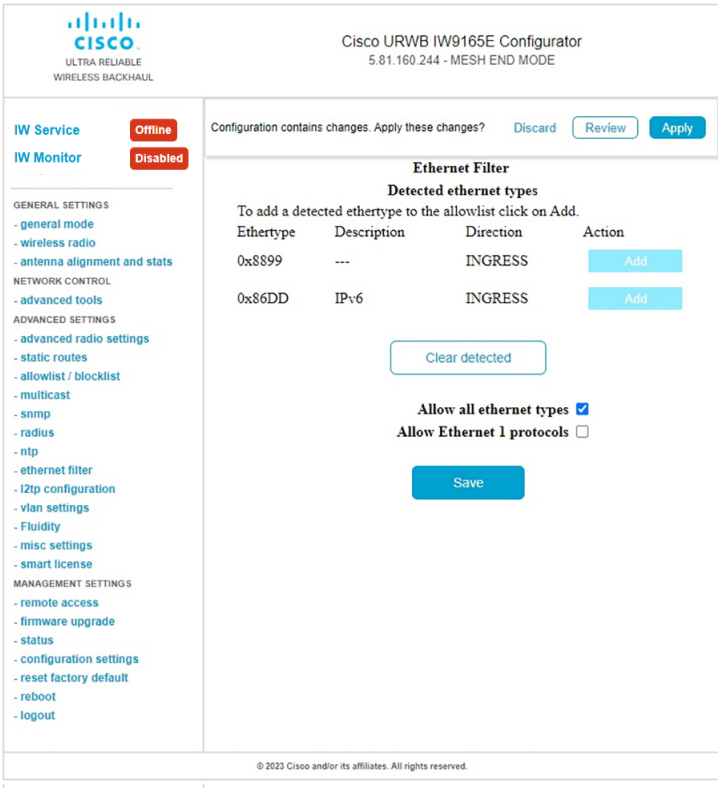
a) In the **ADVANCED SETTINGS**, click **ethernet filter**.

The **Ethernet Filter** window appears.

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

c) Click **Save** and then **Apply** to change the configuration.

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



Step 6 Configure an Ethernet 1 protocol.

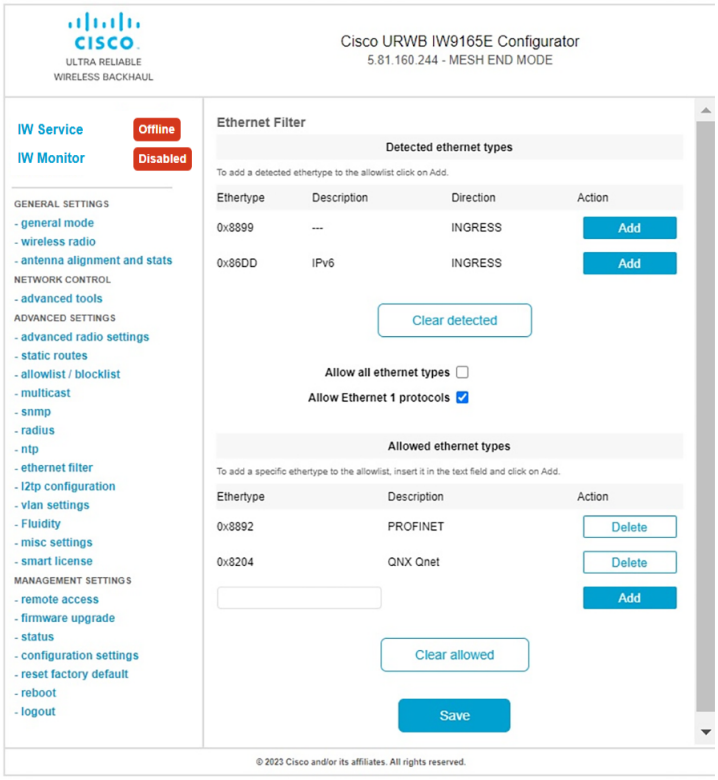
a) In the **ADVANCED SETTINGS**, click **ethernet filter**.

The **Ethernet Filter** window appears.

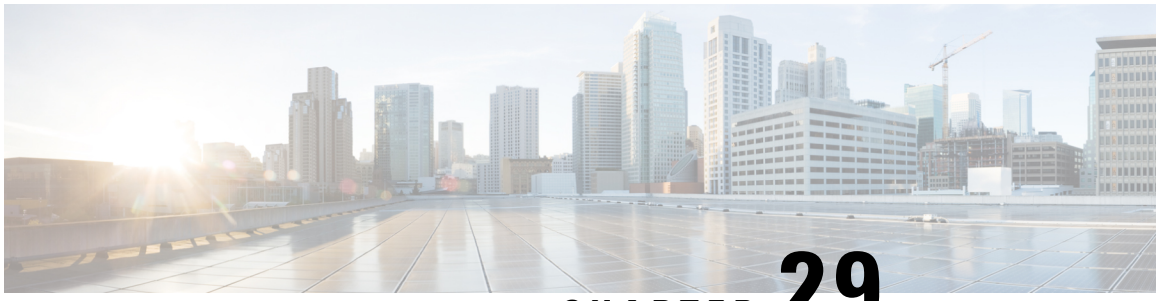
b) Check the **Allow Ethernet 1 protocols** check box in the **Ethernet Filter** section to enable ethernet 1 protocol mode.

c) Click **Save** and then **Apply** to change the configuration.

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


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

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



CHAPTER 29

Multipath Operation

- Multipath operation, on page 175
- MPO working functionality, on page 176
- MPO packet duplication and deduplication, on page 176
- MPO limitations, on page 176
- Configure MPO features using CLI, on page 177
- Verify MPO features using CLI (MPO monitoring), on page 178

Multipath operation

Multipath Operation (MPO) is a patented technology that

- enhances reliability by sending duplicate copies of packets across multiple wireless paths
- duplicates high priority traffic up to 4x to reduce hardware failures and increase availability, and
- establishes multiple label switched paths (LSPs) between a mobile system and the backend infrastructure to reduce packet loss.

MPO benefits and functionality

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.

MPO addresses these challenges by providing:

- Reduced latency for high priority traffic
- Lower effects of interference through redundant path transmission
- Increased system availability through hardware failure mitigation

The multiple LSPs enable high priority packets to be sent through redundant paths to reduce packet loss in mobile wireless network environments.

MPO working functionality

By default, MPLS establishes a single tunnel using one wireless link between the vehicle and the infrastructure for data transmission. Using two radio interfaces on two vehicle radios allows you to set up four MPLS tunnels for transmitting MPO-protected traffic. When you configure MPO to use multiple links for protected traffic, the system creates an MPLS tunnel over each available wireless link. Every wireless link replicates MPO-protected traffic. If one wireless link fails, the others continue replicating the traffic. Fast Failover is supported with MPO since UIW Release 17.14.1.

MPO packet duplication and deduplication

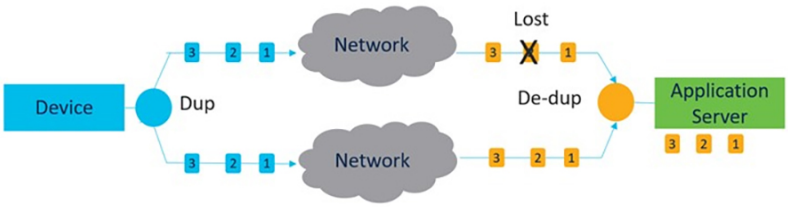
MPO packet duplication and deduplication is a reliability mechanism that

- sends duplicate packets through several wireless channels to various access points to ensure reliability
- uses spatial diversity of receiving access points to increase the chances of at least one packet copy being received correctly, and
- removes duplicate packets received along different wireless paths using sequence numbers and deduplication algorithms.

MPO duplication and deduplication process

The delivered packets have sequence numbers assigned to them, allowing the deduplication algorithm to eliminate copies of packets that it has already received.

The process of duplication and deduplication is shown:



The duplication and deduplication algorithm performs these functions:

- 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.

MPO limitations

Disable the following handoff features when MPO is enabled, as they are not available for use:

- Pole Ban and Pole Proximity

- Coloring
- Load balancing

Configure MPO features using CLI

This task configures Multi-Path Operation (MPO) features to provide traffic redundancy and enable quality of service settings for improved network performance.

MPO features let you configure class-of-service traffic protection. You can also set up redundant paths for mobile devices, RSSI thresholds for wireless links, and telemetry settings. These configurations help ensure reliable network connectivity. They also enable performance monitoring.

Before you begin

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

Procedure

Step 1 Use the **configure fluidity mpo** {**cos** *cos-value*| **path max** *max-value*| **rssi min** *min-value* | **telemetry** {**enabled** | **disabled**}} command to configure MPO features.

Example:

```
Device# configure fluidity mpo cos 5
Device# configure fluidity mpo path max 2
Device# configure fluidity mpo rssi min 10
Device# configure fluidity mpo telemetry enabled
```

This example shows the UDP Telemetry stream with MPO counters.

Example:

```
Device# configure telemetry server 192.168.0.200
Device# configure telemetry export enable
Device# configure fluidity mpo telemetry enabled
```

- **cos** - Configure the class-of-service of traffic to protect with MPO redundancy. Only one CoS can be specified at a time. The valid cos range is zero to seven, and the default value is six.
- **path** - Configure the maximum number of simultaneous redundant paths established by only mobile devices. The valid range for maximum path links is one to four. 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). The valid range for minimum RSSI value is 0 to 96. The default value is 20.
- **telemetry** – Configure enable/disable specific MPO telemetry. The telemetry value can be enabled (M=1) or disabled (M=0). The default is disabled.

Step 2 Use the **configure fluidity mpo status** {**disabled** | **rx-only** | **enabled** } command to configure MPO status.

Example:

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

- **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.

Step 3 Use the **show fluidity mpo config** command to verify the MPO configuration parameters.

Example:

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

Verify MPO features using CLI (MPO monitoring)

This section provides CLI commands and their sample outputs to verify and monitor Multi-Path Operation (MPO) features. Use these commands to check MPO configuration, view packet statistics, examine network topology, and analyze engineering data for troubleshooting and monitoring MPO performance.

MPLS configuration output

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

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

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

MPO statistics output

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

```
Device# show fluidity mpo statistics (on Mesh End)
table-size 2:
MAC address : 40:36:5A:15:C8:50        8C:89:A5:83:EB:71
Tx-1        : 0                        208
Tx-2        : 0                        208
Rx-Accept-1 : 178                      0
Rx-Accept-2 : 30                       0
Rx-Drop-1   : 30                       0
Rx-Drop-2   : 178                      0
Lost-1-only : 0                        0
```

```
Lost        : 0                         0

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

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

This list describes the fields in the command output.

- **MAC address:** Source L2 address of the external network device which is sending packets.
- **Tx-1 and Tx-2:** This field displays the total count of packets 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:** This field shows the 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.

Fluidity network output

The output of the **show fluidity network** command:

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

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

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

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

```
Secondary IDs : 5.21.201.204
```



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

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

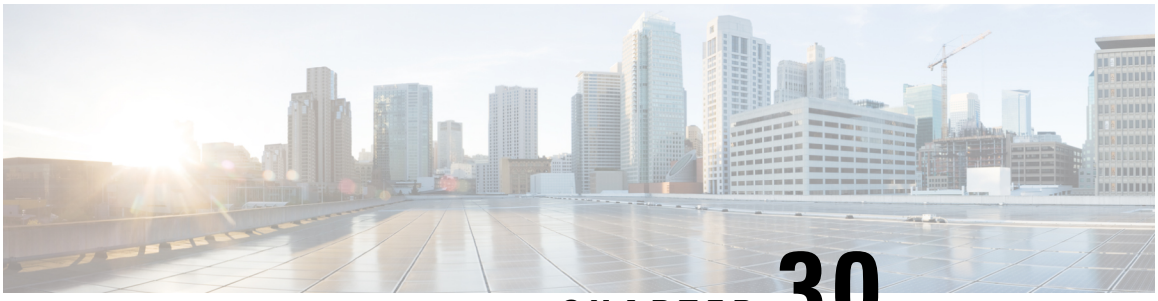
Engineering statistics output

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

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

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

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



CHAPTER 30

Fluidmax Topology

- Fluidmax topology configuration and validation, on page 181

Fluidmax topology configuration and validation

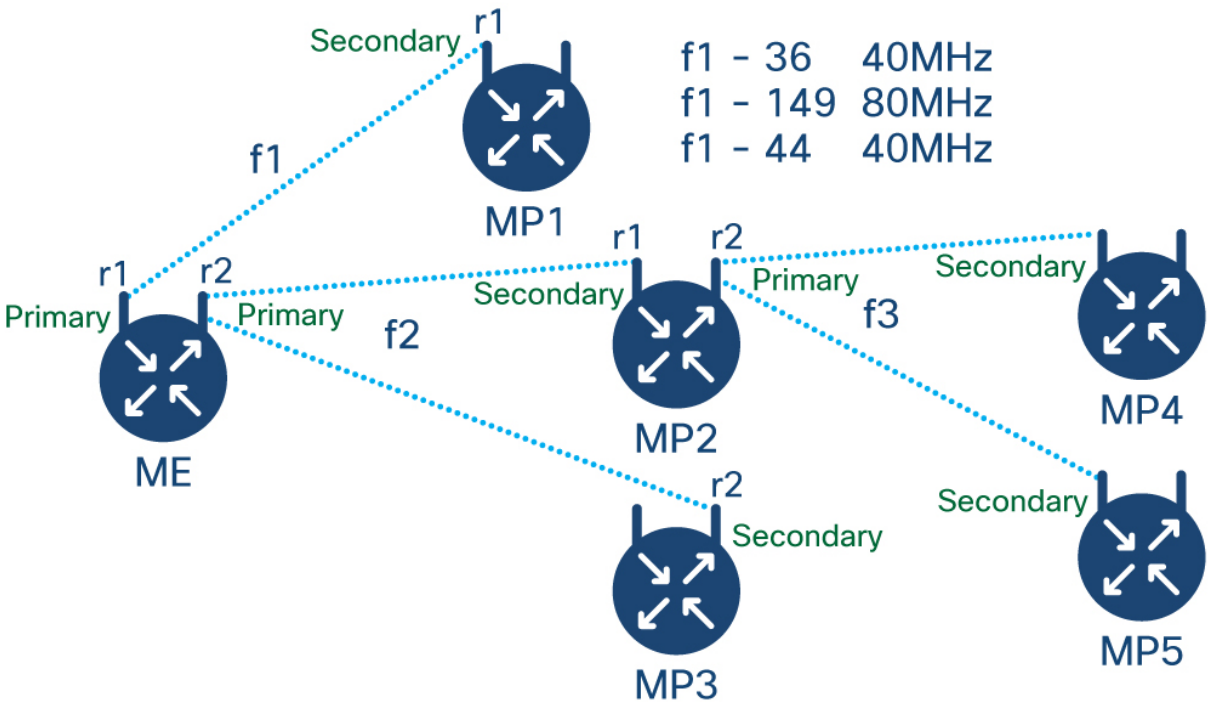
Fluidmax topology configuration is a wireless network setup method that

- enables any wireless interface to operate in Fluidmax mode for point-to-multipoint connections
- uses independent sets of Fluidmax parameters for each interface, and
- allows great flexibility in network topologies for fixed infrastructure.

Cascaded point-to-multipoint clusters

Two cascaded point-to-multipoint clusters demonstrate topology flexibility where the ME (Mesh End) node uses both radios in Fluidmax Primary mode to serve several secondary clients (MP1 (Mesh Point), MP2, and MP3) on two different frequencies. For MP2, the first radio operates in Fluidmax secondary mode to connect to the ME, while the second interface is configured as Fluidmax Primary to serve more downstream clients (MP4 and MP5).

Figure 13: Two cascaded fluidmax topology



Configure point to multipoint topology from CLI

Configure a Fluidmax (point-to-multipoint) topology to establish wireless mesh networks with designated primary and secondary device roles.

The Fluidmax topology enables the creation of mesh networks in which devices function as either primary or secondary nodes. This configuration involves setting up dot11Radio interfaces, selecting operating modes, configuring channels, and specifying bandwidth parameters.

Procedure

Step 1 Use the **configure dot11Radio** *interface* command to configure the dot11Radio interface.

Example:

```
Device# configure dot11Radio 1
```

interface - Valid dot11Radio interface numbers range from 0-3.

Step 2 Use the **configure dot11Radio** *interface* {**enable** | **disable**}command to enable or disable the wireless interface.

Example:

```
Device#configure dot11Radio 1 enable
```

Step 3 Use the **configure dot11Radio** *interface* **mode**{**fluidity** | **fixed**| **fluidmax**}{**primary** | **secondary**} command to set the operating mode and role for the interface.

Example:

```
Device#configure dot11Radio 1 mode fluidity primary
```

Step 4 Use the **configure dot11Radio** *interface* **channel** *channel-id* command to set the operating channel.

Example:

```
Device# configure dot11Radio 1 channel 10
```

channel-id - Valid channel IDs range from 1 – 256.

Step 5 Use the **configure dot11Radio** *interface* **band-width** *channel-bandwidth* command to configure the channel bandwidth.

Example:

```
Device# configure dot11Radio 1 band-width 40
```

channel-bandwidth - Supported values are 20, 40, 80, and 160.

Step 6 Use the **write** command to save the configuration.

Example:

```
Device# write
```

Step 7 Configure Fluidmax cluster ID and tower ID as needed.

a) Use the **configure dot11Radio** *interface* **mode fluidmax** *cluster-id* **fluidmesh** command to configure Fluidmax cluster ID.

Example:

```
Device# configure dot11Radio 1 mode fluidmax 10 fluidmesh
```

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

b) Use the **configure dot11Radio** *interface* **mode fluidmax tower** {**enable** | **disable**} command to enable the Fluidmax Tower ID for a specified interface.

Example:

```
Device# configure dot11Radio 1 mode fluidmax tower enable
```

Tower ID enables or disables the Fluidmax Tower ID for the specified interface.

Note
Use the Tower ID when configurations include both a Gateway and a Mesh Point (MP) that share the same tower ID.

Configuration examples: Point to multipoint topology

ME (Mesh End) Configuration

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

```
Device#configure dot11Radio 2 mode fluidmax primary
Device#configure dot11Radio 2 channel 149
Device#configure dot11Radio 2 band-width 80
```

MP1 (Mesh point) Configuration

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

MP2 Configuration

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

MP3 Configuration

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

MP4 Configuration

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

MP5 Configuration

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

Validate point to multipoint topology using CLI

Use the **show dot11Radio** *interface* **config** command to validate the point-to-multipoint (Fluidmax) topology configuration.

Example:

ME (Mesh End) radio2

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

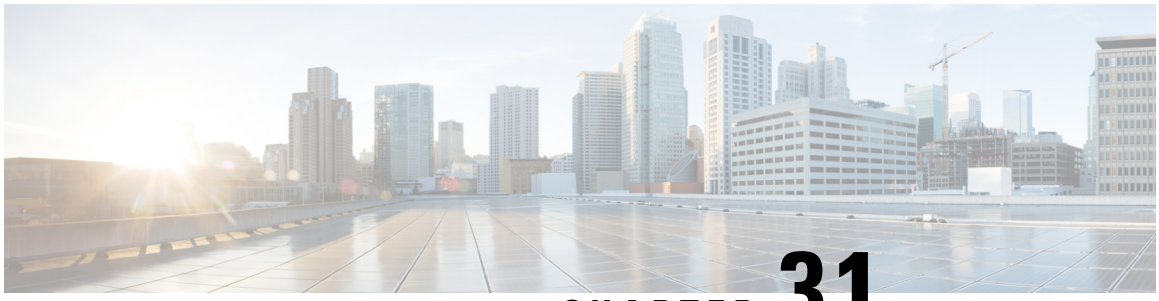
```
Automatic scan : enabled
Automatic scan threshold : disabled
```

MP2 (Mesh Point)

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

MP4 radio1

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



CHAPTER 31

Point-to-Point Relay Topology

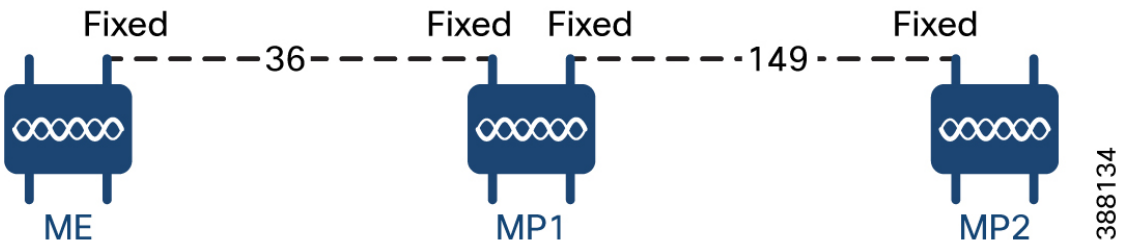
- Configure and validate point-to-point relay topology, on page 187
- Configure point-to-point relay topology from CLI, on page 188
- Validate point to point relay topology from CLI, on page 189

Configure and validate point-to-point relay topology

This task enables you to implement a point-to-point relay topology using two radio interfaces on a single device to establish effective mesh connectivity between mesh points.

A point-to-point relay topology uses two radio interfaces on a single device (MP1) to establish connectivity. This configuration involves mesh endpoints and mesh points operating on different channels to create the relay connection.

Figure 14: Point to point relay topology



Procedure

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

Step 2 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.

Configure point-to-point relay topology from CLI

This task configures a point-to-point relay topology for wireless devices to establish communication links between mesh endpoints and mesh points using CLI commands.

Point-to-point relay topology configuration involves setting up wireless interfaces with specific radio configurations, operating modes, and channel assignments for mesh networks.

Procedure

Step 1 Use the **configure dot11Radio** *interface* command to configure the wireless device with radio interface number.

Example:

```
Device# configure dot11Radio 1
```

Step 2 Use the **configure dot11Radio** *interface* {**enable** | **disable**} command to set wireless interface admin state to enable or disable mode.

Example:

```
Device# configure dot11Radio 1 enable
```

Step 3 Use the **configure dot11Radio** *interface* {**enable** | **disable**}**mode** {**fluidity** | **fixed**| **fluidmax**} command to configure an operating mode for the specified interface (fixed or Fluidity or Fluidmax).

Example:

```
Device# configure dot11Radio 1 enable mode fluidity
```

Step 4 Use the **configure dot11Radio** *interface* {**enable** | **disable**}**mode** {**fluidity** | **fixed**| **fluidmax**}**channel** *channel id*Set the operating channel for the specified interface and the operating channel id valid range is between 1 to 256.

Example:

```
Device# configure dot11Radio 1 enable mode fluidity channel 10
```

Step 5 End the configuration.

Example:

```
Device# end
```

Configuration examples

Basic configuration example:

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

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
```

Validate point to point relay topology from CLI

To validate point-to-point relay topology configuration, use show commands to verify interface settings and wireless parameters across mesh devices.

Use the **show dot11Radio** *interface* **config** command to validate the configuration:

Mesh End (ME) Statistics

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

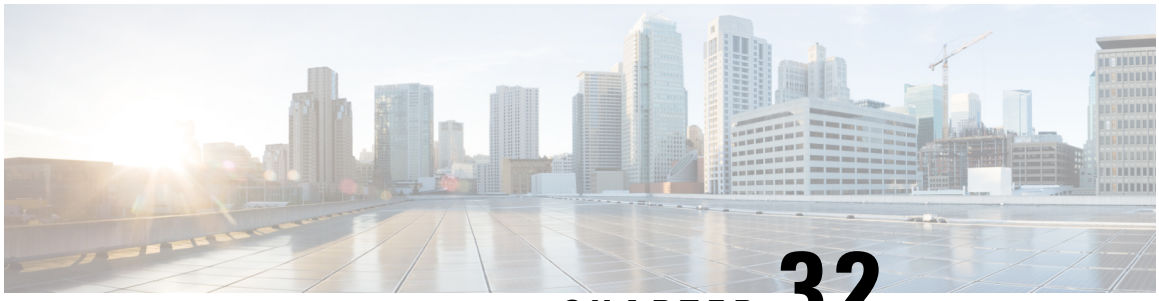
Mesh Point (MP1) Statistics

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

MP2 Statistics

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

```
Passphrase : Cisco
AES encryption : enabled
```



CHAPTER 32

Mixed Mode (Fixed infrastructure + Fluidity) Topology

- Mixed mode topology, on page 191
- Configure mixed mode topology from CLI, on page 192

Mixed mode topology

A mixed mode topology is a wireless configuration that

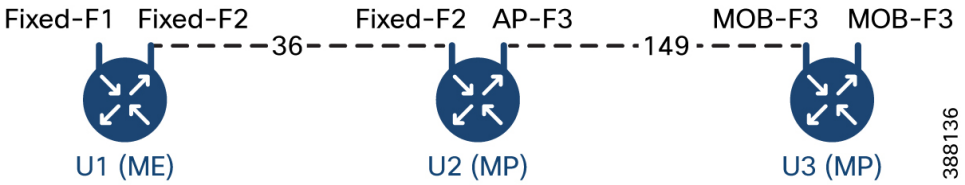
- provides flexibility of configuration on multi-radio device with different frequencies
- allows one radio to operate as fixed infrastructure while the second radio functions as a Fluidity access point to accept vehicle connections simultaneously, and
- enables wireless interfaces to operate in Fluidmax mode without any restriction of the P2MP (Point-to-MultiPoint) role (Primary or Secondary) if fixed infrastructure role is suitable.

Mixed mode configuration examples

The mixed mode topology demonstrates different radio configuration scenarios across multiple devices.

- U2: One radio configured as fixed infrastructure and the second radio as a Fluidity access point to accept vehicle connections simultaneously
- U1: Both radio interfaces configured as fixed infrastructure
- U3: Both radio interfaces configured as Fluidity

Figure 15: Mixed mode topologies



Configure mixed mode topology from CLI

Configure a mixed mode topology to establish different device roles and wireless interface settings for network deployment scenarios.

Mixed mode topology allows devices to operate in different roles, such as vehicle mode, infrastructure mode, and wireless relay mode. Each configuration requires specific CLI commands to set the corresponding parameters.

Procedure

Step 1 Use the **configure fluidity id** {**vehicle-auto** |**vehicle ID** |**infrastructure** |**wireless-relay**} command to configure the fluidity role for the device using the appropriate mode.

Example:

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

- 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.

Step 2 Use the **configure dot11Radio** *interface* command to configure the dot11Radio interface.

Example:

```
Device# configure dot11Radio 1
```

interface values range from 0-3.

Step 3 Use the **configure dot11Radio** *interface*{**enable** | **disable**} command to enable or disable the wireless interface admin state.

Example:

```
Device# configure dot11Radio 1 enable
```

Step 4 Use the **configure dot11Radio** *interface*{**fluidity** | **fixed**| **fluidmax**} command to set the operating mode for the specified interface.

Example:

```
Device# configure dot11Radio 1 mode fluidity
```

Step 5 Use the **configure dot11Radio** *interface***channel** *channel-id* command to set the operating channel for the interface.

Example:

```
Device# configure dot11Radio 1 channel 10
```

The operating channel ID values range from 1 to 256.

Step 6 Use the **write** command to save the configuration.

Example:

```
Device# write
```

Configuration examples: mixed mode topology

U1 Configuration

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

U2 Configuration

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

U3 Configuration

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

Validate mixed mode topology from CLI

To validate a mixed mode topology, use the show commands to check the configuration of dot11 radio interfaces and verify the mode settings for each unit.

Use the **show dot11Radio** *interface* **config** command to validate a mixed mode topology:

U1 Statistics:

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

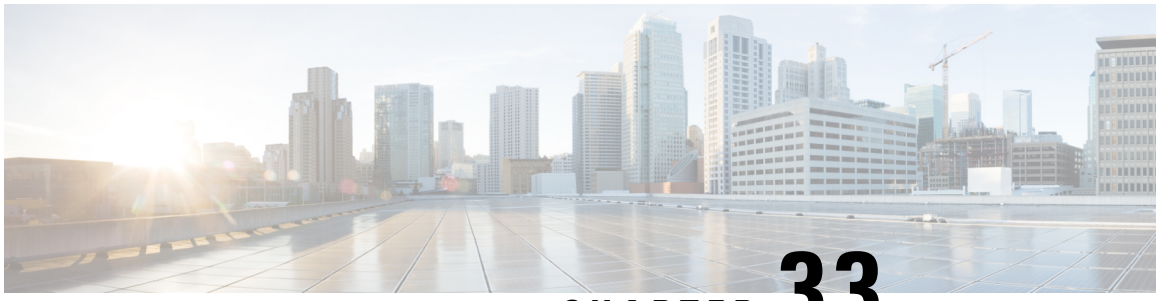
U2 Statistics:

```
Device# show dot11Radio 1 config
Interface : enabled
Mode : fixed infrastructure
Frequency : 5180 MHz
Channel : 36
……
Passphrase : Cisco
AES encryption : enabled
```

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

U3 Statistics:

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



CHAPTER 33

Fast Failover

- Fast failover, on page 195
- Configure and validate fast failover, on page 195

Fast failover

Fast failover is a specific type of failover configuration that

- provides hardware redundancy and carrier-grade availability within URWB-based networks
- monitors server health and can quickly switch over when needed, and
- allows network to recover within less than 30 seconds when Fluidmax is used or less than 500 milliseconds when Fluidity is used.

Recovery time specifications

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

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

- 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.
- 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.

The configure and validate fast failover procedure applies to both Fluidmax and Fluidity modes.

Configure fast failover from CLI

Configure fast failover functionality to provide automatic device failure detection and recovery in mesh network environments.

Fast failover configuration allows mesh point devices to quickly detect failures and switch to backup paths, minimizing network downtime and ensuring continuous connectivity.

Procedure

Step 1 Use the **configure modeconfig mode meshpoint** command to configure the operating mode of the device.

Example:

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

The available modes are mesh end (ME), mesh point (MP), and global gateway (L3).

Step 2 Use the **configure mpls fastfail status** {**enable** | **disable**}command to configure the fast failover status.

Example:

```
Device# configure mpls fastfail status enable
```

MPLS configures MPLS data frame packets for the specified device.

The fast failover feature status can be configured as enabled or disabled.

Step 3 Use the **configure mpls fastfail timeout** *value* command to set the fast failover timeout value.

Example:

```
Device# configure mpls fastfail timeout 100
```

The fast failover timeout determines the period for device failure detection. You can set any value from 0 to 65535.

Step 4 Use the **configure mpls preempt-delay** *value* command to set the preempt delay.

Example:

```
Device# configure mpls preempt-delay 100
```

By default, the preemption delay time is 70 seconds. During this period, the primary device actively gathers updates from the secondary device, allowing it to fully understand the network's current preemption delay status. You can configure a value from 0 to 65535.

Note
The radio interface setting must be the same on both ME and multi-point primaries.

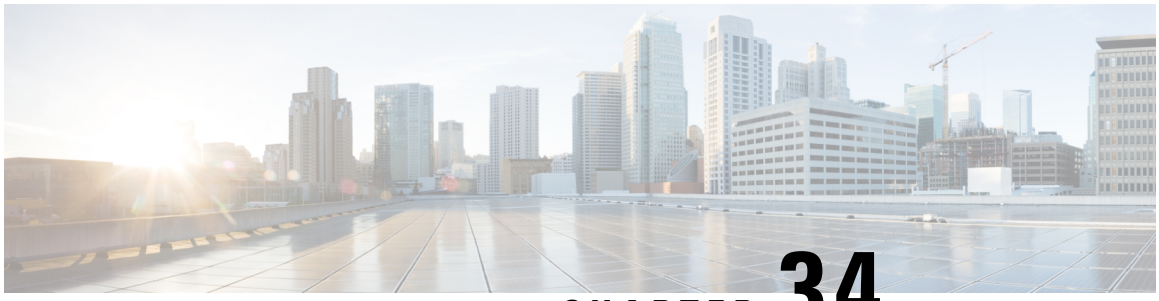
Validate fast failover from CLI

Use this command to validate fast failover.

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

Example:

```
Device# show mpls config
layer 2
unicast-fllod
arp-unicast:
reduce-broadcast:
cluster ID
MPLS fast failover: enabled
Node failover timeout: 100 ms
……
MPLS tunnels:
Idp_id 381877266 debug 0 auto_pw 1
Local_gw 5.21.201.116 global_gw 0.0.0.0 pwlist {}
```



CHAPTER 34

Network Address Translation

- Network address translation, on page 199
- Downstream data flow using NAPT for AGVs, on page 200
- Assign port numbers using NAPT for AGVs, on page 201
- NAPT rule on AP, on page 202
- Upstream data flow using SNAT for AGVs, on page 202
- Configure NAPT using CLI, on page 203
- NAPT configuration example, on page 204
- Configure SNAT using CLI, on page 204
- SNAT configuration example, on page 205
- Delete NAT rule using CLI, on page 205
- Delete all NAT rules, on page 206
- Verify NAT configuration using CLI, on page 206
- Verify NAT translations using CLI, on page 206

Network address translation

Network Address Translation (NAT) is a networking feature that ensures smooth and efficient roaming for Automated Guided Vehicles (AGVs) by using a single public IP address for AGVs to access the outside network and assigns port numbers to each application on the AGV, managing data flow for both downstream and upstream directions.

This feature is supported from UIW Release 17.16.1 only.

NAT functionalities

This feature supports the following functionalities:

- NAT with Port Translation (NAPT)
- Source NAT (SNAT)

NAT with Port Translation (NAPT) for downstream traffic manages and routes incoming data packets to the correct inside device. It uses an address table to find a specific application's inside private IP address and port number to forward the packet. For more information, see Downstream Data Flow using NAPT for AGVs.

Source NAT (SNAT) for upstream traffic modifies the source IP address and port numbers of the outgoing packets from inside network devices before sending them to an external network. For more information, see Upstream Data Flow using SNAT for AGVs.

Note

- NAT is supported only in the Layer 2 mode of the AP.
- The NAT/PAT feature supports rules configuration for TCP and UDP traffic only.

Advantage of NAT

A common IP address scheme for on-board vehicle systems reduces the complexity of uniquely identifying all vehicle equipment and facilitates access from external systems.

Downstream data flow using NAPT for AGVs

Downstream data flow using NAPT for AGVs is a network communication process that

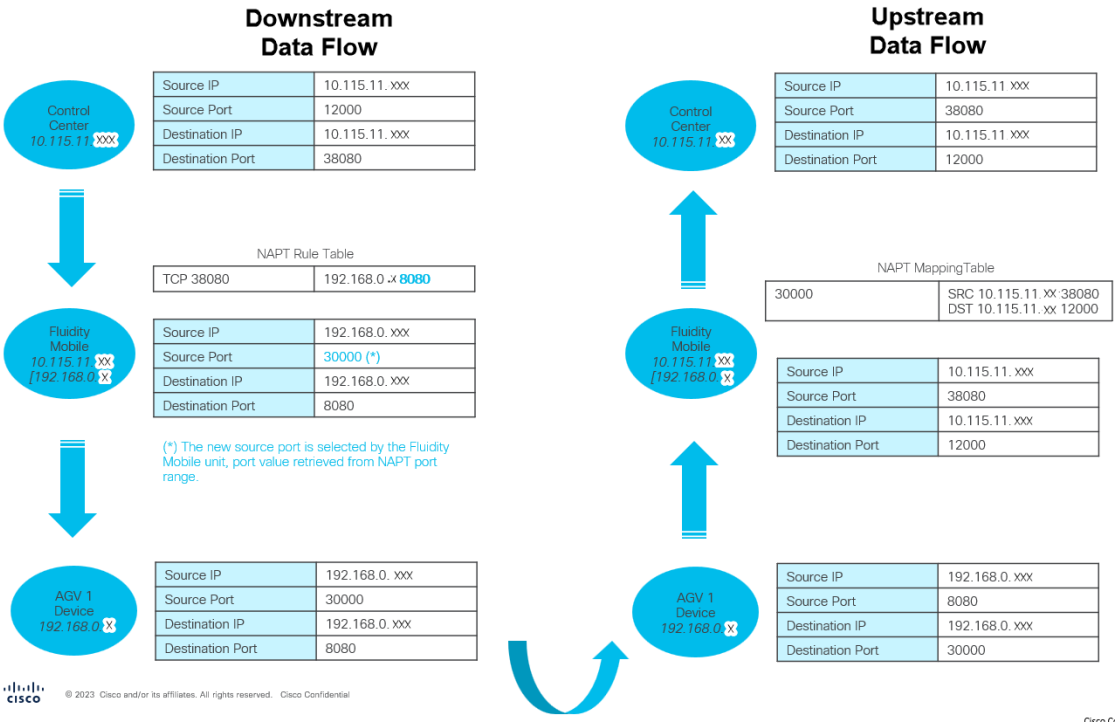
- enables data flow from the outside network to the AGV's inside network
- uses the AP as a gateway between the outside and inside networks
- employs NAPT address tables to find the inside private IP address and port number of specific applications to forward packets.

NAPT functionality for AGVs

By using NAPT:

- Devices from the outside network can connect to services on the AGVs' inside network.
- APs in the AGVs' inside network can direct data flow to specific ports.

Figure 16: Example of downstream data flow using NAPT:



Assign port numbers using NAPT for AGVs

NAPT assigns different port numbers to various services on an AGV. This ensures that responses from the outside network is sent to the correct service on the AGV.

Reserved outside port numbers for NAPT configuration

Protocol / Port Number	Service	Notes
TCP and UDP	—	Port numbers from 1 to 1023 are not allowed on both TCP and UDP protocols.
UDP/1812-1813	RADIUS	—
UDP/6600 UDP/6610	Industrial Wireless Monitor	On-Premises UDP and ping

Protocol / Port Number	Service	Notes
UDP/<telemetry port>	Industrial Wireless Telemetry	• Port number configured for Industrial Wireless Telemetry protocol varies. • The default value configured for Telemetry is 30000.

NAPT rule on AP

A NAPT rule is a network address and port translation rule that sends data flow to specific ports on inside hosts. A typical NAPT rule consists of `<Protocol, Global Destination Port, Translated Local Destination IP, Translated Local Destination Port>`, where the protocol can be either UDP or TCP.

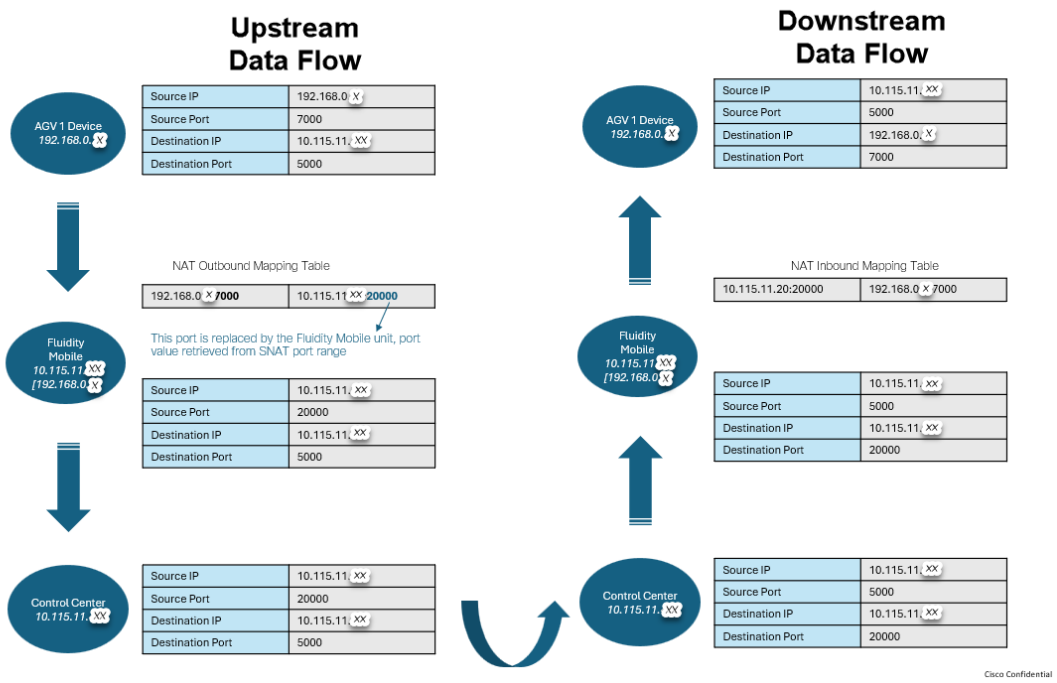
Upstream data flow using SNAT for AGVs

Upstream data flow using Source Network Address Translation (SNAT) for AGVs is a network process that transmits data from the inside network to the outside network through an access point gateway. SNAT modifies outgoing packet headers, changing the source IP address and source port in outgoing packets to match the public IP and port.

Network flow characteristics

The AP serves as a gateway between the inside and outside networks. The AP sends a packet from the inside network to the outside network. SNAT then changes the source IP address and source port in the outgoing packets to match the public IP and port.

Figure 17: Example of upstream data flow using SNAT:



Configure NAPT using CLI

Configure NAPT functionality to enable downstream data flow on the AP.

Perform this task to configure NAPT functionality to enable downstream data flow on the AP.

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the **configure ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat inside port range** *first-port-number second-port-number* command to configure inside port range on the NAT.

Example:

```
Device# configure ip nat inside port range 32000 33000
```

Inside port valid range is from 30000 to 35000. This range should not overlap the SNAT range.

Step 4 Use the **configure ip nat entry add proto** {**TCP** | **UDP**} **outside port** *outside-port-number* **inside ipv4** *inside-ipv4-address* **port** *inside-port-number* command to configure protocol, outside port value, inside IPv4 address, and inside port value on the NAT.

Example:

```
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2 port
8080
```

Step 5 Use the **write** command to save the current configuration.

Example:

```
Device#write
```

Step 6 Use the **reload** command to reload the device.

Example:

```
Device#reload
```

NAPT configuration example

This reference provides the configuration steps for Network Address Port Translation (NAPT) to enable address translation between inside and outside networks with port mapping capabilities.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat inside port range 32000 33000
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2
port 8080
Device# write
Device# reload
```

Configure SNAT using CLI

This task enables SNAT functionality to allow upstream data flow on the access point by configuring NAT rules, inside IPv4 addresses, outside port ranges, and saving the configuration.

Perform this task to configure SNAT functionality to enable upstream data flow on the AP.

Follow these steps to configure SNAT using CLI:

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the configure **ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat outside port range** *left-limit-port-number right-limit-port-number* command to configure outside port range on the NAT.

Example:

```
Device# configure ip nat outside port range 22000 23000
```

Outside port valid range is from 20000 to 25000. This range should not overlap the NAPT range.

Step 4 Use the **write** command to save the current configuration.

Example:

```
Device# write
```

Step 5 Use the **reload** command to reload the device.

Example:

```
Device# reload
```

SNAT configuration example

A sample configuration of SNAT to enable network address translation between inside and outside network parameters.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat outside port range 22000 23000
Device# write
Device# reload
```

Delete NAT rule using CLI

This task deletes a specific NAT rule on the AP.

Procedure

Use the **configure ip nat entry del** command to delete the specific NAT rule on the AP.

Example:

```
Device# configure ip nat entry del 0
```

Delete all NAT rules

This task deletes all NAT rules on the AP.

Procedure

Use the **configure ip nat entry del all** command to delete all the NAT rules on the AP.

Example:

```
Device#configure ip nat entry del all
```

Verify NAT configuration using CLI

The **show ip nat config** command displays the status of NAT configuration.

```
Device# show ip nat config
NAT: enabled
IP: 192.168.1.144
Netmask: 255.255.255.0
NAPT port range: 30000-35000
SNAT port range: 22000-23000
TCP timeout: 300
UDP timeout: 300
NAT max rules: 100
```

Verify NAT translations using CLI

The **show ip NAT translations** command displays all the NAT translations.

```
Device# show ip nat translations

NAT: enabled

Port NAT Translations
---------------------

TCP Translations
(192.168.50.4, 4000, 192.168.50.1, 34200) => (10.115.11.157, 4443, 10.115.11.250, 51010)
(10.115.11.250, 51010, 10.115.11.157, 4443) => (192.168.50.1, 34200, 192.168.50.4, 4000)

UDP Translations
None

Source NAT Translations
-----------------------
```

```
TCP Translations
(192.168.50.4, 51178, 10.115.11.250, 4000) => (10.115.11.157, 20292, 10.115.11.250, 4000)
(10.115.11.250, 4000, 10.115.11.157, 20292) => (10.115.11.250, 4000, 192.168.50.4, 51178)

UDP Translations
(10.115.11.250, 3000, 10.115.11.157, 22068) => (10.115.11.250, 3000, 192.168.50.4, 38318)
(192.168.50.4, 38318, 10.115.11.250, 3000) => (10.115.11.157, 22068, 10.115.11.250, 3000)
```

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)

© 2025 Cisco Systems, Inc. All rights reserved.