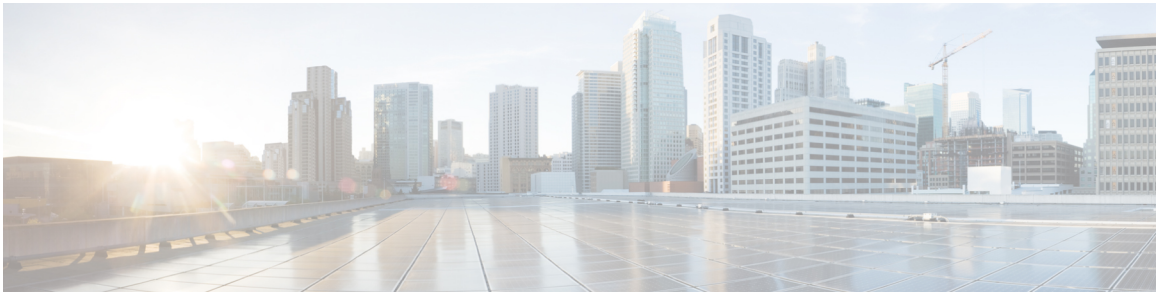


Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide, Cisco IOS XE 17.18.x

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

CHAPTER 1 **Introduction** 1

Cisco Catalyst IW9165E Access Points 1

Cisco Unified Industrial Wireless software releases information 2

CAPWAP modes 2

Unsupported features 4

Determine the correct software image for the AP 4

Verify software running on the AP 5

Convert the AP image between Wi-Fi, URWB, and WGB modes 6

Connect the computer to the AP console port 6

Related documentation 8

CHAPTER 2 **Workgroup Bridge** 9

Introduction and basics 9

Workgroup Bridge 9

WGB mode 9

uWGB mode 10

WGB mode recommendations 11

uWGB mode recommendations 12

Guidelines to reset the login credentials 12

Know your AP status using LED indicators 13

Initial setup and core configuration 14

Configure the WLAN profile 14

Configure wireless policy profile 15

Configure IP address 15

Configure an IPv4 address 15

Configure an IPv6 address 16
Configuring WGB on the Radio Interface 16
Create an SSID profile 17
Configure an SSID profile using open authentication 17
Configure an SSID profile using PSK authentication 18
Configure an SSID profile using Dot1x authentication 18
Configure radio interface for WGB 20
Configure security parameters 20
Configure an EAP profile 21
Configure Dot1X credential 22
Configure trustpoint manual enrollment for terminal 23
Configure trustpoint auto-enrollment 24
Configure manual certificate enrollment using a TFTPserver 25
Configure a PKCS12 or PFX or P12 certificate enrollment using a TFTP server 26
Verify the PKI timer information 27
Configure WGB or uWGB timer 27
Configure the association response timeout 27
Configure the authentication response timeout 27
Configure the EAP timeout 28
Configure the bridge client response timeout 28
Deauthenticate WGB wired client 28
Configure uWGB on the radio interface 28
Conversion between WGB and uWGB modes 29
Conversion from WGB to uWGB mode 29
Conversion from uWGB to WGB mode 30
Import and export WGB configuration 30
Import a WGB configuration 30
Export WGB configuration 30
Upgrade the uWGB image 31
Advanced features and optimizations 32
Configure transmission rate with high throughput 32
Configure legacy rate for WGB 33
802.11v features 33
Enable or disable 802.11v support 34

Configure BSS transition query interval 34
Verify neighbor list 35
Verify the channel list 35
Clear neighbor list 36
Auxiliary scanning 36
Scan-only mode 36
Configure scan-only mode 36
Configure scanning table timer 37
Manually add or remove channels from the channel list 37
Verify scanning table 38
Auxiliary Scanning handoff mode 38
Guidelines and restrictions for Auxiliary Scanning 39
Configure radio 2 in Aux-Scan handoff mode 39
Configure RSSI delta threshold for candidate BSSID 40
Verify WGB scan 41
Optimized roaming with dual-radio WGBs 41
Layer 2 NAT 42
Configure Layer 2 NAT 43
Verify Layer 2 NAT Configuration 43
Configuration Example of Host IP Address Translation 44
Configuration Example of Network Address Translation 46
Native VLAN on Ethernet Ports 46
Configure Native VLAN on Ethernet Ports 47
Low latency profile 47
Enable or disable an optimized-video EDCA profile 47
Enable or disable optimized-automation EDCA profile 48
Configure customized-wmm EDCA profile 49
Configure EDCA parameters using Controller GUI 50
Configure EDCA parameters using Controller CLI 51
A-MPDU 52
SNMP features 53
Supported SNMP MIB files 54
Supported OIDs 54
Configure SNMP parameters 59

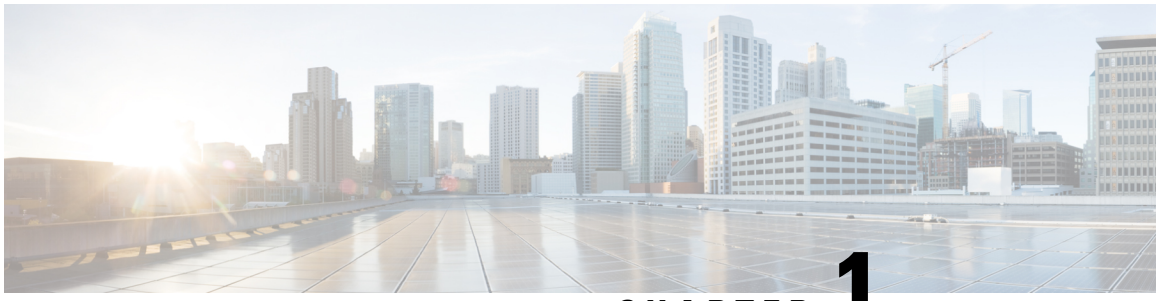
SNMP configuration examples 60
Verifying SNMP 61
QoS ACL classification and marking 61
Rule-based traffic classifications 62
QoS and ACL traffic classification methods 63
Configure QoS Mapping Profile 65
Verify Quality of Service Map 67
Packet Capture: TCP dump utilities 68
Enable wired packet captures 70
Disable wired packet captures 73
Verify wired packet capture 73
Port address translation 74
NAPT rules and mapping tables 75
Upstream and downstream data flows 76
Configure NAPT on WGB 77
Manage uWGB in NAPT deployment 79
Configure NAPT on uWGB 80
Delete NAPT mapping rule 82
Delete NAPT IP address 83
AAA user authentications 83
Configure AAA Server 84
Enable or disable RADIUS authentication for login user 85
Enable or disable TACACS+ authentication for login user 86
AAA authentication configuration example 86
Verification and monitoring 87
Verify the WGB and uWGB configuration 87
Syslog 89
Enable or disable the WGB syslog 89
Radio Statistics Commands 90
Configure event logging 92
Configure remote server 94

CHAPTER 3 **Manage the Workgroup Bridges through Web UI** 97
Workgroup Bridge 97

Access the Cisco Workgroup Bridge Web UI 98
Monitor the client details and configurations 98
Configure and authenticate wireless profiles 99
Create a WLAN 99
Create 802.1X profile 100
EAP profiles and SSID maps 101
Create EAP profile 101
Map EAP profile to SSID 102
Map the SSID to the uplink radio 102
Configure a static route for NAT wired client access to the WebUI in uWGB mode 103
Configure WGB and uWGB radio modes 104
Configure the radio in WGB mode 104
Configure uWGB mode on the radio 105
Set IP address 106
Switch from static IP to dynamic IP 106
Switch from dynamic IP to static IP 107
Modify the RSSI threshold 107
Create NAT rules 108
Manage firmware images 109
Reload the firmware image 109
Load a backup image 110
Perform a factory reset 110
Upgrade the firmware image 110
Import or export a configuration file 111

CHAPTER 4 **Control and Provisioning of Wireless Access Points** 113
Overview 113
Provisioning certificates on Lightweight Access Points 114
Understanding CAPWAP connectivity On AP 115
Reset button settings 117
Ethernet port usage on CAPWAP mode 117
Indoor deployment 118
Verify indoor deployment 118
AP Radio Slot 120

Supported fixed domains and country codes 120
Radio antenna settings 123
AFC support for 6 GHz standard power mode 124
Verify AFC status on an AP 125
GNSS support 125
Antenna disconnection detection 126
Verify Antenna Disconnection Detection on an AP or AP Profile 126
Troubleshooting 127



CHAPTER 1

Introduction

- Cisco Catalyst IW9165E Access Points, on page 1
- Cisco Unified Industrial Wireless software releases information, on page 2
- CAPWAP modes, on page 2
- Unsupported features, on page 4
- Determine the correct software image for the AP, on page 4
- Verify software running on the AP, on page 5
- Convert the AP image between Wi-Fi, URWB, and WGB modes, on page 6
- Connect the computer to the AP console port, on page 6
- Related documentation, on page 8

Cisco Catalyst IW9165E Access Points

The Cisco Catalyst IW9165E Access Point is a rugged wireless device designed to deliver ultra-reliable connectivity for moving vehicles and industrial machines.

- 2x2 Wi-Fi 6E design with external antennas for advanced wireless performance.
- IP30-rated durable construction for use in industrial and rugged environments.
- Low power consumption and compact form factor for easy integration into industrial assets.

Key features and industrial integration

The Catalyst IW9165E Access Points are specifically engineered to integrate seamlessly into industrial assets, thanks to their compact form factor and robust construction.

- Wi-Fi 6E Technology: Supports the latest wireless standards for improved performance and reliability.
- External Antennas: Provides enhanced signal strength and coverage.
- Durable Design: IP30-rated for use in rugged environments.
- Low Power Consumption: Optimized for energy efficiency.
- Compact Form Factor: Simplifies integration into industrial machines and moving vehicles.

These attributes make the Catalyst IW9165E APs a reliable choice for enabling wireless connectivity in demanding industrial settings.

Cisco Unified Industrial Wireless software releases information

The Cisco Unified Industrial Wireless (UIW) Software releases provide enhanced functionality for the Catalyst IW9165E , enabling it to operate in multiple modes for diverse industrial networking needs.

Features and operational modes

These updates are designed to deliver high availability, low latency, and seamless connectivity across various infrastructure setups, making the Catalyst IW9165E a versatile solution for industrial wireless networking.

Table 1: Operating modes and features

Mode	Introduced in Release	Functionality	Application
CURWB	17.12.1	Provides Cisco ultra-reliable wireless backhaul (CURWB) with low latency, zero packet loss, and seamless handoffs.	Mission-critical industrial applications.
WGB	17.13.1	Connects wired clients to Cisco AP infrastructure as a Wi-Fi client.	Cisco-based wireless environments.
uWGB	17.13.1	Connects wired clients to third-party AP infrastructure as a Wi-Fi client.	Third-party wireless environments. Both modes (WGB and uWGB) help in bridging the wired clients behind the WGB to the infrastructure's AP.
CAPWAP	17.14.1	Operates as a lightweight AP using the CAPWAP protocol.	Flexible AP management and deployment.

Note The IW9165E allows you to change its operating mode to CAPWAP, WGB, or URWB by simply updating its software, without replacing the hardware.

CAPWAP modes

CAPWAP modes are operational configurations that define how access points (APs) interact with wireless controllers and the network infrastructure.

- Each mode determines how the AP processes client traffic and performs network functions.

- Modes include Local, FlexConnect, Fabric, Sniffer, Monitor, and Site Survey.
- Modes are selected based on network requirements such as centralized management, resiliency, segmentation, monitoring, or RF analysis.

Modes of operation and their characteristics

CAPWAP modes categorize the operational behavior of APs in a network, affecting traffic handling, management, and additional wireless functions.

Table 2: CAPWAP Modes Comparison Table

Mode	Description	Key Features	Use Case
Local Mode	Default mode where AP serves clients and centralizes traffic through CAPWAP tunnels.	• Creates two CAPWAP tunnels. • Central switching (data bridges to controller).	Centralized traffic management.
FlexConnect	AP switches traffic locally while Controller manages it, ensuring operation even if Controller connection is lost.	• Local traffic switching. • Operates like an autonomous AP. • Resilient to Controller disconnection.	Resiliency and local traffic handling in branch offices or remote sites.
Fabric	AP establishes a VxLAN tunnel to the fabric edge, ensuring network segmentation.	• Maintains segmentation to AP. • Inserts SGT into VxLAN traffic. • Supports EN and PEN nodes.	Segmentation and secure communication in fabric-based networks.
Sniffer	AP captures air traffic on a specific channel for analysis using tools like Wireshark.	• Forwards packets to remote analysis tools. • Tags traffic with SGT during transit.	Network troubleshooting and packet analysis.
Monitor	AP acts as a sensor for LBS, rogue AP detection, and IDS without handling client traffic.	• Dedicated airwave monitoring. • Does not serve clients.	Security monitoring and intrusion detection.

Mode	Description	Key Features	Use Case
Site survey	AP used to configure RF parameters for site surveys. For information, see the AP Survey Mode section in the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .	Assists in RF analysis.	RF analysis for wireless planning.

Note Sniffer mode: Ensure both server and Controller must be on the same VLAN to avoid errors.

Functionalities of each CAPWAP mode

- Local mode: Default mode, two CAPWAP tunnels, central switching.
- FlexConnect mode: Local switching, behaves like an autonomous AP, works even if the controller is unavailable.
- Fabric mode: VxLAN tunnel to fabric edge, supports segmentation, SGT tagging.
- Sniffer mode: Captures packets, sends to analysis tools, tags traffic with SGT.
- Monitor mode: Acts as a sensor, no client traffic, supports LBS, IDS, rogue AP detection.
- Site survey mode: Used for RF configuration during site surveys.

Unsupported features

- 2.4 GHz radio, and
- Scan radio.

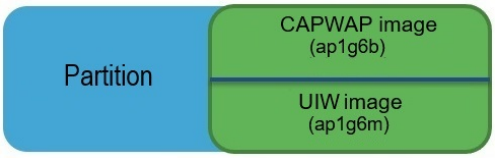
For more information about how to configure the AP on the Controller, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Determine the correct software image for the AP

Before you begin

Select the correct AP software image for the AP based on its mode of operation. This ensures proper functionality and compatibility of the device.

Software images for the AP are stored in various folders within the same section of the device. Each image corresponds to a specific AP mode, such as CAPWAP, URWB, or WGB/uWGB.



Procedure

Step 1 Locate the software images.

Navigate to the section where software images are stored on the AP. Ensure you have access to the appropriate folders containing the images.

Step 2 Identify the AP's mode.

Determine the operational mode of the AP. The device can operate in one of the following modes:

- CAPWAP
- URWB
- WGB or uWGB

Step 3 Select the corresponding software image.

Choose the software image that matches the device's mode of operation. Refer to the table below for the appropriate software image:

IW9165E mode	Software image
CAPWAP	`ap1g6b-k9w8-xxx.tar`
URWB	`UIW image ap1g6m-k9c1-xxx.tar`
WGB or uWGB	

Verify software running on the AP

You can use the **show version** command to determine the image running on AP.

- If the output is shown as **Cisco AP Software, (ap1g6b)** ; AP is running with the CAPWAP mode.

```
Cisco AP Software, (ap1g6b), C9165, RELEASE SOFTWARE
           Technical Support: http://www.cisco.com/techsupport
           Copyright (c) 1986-2024 by Cisco Systems, Inc.
           Compiled Tue Feb 20 23:04:29 GMT 2024
```

- If the output is shown as **Cisco AP Software (ap1g6m)** ; AP is running with the URWB mode or WGB/uWGB.

```
Cisco AP Software, (ap1g6m), C9165, RELEASE SOFTWARE
           Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Tue Feb 20 23:04:29 GMT 2024
```

Convert the AP image between Wi-Fi, URWB, and WGB modes

Perform this task to convert the AP's image between Wi-Fi (CAPWAP), URWB, and WGB modes. Image conversion is necessary to adapt the AP to different operational environments or network requirements.

Before you begin

Warning Image conversion performs a full factory reset, that erases all configurations and data on the device.

Procedure

Step 1 Use the **configure boot mode urwb** command to convert from CAPWAP to URWB mode or from WGB/uWGB to URWB mode.

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

Or

Step 2 Use the **configure boot mode capwap** command to convert from URWB to CAPWAP mode or from WGB/uWGB to CAPWAP mode.

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

Or

Step 3 Use the **configure boot mode wgb** command to convert from CAPWAP to WGB/uWGB mode or from URWB to WGB/uWGB mode.

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

Note
Once you perform these commands, the AP will reboot, and the new configuration will take effect.

Connect the computer to the AP console port

Perform this task to configure an access point locally without connecting it to a wired LAN. This access enables you to use the CLI and execute the configuration commands required for setup.

Before you begin

This task is applicable when direct access to the access point through a wired network is unavailable or unnecessary. You need a DB-9 to RJ-45 serial cable and a terminal emulator application to complete the task.

Procedure

Step 1 Connect the serial cable to the AP and computer.

- Attach a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the AP.
- Connect the other end of the cable to the COM port on your computer.

Step 2 Configure the terminal emulator.

- Launch a terminal emulator application on your computer.
- Configure the terminal emulator with these settings:

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

Step 3 Log In to the AP.

- Upon connecting, two command-prompt modes are available:
  - Standard Command Prompt (`>`)
  - Privileged Command Prompt (`#`)
- When you log in for the first time, the CLI shows the standard command prompt (>) for unprivileged commands.
- To switch to the privileged command prompt (#), enter the `enable` command (or its abbreviation `en`) and provide the enable password.

Step 4 Use default credentials to login.

- Username: `Cisco`
- Password: `Cisco`

Note
After the initial configuration completes, remove the serial cable from the AP.

Related documentation

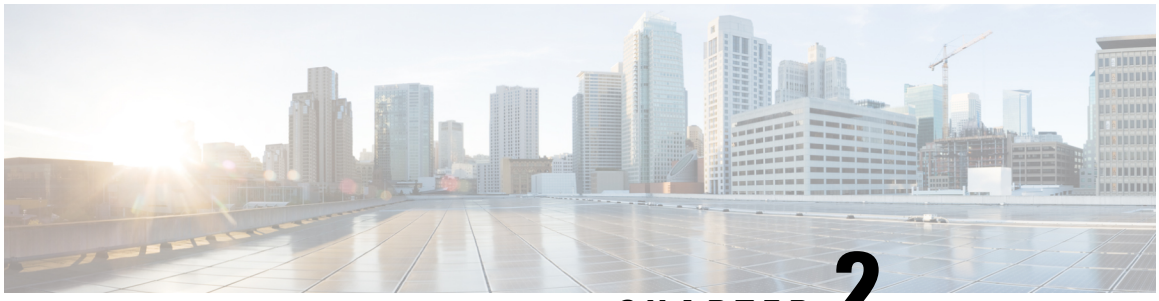
This topic provides links to related documentation and support information for the Cisco Catalyst IW9165 Rugged Series.

To view all support information for the Cisco Catalyst IW9165 Rugged Series, see https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html .

In addition to the documentation available on the support page, you will need to refer to these guides:

- For information about IW9165E hardware, see Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Hardware Installation Guide .
- A full listing of the AP's features and specifications is provided in Cisco Catalyst IW9165 Series Data Sheet .
- For information about Cisco URWB mode configuration, see the relevant documents at:

  https://www.cisco.com/content/en/us/support/wireless/catalyst-iw9165-rugged-series/series.html .
- For more information about the configuration on Cisco Catalyst 9800 Series Wireless Controllers, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .



CHAPTER 2

Workgroup Bridge

- Introduction and basics, on page 9
- Initial setup and core configuration, on page 14
- Upgrade the uWGB image, on page 31
- Advanced features and optimizations, on page 32
- AAA user authentications, on page 83
- Verification and monitoring, on page 87

Introduction and basics

Workgroup Bridge

A Workgroup Bridge (WGB) is a feature in wireless networking that allows a wired device or a group of wired devices to connect to a wireless network.

Both Workgroup Bridge (WGB) and Universal Workgroup Bridge (uWGB) modes are part of WGB and that enable seamless connectivity between wired and wireless networks.

From Unified Industrial Wireless (UIW) Release 17.13.1, both of these modes are supported on the Cisco Catalyst IW9165E Rugged Access Point (AP) and wireless client.

WGB mode

WGB mode provides wireless connectivity to wired clients connected to the Ethernet port of the WGB.

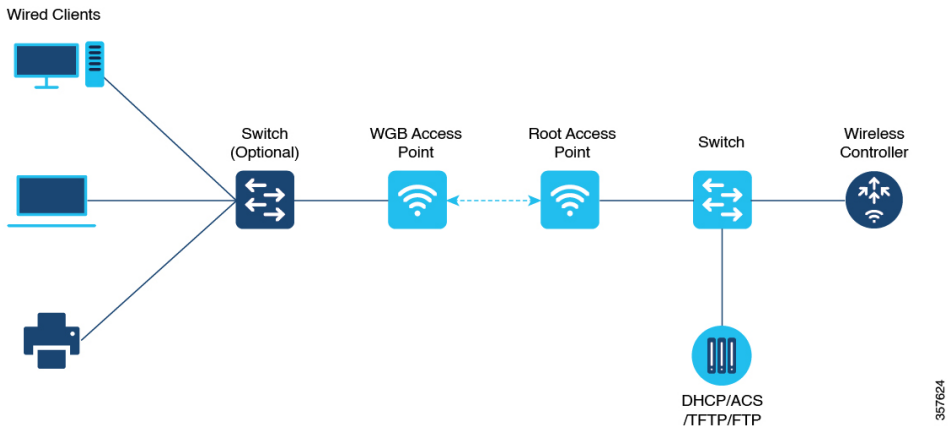
- Bridges the wired network to a wireless segment.
- Learns the MAC addresses of connected Ethernet-wired clients and shares these identifiers with the Controller. This is done through an AP infrastructure using Internet Access Point Protocol (IAPP) messaging.
- Establishes a single wireless connection to the root AP, which treats the WGB as a wireless client.

This mode is ideal for environments requiring wireless connectivity for wired devices that lack native wireless capabilities.

Use case of WGB mode

A factory floor uses wired devices such as sensors and PLCs, which lack built-in wireless connectivity. These devices connect to the WGB using Ethernet, and it bridges them to the wireless infrastructure through a single connection to the root AP.

Figure 1: WGB mode implementation



uWGB mode

uWGB mode is a complementary category to the WGB mode, designed to act as a wireless bridge between wired clients and wireless infrastructure.

- Supports both Cisco and non-Cisco wireless networks.
- Uses a wireless interface to connect with the AP, employing the radio MAC address for association.
- Ensures that wired clients connected to the uWGB can access wireless networks seamlessly.

Use case of uWGB mode

A retail store employs a point-of-sale (POS) system with wired devices that require connectivity to a wireless network. uWGB connects these devices to the store's wireless infrastructure, supporting both Cisco and non-Cisco wireless networks. The uWGB uses its wireless interface to associate with the AP, enabling seamless communication between the wired POS devices and the wireless network.

Use both of these modes to efficiently extend wireless capabilities to wired devices to enhance both network scalability and flexibility.

Comparison of key features of WGB and uWGB modes

This table outlines the differences between these two modes.

Feature	WGB mode	uWGB mode
Connectivity	Cisco wireless networks only	Cisco and non-Cisco wireless networks
Interface usage	Learns MAC addresses using Ethernet ports	Uses radio MAC address for association

WGB mode recommendations

Understand the limitations and restrictions of both WGB and uWGB modes to ensure optimal performance and avoid potential network issues.

- The WGB can associate only with Cisco lightweight access points.
- Speed and duplex settings are negotiated automatically based on the capabilities of the connected endpoint. Manual configuration is not supported on the wired-0 and wired-1 interfaces of the AP.
- When the WGB roams to a foreign controller, a wired client can connect to the WGB network. In this case, the anchor controller shows the IP address of the wired client, but the foreign controller does not.
- Deauthenticating a WGB record from a controller clears all entries of wired clients connected to that WGB.
- Wired clients connected to a WGB do not support:
  - MAC filtering
  - link tests
  - idle timeout
  - web authentication
- A WGB cannot associate with a WLAN configured with adaptive 802.11r.

Note The WGB drops Bridge Protocol Data Unit (BPDU) frames, which may lead to Layer 2 network loops.

IPv6 and IPv4 support

- The WGB supports IPv6 traffic exclusively for wired clients, even though IPv4 is enabled.
- IPv6 management does not function properly on the WGB, even if the device associates successfully with an uplink. In this scenario, IPv6 pings and SSH access to the WGB management IPv6 address fail.

Note Re-enable IPv6 on the WGB, even if it is already enabled and an IPv6 address has been assigned.

Channel bandwidth issue

If the infrastructure AP operates on a non-dynamic frequency selection (non-DFS) channel and changes its channel bandwidth, the WGB continues to use the original channel bandwidth.

Note Confirm that the WGB connects to the AP using the correct channel bandwidth.

uWGB mode recommendations

- TFTP and SFTP are not supported in uWGB mode. Perform software upgrades in WGB mode only. For more information, see uWGB Image Upgrade.
- uWGB mode supports wired clients connected to the wired0 interface. However, it doesn't support wired clients connected to the wired1 interface.
- You should configure an arbitrary non-routable IP address for uWGB. Using a static or dynamic IP address in the same range as the end device can result in unexpected behavior.
- From UIW Release 17.13.1, an AP in uWGB mode is managed using SSH. Image upgrade can be performed when no wired clients are connected to the AP.
  - When a wired client is detected, the AP in uWGB mode remains in the same uWGB mode. You cannot upgrade the image of the AP.
  - When a wired client is not detected, the AP in uWGB mode switches to WGB mode. You can manage as well as upgrade the image of the AP.

Guidelines to reset the login credentials

Credential requirements

Reset your login credentials in day 0 to ensure the security of your network device. Follow these guidelines to configure new login credentials after the first login.

Table 3: Username and password recommendations

Rule type	Details
Username length	must be between 1 and 32 characters
Password length	must be between 8 and 120 characters
Password must include	• at least one uppercase character • one lowercase character • one digit, and • one punctuation mark.
Password can include	• alphanumeric characters, and • special characters (ASCII decimal code from 33 to 126).
Password must exclude	• " (double quote), • ' (single quote), and • ? (question mark).

Rule type	Details
Password cannot	• contain three consecutive characters in sequence (ABC/ CBA), • contain three consecutive identical characters (AAA), and • be the same as or the reverse of the username.
Password must contain	A new password that must have at least four characters different from the current password.

Default credentials example:

```
Username: Cisco
Password: Cisco
Enable Password: Cisco
```

User credentials 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
```

Note In the provided example, passwords are displayed in plain text for clarity. In real-world scenarios, passwords are masked with asterisks (*).

Know your AP status using LED indicators

LED patterns are indicator light sequences that display the operational status and signal strength of a device.

These patterns use visual cues, such as blinking or solid lights, to convey specific conditions or performance metrics. In the context of the IW9165E device, LED patterns help identify system status and signal quality.

IW9165E LED Indicators

The IW9165E device features two LEDs located on the front panel:

1. System Status LED
2. RSSI Status LED

Table 4: Visual Reference: LED Status Indicators

LED	Color or Pattern	Indication
System Status LED	Blinking Red	WGB is disassociated.
	Solid Green	WGB is associated with the parent AP.
RSSI Status LED	Solid Green	RSSI ≥ -71 dBm.
	Blinking Green	RSSI between -81 dBm and -70 dBm.
	Solid Yellow	RSSI between -95 dBm and -81 dBm.
	Off	RSSI outside specified ranges.

Initial setup and core configuration

Configure the WLAN profile

The purpose of this procedure is to enable a Workgroup Bridge (WGB) to join a wireless network by configuring the WLAN and its associated configuration. Completing this configuration ensures that the WGB can establish secure and reliable communication with the access point (AP), thereby maintaining proper network connectivity.

Procedure

Step 1 Use the **wlan** *profile-name* command to enter the WLAN configuration submode.

Example:

```
Device# wlan test-wlan
```

Here, *profile-name* refers to the name of the configured WLAN.

Step 2 Use the **ccx aironet-iesupport** command to configure the Cisco Client Extensions (CCX) option and enable support for Aironet Information Element (IE) on the WLAN.

Example:

```
Device# ccx aironet-iesupport
```

Note
This configuration is mandatory for the WGB to associate with the AP.

Configure wireless policy profile

Perform this task to configure wireless policy profile and enable VLAN client support for a WGB on the AP. This ensures seamless client connectivity and proper VLAN assignment for WGBs in the network.

Before you begin

- Ensure that you have administrative access to the device before configuring.
- Verify that the VLAN ID you assign exists and is configured on the network infrastructure.

Procedure

Step 1 Use the **wireless profile policy** *profile-policy* command to access the wireless policy configuration mode for the desired profile.

```
Device# wireless profile policy Corp-Policy
```

Step 2 Use the **vlan** *vlan-id* command to map the WLAN policy profile to the corresponding VLAN ID.

```
Device# vlan 20
```

Step 3 Use the **wgb vlan** command to enable VLAN client support for the WGB.

```
Device# wgb vlan
```

Configure IP address

Configure an IPv4 address

Perform this task to configure an IPv4 address on a device using either the DHCP or a static configuration. This task ensures proper network connectivity and device management.

Procedure

Step 1 Configure an IPv4 address on a device using one of the options.

Option	Description
Dynamically obtain IPv4 address	Use the **configure ap address ipv4 dhcp** command. `Device# configure ap address ipv4 dhcp`
Manually assign a static IPv4 address	Use the **configure ap address ipv4 static** *ipv4_addr netmask gateway* command. `Device# configure ap address ipv4 static 192.168.10.25 255.255.255.0 192.168.10.1`

Step 2 (Optional) Use the **show ip interface brief** command to to view the current IP address configuration.

```
Device# show ip interface brief
```

Configure an IPv6 address

Perform this task to configure IPv6 address for the device.

Procedure

Step 1 Configure or obtain an IPv6 address on a device using one of the options.

Option	Description
Dynamically obtain IPv6 address	Use the **configure ap address ipv6 dhcp** command. `Device# configure ap address ipv6 dhcp`
Automatically obtain an IPv6 address	Use the **configure ap address ipv6 auto-config enable** command. `Device# configure ap address ipv6 auto-config enable` **Note** Enabling IPv6 auto-configuration also activates Stateless Address Auto-Configuration (SLAAC),but SLAAC does not apply to CoS of WGB. This command configures IPv6 address using DHCPv6 instead of SLAAC. Use the **configure ap address ipv6 auto-config disable** command to disable the IPv6 auto configuration on the AP.
Manually assign a static IPv6 address	Use the **configure ap address ipv6 static** *ipv6_addr prefix-length gateway* command. `Device# configure ap address ipv6 static 2001:db8:abcd:100::25 64 2001:db8:abcd:100::1` Configuring a static IPv6 address allows you to manage the AP through a wired interface, even if there is no uplink connection.

Step 2 (Optional) Use the **show ipv6 interface brief** command to verify current IP address configuration.

```
Device# show ipv6 interface brief
```

Configuring WGB on the Radio Interface

A Workgroup Bridge (WGB) provides a way for non-wireless, wired devices to gain access to a wireless network. By acting as a bridge, the WGB connects wired endpoints to the WLAN, extending wireless connectivity to equipment that does not have native Wi-Fi capability. To enable this functionality, you must first create an SSID profile that defines the wireless parameters. The WGB is then configured on the radio interface, after which the SSID profile is associated with the interface to establish the connection.

Summary

WGB allows non-wireless devices to connect to a wireless network. This configuration involves creating an SSID profile, configuring the WGB on the radio interface, and associating the SSID profile with the interface.

Workflow

1. Create an SSID Profile

   Choose the authentication method based on your network requirements.

2. Configure the Radio Interface

   Access the radio interface settings. Apply the required configuration to enable WGB functionality.

3. Associate the SSID Profile with the Radio

   Link the previously created SSID profile to the radio interface. This establishes the connection.

4. Enable the Radio Interface

   Activate the radio interface to complete the WGB configuration. This will begin operation.

Create an SSID profile

Before you begin

Perform this task to configure an SSID profile that meets your network's authentication requirements and ensures secure access for users.

Procedure

Select an authentication protocol for the SSID profile based on your network requirements.

Options are:

- Open authentication: Allows access without requiring user credentials.
- PSK authentication: Provides encryption for secure access.
- Dot1x authentication: Utilizes a centralized authentication server for user verification.

Note
For PSK configurations, ensure that the pre-shared key is strong and follows recommended security practices.

MSCHAPv2 authentication using RADIUS is incompatible with FIPS mode on Cisco IW9165E APs.

Configure an SSID profile using open authentication

Open authentication allows devices to connect to the network without requiring credentials, making it suitable for specific scenarios like guest networks or public access points.

Procedure

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication open** command to configure an SSID profile using open authentication.

```
Device# configure ssid-profile Guest-WiFi ssid Guest authentication open
```

Configure an SSID profile using PSK authentication

PSK authentication secures wireless networks by providing users with a shared key. This task provides instructions for configuring SSID profiles with PSK authentication, tailored to different key management protocols.

Procedure

Configure an SSID with PSK authentication, using one of these options: WPA2, 802.11r, or 802.11w.

Option	Description
Enhanced wireless security	Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command. `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management wpa2`
Fast roaming for mobile devices	Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command. `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management dot11r`
Management frame protection	Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command. `Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication psk StrongP@ss123 key-management dot11w`

Configure an SSID profile using Dot1x authentication

Dot1x authentication is a network access control method that enhances security by requiring user credentials before granting access. This task guides you in configuring the SSID profile with appropriate key management options.

Perform this task to set up an SSID profile with Dot1x authentication, ensuring secure network access using Extensible Authentication Protocol (EAP).

Procedure

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}} command to configure an SSID profile using Dot1x authentication.

```
Device# configure ssid-profile Corp-WiFi ssid CorpNet authentication eap profile EAP-Profile1
key-management wpa2
```

If..	Then..
If you want to enable fast roaming	Use the **dot11r** key-management option.
If WPA2 security is required	Use the **wpa2** key-management option.
If management frame protection is needed	Use the **dot11w** key-management option with **optional** or **required**.

Configure an SSID profile using Dot1x EAP-PEAP authentication

Before you begin

Perform this task to set up a secure SSID profile using Dot1x EAP-PEAP authentication, which provides enhanced security for wireless networks.

This task is applicable when configuring wireless profiles on devices that support Dot1x EAP-PEAP authentication. This ensures the device can authenticate securely using a specified username and password.

Procedure

Step 1 Use the **configure dot1x credential** *credential_name* **username** *username* **password** *password* command to create Dot1x credentials.

```
Device# configure dot1x credential Corp-Cred username corpuser password C!sc0Str0ng
```

Step 2 Use the **configure eap-profile** *profile_name* **dot1x-credential** *credential_name* command to configure the EAP profile and associate it with the configured Dot1x credentials.

```
Device# configure eap-profile Corp-EAP dot1x-credential Corp-Cred
```

Step 3 Use the **configure eap-profile** *profile_name* **method peap** command to define the EAP method for the profile as PEAP.

```
Device# configure eap-profile Corp-EAP method peap
```

Step 4 Use the **configure ssid-profile** *ssid-profile-name* **ssid** *ssid name* **authentication eap profile** *eap-profile-name* **key-management wpa2** command to create an SSID profile and set up authentication using the EAP profile.

```
Device# configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1 key-management
wpa2
```

Configure radio interface for WGB

Before you begin

The IW9165E device does not support a 2.4 GHz radio. Therefore, only the dot11radio 1 interface can be configured as the uplink to operate in WGB mode.

Configure the radio interface to enable the WGB mode and establish a connection to the appropriate SSID profile.

Procedure

Step 1 Use the **configure dot11radio** *slot_id* **mode wgb ssid-profile** *ssid-profile-name* command to configure a radio interface to a WGB SSID profile.

```
Device# configure dot11radio 1 mode wgb ssid-profile Corp-WiFi
```

Note
Ensure that the SSID profile being used is already configured and accessible by the device.

Step 2 Use the **configure dot11radio** *slot_id* **enable** command to enable a radio interface.

```
Device# configure dot11radio 1 enable
```

Step 3 (Optional) Use the **configure dot11radio** *slot_id* **disable** command to disable a radio interface.

```
Device# configure dot11radio 1 disable
```

Configure security parameters

Use this process to configure security parameters on the WGB to ensures secure authentication and encryption for wireless communication.

Procedure

Step 1 Set up the device parameters.

- Configure the device username and password.
- Configure the NTP server to ensure accurate time synchronization.
- Define the hostname and assign a valid IP address.

Step 2 Create and import trustpoints.

Establish trustpoints and import the required certificates using your preferred method.

Step 3 (Optional) Configure the dot1x credentials.

Provide the necessary dot1x username and password credentials if required by your setup.

Step 4 Create the EAP profile.

Map the EAP method, trustpoint name, and (optionally) the dot1x credentials to the EAP profile.

Step 5 Bind the EAP profile to the SSID profile.

Associate the EAP profile with the desired SSID profile to enable secure wireless connections.

Step 6 Bind the SSID profile to the radio.

Link the SSID profile to the preferred radio interface to activate the configuration.

Note

- Ensure that the NTP server is reachable and the certificates are valid to avoid authentication failures.
- Use a secure method to import certificates to maintain system integrity.
- If the certificate import fails, verify the certificate format and re-import using a valid method.

What to do next



Note If you make any modifications to the dot1x credential profile, trustpoint profile, or EAP profile, the changes do not take effect immediately. You must manually re-attach the EAP profile to the SSID profile for the changes to apply.

Use **configure ssid-profile** *ssid_prof_name* **ssid** *ssid***authentication eap profile** *eap_prof_name* **key-management** *key_type* command to re-attach the EAP profile to the SSID profile.

```
Device# configure ssid-profile Corp-SSID ssid CorpNet authentication eap profile Corp-EAP
key-management wpa2
```

Configure an EAP profile

This task guides you through the steps required to configure an Extensible Authentication Protocol (EAP) profile, ensuring secure and efficient authentication for your network.

Before you begin

An EAP profile is critical in ensuring secure authentication for wireless clients. Configuring the profile correctly ensures seamless integration with Dot1x credentials, SSID profiles, and radio configurations.

Before you begin configuring an EAP profile, ensure the following:

1. A valid Dot1x credential profile is already created.
2. The SSID profile has been configured.
3. The radio to which the SSID will be attached is properly set up.
4. Administrative access to the device's CLI.

Procedure

Step 1 Use the **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} command to configure the EAP profile with the desired method.

```
Device# configure eap-profile Corp-EAP method peap
```

If..	Then..
If the TLS method is selected for the EAP profile	Attach a CA trustpoint using Step 2.
If a profile is no longer needed	Use Step 4 to delete the EAP profile.

Step 2 Use the **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} command to attach the CA trustpoint for TLS. By default, the WGB uses the internal MIC certificate for authentication.

```
Device# configure eap-profile Corp-EAP trustpoint default
```

Note
To ensure any newly created trustpoint to take effect, update the trustpoint name that is mapped to the eap-profile.

Example:

```
Device# configure eap-profile Corp-EAP trustpoint Corp-CA
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* command to attach the dot1x-credential profile.

```
Device# configure eap-profile Corp-EAP dot1x-credential Corp-Cred
```

Step 4 (Optional) Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

```
Device# configure eap-profile Corp-EAP delete
```

Configure Dot1X credential

This task configures a Dot1X credential to ensure the device is correctly set up for 802.1X authentication, enabling secure access control and network protection.

Procedure

Step 1 Use the **configure dot1x credential** *credential-profile-name* **username** *username* **password** *password* command to configure the Dot1X credential.

```
Device# configure dot1x credential Corp-Cred username corpuser password C!sc0Str0ng
```

Step 2 (Optional) Use the **show wgb eap dot1x credential profile** command to view the status of the WGB EAP Dot1x profile.

```
Device# show wgb eap dot1x credential profile
```

Configure trustpoint manual enrollment for terminal

This procedure explains how to manually configure a trustpoint for terminal-based enrollment. It ensures secure communication between the device and the Certificate Authority (CA) server by enabling the use of a trusted certificate.

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** command to create a trustpoint for the WGB.

```
Device# configure crypto pki trustpoint Corp-CA enrollment terminal
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate the trustpoint manually.

Enter the base64-encoded CA certificate. If you use an intermediate certificate, you must import the entire certificate chain into the trustpoint. Type `quit` to finish.

```
Device# configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] command to configure the subject-name for the trustpoint.

```
Device# configure crypto pki trustpoint Corp-CA subject-name AP1.cisco.com US California SanJose
CorpNet IT admin@cisco.com
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and CSR.

```
Device# configure crypto pki trustpoint Corp-CA enroll
```

Note
Generate a digitally signed certificate on the CA server using the CSR output.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate.

```
Device# configure crypto pki trustpoint Corp-CA import certificate
```

Enter the base64-encoded CA certificate and type `quit` to finish importing the certificate.

Step 7 (Optional) Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

Example:

```
Device# configure crypto pki trustpoint Corp-CA delete
```

Step 8 (Optional) Use the **show crypto pki trustpoint** command to display a summary of all trustpoints.

```
Device# show crypto pki trustpoint
```

Step 9 (Optional) Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device# show crypto pki trustpoint Corp-CA certificate
```

Configure trustpoint auto-enrollment

Perform this task to configure auto-enrollment for trustpoints on a WGB, ensuring secure certificate management and streamlined operations.

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* command to enroll a trustpoint in the WGB using the server URL.

Example:

```
Device# configure crypto pki trustpoint Corp-CA enrollment url
http://192.168.71.2/certsrv/mscep/mscep.dll
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint.

Example:

```
Device# configure crypto pki trustpoint Corp-CA authenticate
```

Note
This command automatically fetches the Certificate Authority (CA) certificate from the CA server.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

Example:

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] command to configure the subject-name.

Example:

```
Device# configure crypto pki trustpoint Corp-CA subject-name AP1.cisco.com US California SanJose
CorpNet IT admin@cisco.com
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to enroll the trustpoint.

Example:

```
Device# configure crypto pki trustpoint Corp-CA enroll
```

Note
This step requests a digitally signed certificate from the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name***auto-enroll enable** *renew-percentage* command to enable auto-enroll.

Example:

```
Device#configure crypto pki trustpoint Corp-CA auto-enroll enable renew-percentage
```

Note
Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll disable** command to disable the auto-enroll.

Step 7 (Optional) Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

Example:

```
Device# configure crypto pki trustpoint Corp-CA delete
```

Step 8 (Optional) Use the **show crypto pki trustpoint** command to display a summary of all trustpoints.

Example:

```
Device# show crypto pki trustpoint
```

Step 9 (Optional) Use the **show crypto pki trustpoint** *trustpoint-name***certificate** command to view the content of the certificates that are created for a trustpoint.

Example:

```
Device# show crypto pki trustpoint trustpoint-name certificate
```

Configure manual certificate enrollment using a TFTPserver

Perform this task to manually enroll certificates using a TFTP server. This ensures secure communication by retrieving, authenticating, and managing certificates for a trustpoint.

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment server** *<proto>://<server_IP_address>/file-name* command to retrieve the CA and client certificate for a trustpoint.

Example:

```
Device# configure crypto pki trustpoint Corp-CA enrollment server 192.168.1.100/certs/corp-ca-cert.pem
```

Step 2

```
Device# configure crypto pki trustpoint Corp-CA authenticate
```

Note
This command retrieves and authenticates the CA certificate from the specified server. The server should contain the CA certificate file with **.ca** extension in the specified path.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to set the private key size.

```
Device# configure crypto pki trustpoint Corp-CA key-size 2048
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code state-name locality org-name org-unit email*] command to configure the subject-name.

```
Device# configure crypto pki trustpoint Corp-CA subject-name AP1.cisco.com US California SanJose
CorpNet IT admin@cisco.com
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and a CSR. Then copy the CSR to the TFTP server.

Example:

```
Device#configure crypto pki trustpoint Corp-CA enroll
```

Note
This generates certificate request and sends the request to the TFTP server. The filename to be written is appended with the **.req** extension.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate into the WGB.

```
Device#configure crypto pki trustpoint Corp-CA import certificate
```

The console terminal uses TFTP to import a certificate. The WGB attempts to retrieve the approved certificate from the TFTP. The filename to be written is appended with the **.crt** extension.

Step 7 (Optional) Use the **show crypto pki trustpoint** command to display a summary of all trustpoints.

```
Device# show crypto pki trustpoint
```

Step 8 (Optional) Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device# show crypto pki trustpoint Corp-CA certificate
```

Configure a PKCS12 or PFX or P12 certificate enrollment using a TFTP server

This task enables you to import a PKCS12 full certificate bundle for EAP-TLS authentication and private key configuration. This ensures secure communication and device authentication in WGB mode.

Procedure

Step 1 Use **configure crypto pki trustpoint** *trustpoint_name* **import pkcs12 tftp** *tftp://IP_ADDRESS/path_to_certificate* **password** *certificate_password* command to import PKCS12 full certificate bundle for EAP-TLS authentication and private key.

```
Device# configure crypto pki trustpoint Corp-CA import pkcs12 tftp tftp://1.2.3.4/corp-ca.p12
```

Step 2 (Optional) Use the **show crypto pki trustpoint** command to verify the downloaded PKCS12 certificate.

```
Device# show crypto pki trustpoint

Crypto PKI trustpoints are:-
================================================================
     Trustpoint name : example
   Enrollment method : TFTP
           TFTP path : tftp://192.168.0.1/users/example/ca
        CA-Cert file : /storage/wbridge_pki_cert/example/example_ca.pem
             Subject : C=US,ST=Unknown,L=Unknown,O=Cisco,OU=Wnbu,CN=ap.cisco.com
```

```
,emailAddress=wgb@cisco.com
            Key size : 2048
```

Verify the PKI timer information

Procedure

Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

```
Device#show crypto pki timers
```

Configure WGB or uWGB timer

Configure timers for the WGB or uWGB modes to ensure proper timeout settings for association, authentication, EAP, and bridge client responses. The CLI commands for timer configuration are identical for both the WGB and uWGB modes.

Configure the association response timeout

Procedure

Use the **configure wgb association response timeout** *response-millisecs* command to configure the WGB association response timeout.

```
Device#configure wgb association response timeout 400
```

- Default Value: 100 milliseconds
- Valid Range: 100–5000 milliseconds

Configure the authentication response timeout

Procedure

Use the **configure wgb authentication response timeout** *response-millisecs* command to configure the WGB authentication response timeout.

```
Device#configure wgb authentication response timeout 400
```

- Default Value: 100 milliseconds

- Valid Range: 100 –5000 milliseconds

Configure the EAP timeout

Procedure

Use the **configure wgb eap timeout** *timeout-secs* command to configure the WGB EAP timeout.

```
Device#configure wgb eap timeout 15
```

- Default value: 3 seconds
- Valid range: 2–60 seconds

Configure the bridge client response timeout

Procedure

Use the **configure wgb bridge client timeout** *timeout-secs* command to configure the WGB bridge client response timeout.

```
Device#configure wgb bridge client timeout 400
```

- Default Value: 300 seconds
- Valid Range: 10–1,000,000 seconds

Deauthenticate WGB wired client

Use the **clear wgb client** {**all** | **single** *mac-addr*} command to deauthenticate WGB wired client.

```
Device#clear wgb client all
```

Configure uWGB on the radio interface

The uWGB mode can associate with third-party APs using uplink radio MAC address, thus the uWGB role supports only one wired client.

Procedure

Use **configure dot11** *slot_id* **mode uwgb** *uwgb_wired_client_mac_address* **ssid-profile** *ssid-profile* command to configure the wired client's MAC address.

```
Device# configure dot11 1 mode uwgb 00:11:22:33:44:55 ssid-profile IoT-SSID
```

Note
Most WGB configurations also apply to uWGB mode. The only difference is that you configure wired client's MAC address using this command:

What to do next

These configurations outlines the detailed information about uWGB setup. The settings are common for both WGB and uWGB:

- Create an SSID profile, on page 17
- Configure dot1X credential
- Configure EAP-TLS security
- Configure an EAP profile
- Configure trustpoint manual enrollment for terminal
- Configure trustpoint auto-enrollment for WGB
- Configure manual certificate enrollment using a TFTP server
- Configure a PKCS12 or PFX or P12 certificate enrollment using a TFTP server
- Configure WGB or uWGB timer

Conversion between WGB and uWGB modes

Conversion from WGB to uWGB mode

Perform this task to convert the device from WGB to uWGB mode. This conversion enables enhanced functionality and integration of wired clients with the desired SSID profile.

Procedure

Use the **configure dot11radio** *radio_slot_id* **mode uwgb** *wired_client_mac* **ssid-profile** *ssid_profile_name* command to convert from WGB to uWGB mode.

```
Device#configure dot11radio 1 mode uwgb 00:11:22:33:44:55 ssid-profile IoT_Profile
```

Conversion from uWGB to WGB mode

Perform this task to convert an AP from uWGB mode to WGB mode, enabling it to function in WGB mode.

Procedure

Step 1 Use the **configure dot11radio** *radio_slot_id* **mode wgb ssid-profile** *ssid_profile_name* command to convert from uWGB to WGB mode. This conversion involves rebooting of the AP.

```
Device# configure dot11radio 1 mode wgb ssid-profile IoT_Profile

 This command will reboot with downloaded configs.
 Are you sure you want continue? [confirm]
```

Step 2 After entering the command, the system prompts you to confirm the action. This step is necessary as the AP reboots to apply the new configuration.

When prompted, type **confirm** to proceed with the conversion.

Import and export WGB configuration

Import a WGB configuration

Perform this task to download a sample configuration file to all WGBs in the deployment. This ensures the devices are configured with the necessary settings for proper operation.

Procedure

Use the **copy configuration download** {**tftp:**| **sftp:scp:**| | **http:**}*ip-address* [*directory*] [*file-name*] command to download a sample configuration to all WGBs in the deployment.

```
copy configuration download tftp: 192.168.1.100 configs startup-config.cfg
```

Note

- When you execute the **copy configuration download** command, the AP starts to reboot. The new configuration takes effect only after the reboot.
- Ensure that the configuration file is accessible from the specified `sftp:` or `tftp:` server and that the file path is correctly specified.

Export WGB configuration

Export the configuration of an existing WGB to make it reusable for newly deployed WGBs. This ensures consistency and simplifies deployment.

You can upload the current configuration of a WGB to a server using the appropriate protocol. This configuration file can later be downloaded to configure additional WGBs, streamlining the setup process.

Procedure

Upload the WGB configuration to a server

Use the **copy configuration upload** {**tftp:**| **sftp:**| **scp:**| **http:**}*ip-address* [*directory*] [*file-name*] command to upload the working configuration of an existing WGB to a server.

```
Device# copy configuration upload tftp: 192.168.1.100 configs running-config.cfg
```

Upgrade the uWGB image

To upgrade the uWGB software image, first convert the device from uWGB mode to WGB mode, as uWGB mode does not support TFTP or SFTP protocols for image upgrades. Then, download the software image by using either the TFTP or SFTP protocol. After the download, install the software image to complete the upgrade. Finally, revert the device from WGB mode back to uWGB mode.

Procedure

Step 1 Connect a TFTP or SFTP server to the wired 0 port of the uWGB.

Step 2 Use the **configure Dot11Radio** *slot_id* **disable** command to disable the radio interface.

```
Device#configure Dot11Radio 1 disable
```

Step 3 Use the **configure Dot11Radio** *slot_id* **mode wgb ssid-profile** *ssid_profile_name* command to configure the device to WGB mode using an existing SSID profile.

```
Device# configure Dot11Radio 1 mode wgb ssid-profile WGB-SSID


            This command will reboot with downloaded configs.
            Are you sure you want continue? <confirm>
```

Note
This command reboots the device with the downloaded configuration.

Step 4 Use the **configure ap address ipv4 static** *IPv4_address* *netmask* *Gateway_IPv4_address* command to assign a static IP address to the device.

```
Device# configure ap address ipv4 static 192.168.1.101 255.255.255.0 192.168.1.1
```

Step 5 Use the **ping** *server_IP* command to test ICMP connectivity to the server.

```
Device# ping 192.168.1.20
            Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds
            PING 192.168.1.20
            !!!!!
            Success rate is 100 percent (5/5), round-trip min/avg/max = 0.858/0.932/1.001 ms
```

Step 6 Use the **archive download/reload** [**tftp | sftp | http**] :// *server_ip* / *file_path* command to download andupgrade the uWGB image using TFTP, SFTP, or HTTP.

```
archive download /reload tftp://192.168.1.100/xxxx_iosxe.17.13.01.SPA.bin
```

Step 7 Use the **configure Dot11Radio** *slot_id* **mode uwgb** *wired_client_mac_addr* **ssid-profile** *ssid_profile_name* command to switch the device back to uWGB mode.

```
Device#configure Dot11Radio 1 mode uwgb 0011.2233.4455 ssid-profile uWGB-SSID
```

Advanced features and optimizations

Configure transmission rate with high throughput

To configure high throughput transmission rate for WGB in moving deployments, perform this task. You can manually limit the transmission rate using the high throughput modulation and coding scheme (MCS).

Procedure

Step 1 Use the **config dot11radio** *interface* **802.11ax disable** command to disable the 802.11ax standard on the specified dot11radio interface.

```
Device# config dot11radio 1 802.11ax disable
```

Step 2 Use the **config dot11radio** *interface* **802.11ac disable** disable command to disable the 802.11ax standard on the selected dot11radio interface.

```
Device# config dot11radio 1 802.11ac disable
```

Step 3 Use the **config dot11radio** *interface speed ht-mcs m4 m5* command to configure the desired HT MCS rate for the specified dot11radio interface. This action helps achieve the required transmission rates.

```
Device# config dot11radio 1 speed ht-mcs m4 m5
```

Step 4 (Optional) Use the **debug wgb dot11 rate** command to check the WGB Tx MCS rate. An example demonstrates the output of this command.

```
JWGB1#debug wgb dot11 rate
[*10/14/2023 03:16:08.6175]
[*10/14/2023 03:16:08.6175]                MAC    Tx-Pkts    Rx-Pkts                Tx-Rate(Mbps)                Rx-Rate(Mbps)  RSSI Tx-Retries
[*10/14/2023 03:16:08.6175] 24:16:1B:F8:02:6E          0          0          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70          0
JWGB1#[*10/14/2023 03:16:09.6179] 24:16:1B:F8:02:6E        330          3          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         15
[*10/14/2023 03:16:10.6183] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         25
[*10/14/2023 03:16:11.6187] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:12.6190] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         13
[*10/14/2023 03:16:13.6194] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         21
[*10/14/2023 03:16:14.6198] 24:16:1B:F8:02:6E        331          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         16
[*10/14/2023 03:16:15.6202] 24:16:1B:F8:02:6E        328          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         24
[*10/14/2023 03:16:16.6206] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         21
[*10/14/2023 03:16:17.6210] 24:16:1B:F8:02:6E        332          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         22
[*10/14/2023 03:16:18.6214] 24:16:1B:F8:02:6E        327          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         22
[*10/14/2023 03:16:19.6218] 24:16:1B:F8:02:6E        333          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         18
[*10/14/2023 03:16:20.6221] 24:16:1B:F8:02:6E        330          2          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -71         17
[*10/14/2023 03:16:21.6258] 24:16:1B:F8:02:6E        328          3          HT-20,1SS,MCS5,(52)          HT-20,1SS,MCS5,SGI(57)   -70         16
```

Configure legacy rate for WGB

You can also configure legacy rates for WGB if required.

Procedure

Use the **config dot11radio** *interface* **speed legacy-rate***legacy-rate* command to cofigure the specific legacy rate on the dot11radio interface.

```
Device# config dot11radio 1 speed legacy-rate basic-6.0
```

- Both 802.11 management and control frames use legacy rates.
- Ensure that the WGB's legacy rates match or overlap with the Access Point's (AP) legacy rates to avoid WGB association failures.

802.11v features

The 802.11v is a wireless network management standard that

- enables network-assisted roaming to optimize client connectivity,
- helps balance client load by providing guidance to client devices, and
- improves wireless performance through enhanced management frames and procedures.

802.11v is part of the IEEE 802.11 family of Wi-Fi standards. It includes features such as network-assisted roaming, which allows network infrastructure (such as wireless controllers) to direct clients to better access points (APs), reducing congestion and improving overall network efficiency.

Enhancement of roaming with 802.11v support

When 802.11v support is enabled on a Workgroup Bridge (WGB), it enhances roaming by enabling the WGB to proactively select optimal APs based on updated neighborhood information:

- The WGB can actively initiate roaming to suitable APs from dynamically updated lists.
- Periodic checks ensure that the WGB maintains the most accurate AP neighbor data, enabling optimal decisions during roaming.

Basic service set transition request frame

The Basic Service Set (BSS) Transition Request frame includes channel information of neighboring APs. Limiting scanning to these specified channels significantly reduces roaming latency in environments that use multiple channels.

Disassociate the client on the AP using WLC

The Wireless LAN Controller (WLC) can disassociate a client based on factors such as AP load, Received Signal Strength Indicator (RSSI), and data rate. Key points include:

- The WLC can notify 802.11v-enabled clients of an impending disassociation through the BSS transition management request frame.
- If the client fails to re-associate with another AP within a configurable time, the disassociation is enforced.

Additional reference information

Administrators can enable the disassociation-imminent configuration on the WLC, which activates the optional field within the BSS transition management request frame.

For detailed information of 802.11v configuration on the WLC, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Enable or disable 802.11v support

Enable 802.11v support on the WGB to optimize roaming performance by restricting channel scanning to those learned from the neighbor list.

Procedure

Enable or disable 802.11v support on WGB.

Option	Description
Enable 802.11v support on WGB	Use the **configure wgb mobile station interface dot11Radio** *radio_slot_id* **dot11v-bss-transition enable** command. `Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition enable` **Note** • When 802.11v support is enabled, the WGB scans only the channels provided in the neighbor list, improving efficiency during roaming. • Ensure that the neighbor list is properly configured on the infrastructure side to facilitate seamless channel transitions.
Disable 802.11v support on WGB	Use the **configure wgb mobile station interface dot11Radio** *radio_slot_id* **dot11v-bss-transition disable** command. `Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition disable`

Configure BSS transition query interval

Perform this task to configure the time interval at which the WGB sends BSS transition query messages to the parent AP. This ensures optimal network performance by managing the frequency of transition queries.

Procedure

Use **configure wgb neighborlist-update-interval** *interval* command to configure the time interval that WGB sends BSS transition query message to the parent AP.

```
Device# configure wgb neighborlist-update-interval 50
```

Note
The valid range is from 1 to 100 and the default value is 10. Configure the time interval in seconds format.

Verify neighbor list

Ensure the neighbor list received from the associated AP is accurate and up to date.

Procedure

Use **show wgb dot11v bss-transition neighbour** command to display the neighbor list received from the associated AP.

```
Device#show wgb dot11v bss-transition neighbour
```

Note

- This command provides details about neighboring APs that the device can transition to as part of 802.11v wireless network enhancements.
- Accurate neighbor lists can improve handoff and roaming efficiency for wireless clients.

Verify the channel list

Verify the channel list to ensure the device is correctly identifying channels from the dot11v neighbor, auxiliary radio scan, and residual channel scan. This step is crucial for troubleshooting connectivity or performance issues related to wireless networks.

Procedure

Use **show wgb dot11v bss-transition channel** command to check channel list from dot11v neighbor, aux radio scanned, and residual channel scanned.

```
Device#show wgb dot11v bss-transition channel
```

Note
This command is typically used in scenarios where you need to validate the channels identified by the WGB.

Clear neighbor list

Perform this task to clear the neighbor list for error condition recovery. This ensures optimal device performance by resolving potential connectivity issues related to neighbors.

Procedure

Use **clear wgb dot11v bss-transition neighbor** command to clear neighbor list to provide error condition recovery.

```
Device#clear wgb dot11v bss-transition neighbor
```

Note
This command is used specifically to reset the neighbor list in scenarios where error conditions need to be resolved.

Auxiliary scanning

You can configure aux-scan mode as either scanning-only or handoff mode on WGB radio 2 (5 GHz) to improve roaming performance.

Scan-only mode

The scanning-only mode is a wireless access point operational mode that:

- enables radio operation exclusively for scanning,
- continuously monitors the wireless environment to collect data on network performance, interference, and rogue devices, and
- allows configuration of scanning parameters such as channel lists and scanning intervals.

When slot 2 radio is configured in scanning-only mode, slot 1 (5G) radio is always selected as the uplink. Slot 2 (5G) radio continues to scan the configured SSID based on the channel list. By default, the channel list contains all supported 5G channels (based on reg domain). You can configure the scanning list manually, or the device can learn it from 802.11v.

When roaming is triggered, the algorithm looks for candidates in the scanning table and skips the scanning phase if the table is not empty. The WGB then associates to the selected candidate AP.

Configure scan-only mode

Enable the device to operate in scan-only mode, facilitating network monitoring and assessment without transmitting data.

Procedure

Use the **configure dot11Radio 2 mode scan only** command to configure scanning only mode.

```
Device# configure dot11Radio 2 mode scan only
```

Configure scanning table timer

Adjust the scanning table timer to optimize the candidate AP selection process and prevent roaming failures caused by outdated RSSI values.

Before you begin

The scanning table maintains a list of candidate APs detected by the device. By default, entries in this table expire after 1200 milliseconds. Modifying the expiration timer may help improve roaming efficiency by allowing more time for RSSI updates.

Procedure

Use the **configure wgb scan timeout** *interval* command to adjust the timer. By default, candidate AP entries in scanning table are automatically removed in 1200 ms.

```
Device#configure wgb scan timeout 1500
```

Note

- Scanning AP expire time is from 1 to 5000.
- From the scanning table, the AP selects the candidate with the best RSSI value. However, sometimes the RSSI values might not be updated and it lead to roaming failures.

Manually add or remove channels from the channel list

Perform this task to manually add or remove channels from the channel list to optimize wireless network performance or for specific configuration requirements.

Procedure

Add or remove channels from the channel list using one of the options.

Option	Description
Add a channel to the channel list	Use the **configure wgb mobile station interface dot11Radio** *interface* **scan** *channel* **add** command. `Device#configure wgb mobile station interface dot11Radio 1 scan 36 add`

Option	Description
Remove a channel from the channel list	Use the **configure wgb mobile station interface dot11Radio** *interface* **scan** *channel* **delete** command. `Device# configure wgb mobile station interface dot11Radio 1 scan 36 delete`

Verify scanning table

Perform this task to confirm the current AP scanning details and identify the best AP for optimal connectivity.

Procedure

Use **show wgb scan** command to verify the scanning table.

```
Device#show wgb scan
Best AP expire time: 5000 ms

************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:E2:4F     84     136       1531
FC:58:9A:15:DE:4F     37     136       41

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4F    37     136       41
```

Auxiliary Scanning handoff mode

An Auxiliary Scanning handoff mode is a wireless radio configuration that

- allows both radios (radio 1 and radio 2) to serve as uplink connections,
- supports dynamic switching of roles and traffic between radios after each roaming event, and
- enables efficient roaming by using a scanning radio to associate with the best available access point.

The Auxiliary Scanning list can be manually configured or learned automatically using the 802.11v standard. This handoff mode improves roaming performance by quickly associating with the best available access point.

Radio roles

The radio 2 shares the same MAC address with the radio 1 and supports scanning, association, and data serving. Both radios can operate in either a serving or scanning role. After each roaming event, the roles and traffic automatically switch between radio 1 and radio 2.

Roaming of AP

When roaming is triggered, the system algorithm checks the scanning database for the best AP to establish a connection. WGB always uses the radio in the scanning role to complete the roaming association with the new AP. This configuration reduces roaming interruptions to between 20 and 50 milliseconds.

This table shows an example of aux-scan handoff radio mode configuration on IW9165E:

Slot 0 (2.4 G)	Slot 1 (5G)	Slot 2 (5G only)	Slot 3 (scanning radio)
N/A	WGB	Scan handoff	N/A

This table shows how long roaming interruptions last for different methods when using three different modes:

Roaming interruption time	Normal channel setting	Auxiliary Scanning only	Auxiliary Scanning Handoff
Scanning	(40+20)*3=180 ms	0-40 ms	0 ms
Association	30-80 ms	30-80 ms	20-50 ms
Total	~210 ms	70-120 ms	20-50 ms

Guidelines and restrictions for Auxiliary Scanning

- The `different-parent` threshold applies to both `scan-only` and `handoff` modes.
  - In `scan-only` mode, roaming decisions are strictly based on selecting a different candidate BSSID. This supports combinations such as dual 2.4 GHz and dual 5 GHz.
  - In `handoff` mode, the WGB can either roam to a different BSSID or switch radios while remaining on the same parent BSSID.
- The `same-parent` threshold is only relevant when the WGB is operating in `handoff` mode.

Configure radio 2 in Aux-Scan handoff mode

Perform this task to configure the WGB slot 2 radio in auxiliary-scan handoff mode, ensuring seamless connectivity and optimized network performance.

Before you begin

Auxiliary-scan handoff mode allows the radio to scan for available access points without interrupting active connections. This feature is particularly useful for improving handoff reliability in environments with multiple access points.

Procedure

Step 1 Use the **configure dot11Radio** *radio-num* **mode scan handoff** command to configure the WGB slot 2 radio to aux-scan mode:

```
Device# configure dot11Radio 2 mode scan handoff
```

Step 2 (Optional) Use the **show running-config** command to view the radio configuration.

```
Device# show running-config
...
Radio Id                    : 1
   Admin state              : ENABLED
   Mode                     : WGB
   Spatial Stream           : 1
   Guard Interval           : 800 ns
   Dot11 type               : 11n
   11v BSS-Neighbor         : Disabled
   A-MPDU priority          : 0x3f
   A-MPDU subframe number   : 12
   RTS Protection           : 2347(default)
   Rx-SOP Threshold         : AUTO
   Radio profile            : Default
   Encryption mode          : AES128
Radio Id                    : 2
   Admin state              : ENABLED
   Mode                     : SCAN - Handoff
   Spatial Stream           : 1
   Guard Interval           : 800 ns
   Dot11 type               : 11n
   11v BSS-Neighbor         : Disabled
   A-MPDU priority          : 0x3f
   A-MPDU subframe number   : 12
   RTS Protection           : 2347(default)
   Rx-SOP Threshold         : AUTO
   Radio profile            : Default
```

Configure RSSI delta threshold for candidate BSSID

This section explains how the WGB evaluates candidate APs during auxiliary scans. By adjusting the RSSI delta threshold, you can control how much stronger a new signal must be before it triggers a roam or radio switch. This adjustment helps prevent unnecessary transitions when signal strengths are similar.

Procedure

Step 1 Use the **configure wgb mobile aux-scan delta-rssi different-parent***threshold* command to configure the RSSI-delta threshold (in dB) when the candidate BSSID is different from the current BSSID.

```
Device# configure wgb mobile aux-scan delta-rssi different-parent 7
```

Default threshold value is 6 dB.

Step 2 Use the **configure wgb mobile aux-scan delta-rssi same-parent***threshold* command to configure the RSSI-delta threshold (in dB) when the candidate remains on the same parent BSSID.

```
Device# configure wgb mobile aux-scan delta-rssi same-parent 7
```

Note
This applies only in handoff mode.

Default threshold value is 100 dB.

Verify WGB scan

Perform this task to confirm the current role of each radio and analyze the auxiliary scanning results, including the best AP selection and performance metrics.

WGB scan provides detailed information about the auxiliary scanning process for each radio. This data helps to determine the best AP based on signal strength (RSSI), channel, and scan time.

Procedure

Use the **show wgb scan** command to view the current role of each radio and the results of aux scanning.

```
Device#show wgb scan
Best AP expire time: 2500 ms

Aux Scanning Radio Results (slot 2)
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     54     153       57
FC:58:9A:15:E2:4E     71     153       64

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    54     153       57

Aux Serving Radio Results
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     58     153       57
FC:58:9A:15:E2:4E     75     153       133

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    58     153       57
```

Optimized roaming with dual-radio WGBs

Dual-radio WGBs are wireless workgroup bridges that

- use two radios to enhance roaming efficiency,
- minimize service disruption by skipping the active scanning phase with an existing scanning table, and
- initiate roaming when beacon frames are missed or packet retry thresholds are reached.

From the Cisco IOS-XE 17.15.1 release, devices with dual-radio configurations have improved roaming efficiency. This reduces service downtime.

Trigger factors for roaming

Trigger factors for roaming include:

- Low RSSI: Measures the power level that a wireless device, such as an AP, receives from a signal. Use RSSI values to determine the quality of the wireless connection to troubleshoot and optimize wireless networks.
- Beacon miss-count: Indicates the number of consecutive beacon frames that a client device has missed from an AP in a wireless network.
- Maximum packet retries: Specifies the maximum number of times a data packet can be retransmitted if the client device does not send an acknowledgement.

Configuration options for dual-radio

Here are the possible configurations for the IW9165E AP in a dual-radio setup:

Dual-radio	AP
5 GHz radio 1 + radio 2 (scanning only mode)	IW9165E
5 GHz radio 1 + radio 2 (aux-scan handoff mode)	

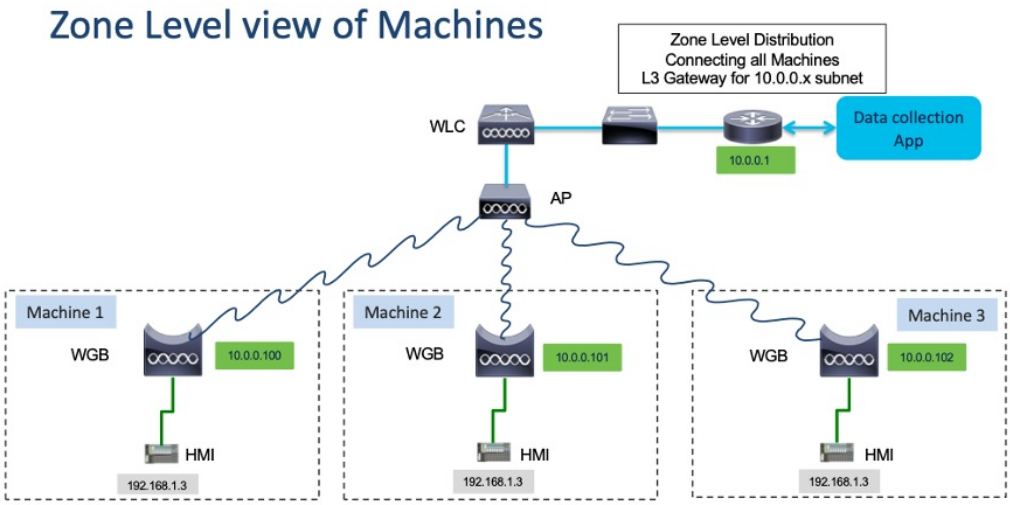
Layer 2 NAT

One-to-one (1:1) Layer 2 NAT allows you to assign a unique public IP address to an existing private IP address (end device). This enables the end device to communicate with a public network.

Layer 2 NAT maintains two translation tables:

- private-to-public subnet translations
- public-to-private subnet translations

In industrial deployments, such as Human Machine Interfaces (HMIs) or robots, the same firmware is often programmed on every machine. This results in duplicate IP addresses across multiple devices. Layer 2 NAT resolves this issue by enabling devices with duplicate private IP addresses to communicate with public networks.



Configure Layer 2 NAT

The Layer 2 NAT (Network Address Translation) configuration commands are used to control IP address translation for wired clients within a VLAN at Layer 2.

These commands allow administrators to:

- Enable or disable Layer 2 NAT globally on the device.
- Define a default VLAN where NAT rules are applied.
- Translate individual host addresses from private to public, or from public to private.
- Translate entire subnets from private-to-public or public-to-private.

This configuration ensures seamless communication between private networks and external/public networks by dynamically or statically mapping IP addresses, while maintaining VLAN-based traffic segregation.

Procedure

Step 1 Use the **configure l2nat** {**enable** | **disable**} command to enable or disable Layer 2 NAT.

```
Device# configure l2nat enable
```

Step 2 Use the **configure l2nat default-vlan** *vlan_id* command to define the VLAN where all NAT rules are applied.

```
Device# configure l2nat default-vlan 10
```

Note
If you do not specify a VLAN ID, VLAN 0 is used.

Step 3 Use the **configure l2nat** {**add** | **delete**} **inside from host** *original_ip_addr* **to** *translated_ip_addr* command to translate a private IP address of a wired client to a public IP address.

```
Device# configure l2nat add inside from host 192.168.1.10 to 203.0.113.10
```

Step 4 Use the **configure l2nat** {**add** | **delete**} **outside from host** *original_ip_addr* **to** *translated_ip_addr* command to translate a public IP address to a private IP address.

```
Device# configure l2nat add outside from host 203.0.113.20 to 192.168.1.20
```

Step 5 Use the **configure l2nat** {**add** | **delete**} **inside from network** *original_nw_prefix* **to** *translated_nw_prefix subnet_mask* command to translate a private subnet to a public subnet.

```
Device# configure l2nat add inside from network 192.168.1.0 to 203.0.113.0 255.255.255.0
```

Step 6 Use the **configure l2nat** {**add** | **delete**} **outside from network** *original_nw_prefix* **to** *translated_nw_prefix subnet_mask* command to translate a public subnet to a private subnet.

```
Device# configure l2nat add outside from network 203.0.113.0 to 192.168.1.0 255.255.255.0
```

Verify Layer 2 NAT Configuration

Use the following commands to verify Layer 2 NAT configuration, check translation statistics, and clear rules or counters for troubleshooting.

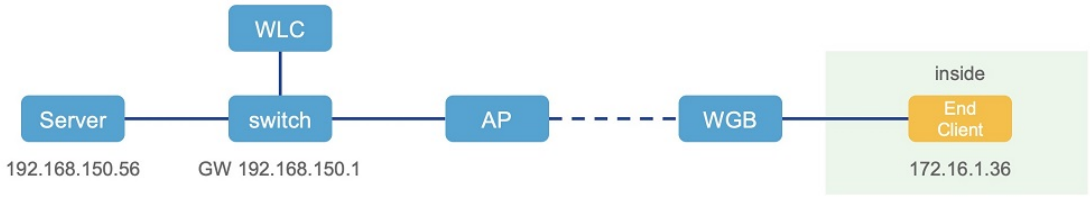
- **show l2nat entry**: Displays the Layer 2 NAT running entries.
- **show l2nat config**: Displays the Layer 2 NAT configuration details.
- **show l2nat stats**: Displays the Layer 2 NAT packet translation statistics.
- **show l2nat rules**: Displays the Layer 2 NAT rules from the configuration.
- **clear l2nat statistics**: Clears packet translation statistics.
- **clear l2nat rule**: Clears Layer 2 NAT rules.
- **clear l2nat config**: Clears Layer 2 NAT configuration.
- **debug l2nat**: Enables debugging of packet translation process.
- **debug l2nat all**: Prints out the NAT entry match result when a packet arrives.

Caution This command may create overwhelming log print in console. Console may lose response because of this command, especially when Syslog service is enabled with a broadcast address.

- **undebug l2nat**: Disables debugging of packet translation process.

Configuration Example of Host IP Address Translation

In this scenario, the end client (172.16.1.36) connected to WGB needs to communicate with the server (192.168.150.56) connected to the gateway. Layer 2 NAT provides an address for the end client on the outside network (192.168.150.36) and an address for the server on the inside network (172.16.1.56).



Layer 2 NAT configuration example

This example displays Layer 2 NAT configuration details. In the output, I2O means 'inside to outside' and O2I means 'outside to inside.

```
Device# show l2nat config

L2NAT Configuration are:
==================================
Status: enabled
Default Vlan: 0
The Number of L2nat Rules: 4
Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

Layer 2 NAT rules example

This example displays the Layer 2 NAT rules.

```
Device# show l2nat rule

Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

Layer 2 NAT entries example

This example displays the current Layer 2 NAT entries.

```
Device# show l2nat entry

Direction           Original            Substitute            Age    Reversed
inside-to-outside   172.16.1.36@0       192.168.150. 36@0     -1     false
inside-to-outside   172.16.1.56@0       192.168.150. 56@0     -1     true
inside-to-outside   172.16.1.1@0        192.168.150. 1@0      -1     false
inside-to-outside   172.16.1.255@0      192.168.150. 255@0    -1     false
outside-to-inside   192.168.150.36@0    172.16.1.36@0         -1     true
outside-to-inside   192.168.150.56@0    172.16.1.56@0         -1     false
outside-to-inside   192.168.150.1@0     172.16.1.1@0          -1     true
outside-to-inside   192.168.150.255@0   172.16.1.255@0        -1     true
```

WGB wired clients example

This example displays the WGB wired clients over the bridge.

Before Layer 2 NAT is enabled:

```
Device# show wgb bridge
    ***Client ip table entries***
              mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0      172.16.1.36     0.360000      true
24:16:1B:F8:05:0F   0 wbridge1       0          0.0.0.0  3420.560000      true
```

After Layer 2 NAT is enabled:

```
Device# show wgb bridge
    ***Client ip table entries***
              mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0   192.168.150.36     0.440000      true
24:16:1B:F8:05:0F   0 wbridge1       0          0.0.0.0  3502.220000      true
```



Note If the wired client in NAT experiences E2E traffic issues, you can restart the client registration process by using the **clear wgb client single** command:

Layer 2 NAT packet translation statistics example

This example displays the Layer 2 NAT packet translation statistics.

```
Device# show l2nat stats

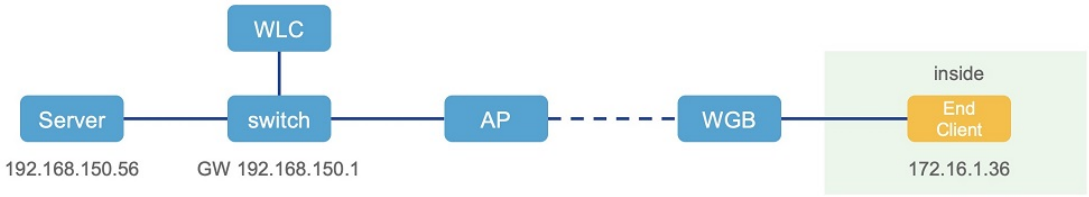
Direction          Original             Substitute            ARP  IP   ICMP UDP  TCP
inside-to-outside  172.16.1.1@2660      192.168.150.1@2660    1    4    4    0    0
inside-to-outside  172.16.1.36@2660     192.168.150.36@2660   3    129  32   90   1
```

```
inside-to-outside  172.16.1.56@2660      192.168.150.56@2660   2    114  28   85   1
inside-to-outside  172.16.1.255@2660     192.168.150.255@2660  0    0    0    0    0
outside-to-inside  192.168.150.1@2660    172.16.1.1@2660       1    4    4    0    0
outside-to-inside  192.168.150.36@2660   172.16.1.36@2660      3    39   38   0    1
outside-to-inside  192.168.150.56@2660   172.16.1.56@2660      2    35   34   0    1
outside-to-inside  192.168.150.255@2660  172.16.1.255@2660     0    0    0    0    0
```

Note To reset the statistics, you can use the **clear l2nat stats** command.

Configuration Example of Network Address Translation

In this scenario, Layer 2 NAT translates inside addresses in the 172.16.1.0/24 subnet to addresses in the 192.168.150.0/24 subnet, replacing only the network prefix during translation. The host bits remain the same.



The command used for this scenario is here:

```
Device# configure l2nat add inside from network 172.16.1.0 to 192.168.150.0 255.255.255.0
```

Native VLAN on Ethernet Ports

In a typical Workgroup Bridge (WGB) deployment, a single wired client connects directly to the WGB Ethernet port. Consequently, the wired client traffic must reside on the same VLAN as the WGB management VLAN. If you require the wired client traffic to be on a different VLAN than the WGB management VLAN, configure the native VLAN on the Ethernet port.

Important Configuring native VLAN ID per Ethernet port is not supported. Both Ethernet ports share the same native VLAN configuration.

Caution When WGB broadcast tagging is enabled and a single wired passive client connects directly to the WGB Ethernet port, an issue may arise where the infrastructure downstream (DS) side client fails to ping the WGB behind the passive client. To resolve this, configure the following commands: `configure wgb ethport native-vlan enable` and **configure wgb ethport native-vlan id X**, where X is the same VLAN as the WGB management VLAN.

To verify your configuration, use the **show wgb ethport config** or **show running-config** command.

Configure Native VLAN on Ethernet Ports

The native VLAN configuration commands are used to manage how untagged traffic is handled on the Workgroup Bridge (WGB) Ethernet port.

These commands allow administrators to:

- Enable or disable native VLAN configuration on the WGB Ethernet port.
- Specify the native VLAN ID to ensure that untagged traffic is correctly assigned to the intended VLAN.

Procedure

Step 1 Use the **config wgb ethport** *ethport* **native-vlan** {**enable** | **disable** } command to enable or disable native VLAN configuration.

```
Device# config wgb ethport 1 native-vlan enable
```

Step 2 Use the **config wgb ethport** *ethport* **native-vlan** *vlan_id* command to specify the native VLAN ID.

```
Device# config wgb ethport native-vlan id 2735
```

Step 3 (Optional) Use the **show wgb ethport config** or **show running-config** command to verify your configuration.

```
Device# show wgb ethport config
```

Low latency profile

Low latency profiles are configurations that optimize IEEE 802.11 networks to meet the low latency and Quality of Service (QoS) requirements essential for IoT applications. IEEE 802.11 networks play a vital role in enabling IoT applications by providing mechanisms that reduce latency and ensure QoS. The following features are key to achieving these goals:

- Enhanced Distributed Channel Access (EDCA): EDCA parameters prioritize wireless channel access for latency-sensitive traffic, such as voice and video streams, ensuring consistent QoS performance.
- Aggregated MAC Protocol Data Unit (AMPDU): This mechanism combines multiple data frames into a single transmission, reducing overhead and improving efficiency.
- Packet Retry (Aggregated or Non-Aggregated): The retry mechanism ensures successful data delivery, either by retransmitting aggregated packets or individual packets, depending on network conditions.

These features collectively support the deployment of IoT devices and applications that demand low latency and high QoS in wireless environments.

Enable or disable an optimized-video EDCA profile

Configure an optimized low-latency profile for video use cases to improve video performance by reducing delays and enhancing the quality of service.

This task focuses on enabling or disabling the optimized-video EDCA profile on a specific radio interface of WGB. The optimized-video profile ensures better handling of video traffic by prioritizing it in the network.

Procedure

Step 1 Enable or disable the optimized-video EDCA profile on a specific radio interface of WGB using one of the options.

Option	Description
Enable optimized video EDCA profile	Use the **configure dot11Radio** *radio_slot_id* **profile optimized-video enable** command. `Device# configure dot11Radio 1 profile optimized-video enable`
Disable optimized video EDCA profile	Use the **configure dot11Radio** *radio_slot_id* **profile optimized-video disable** command. `Device# configure dot11Radio 1 profile optimized-video disable`

Step 2 (Optional) Use the **show controllers dot11Radio** *radio_slot_id* command to verify the configuration:

```
Device# show controllers dot11Radio 1
EDCA profile: optimized-video
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 4 10 11 0 0
AC_BK L 6 10 11 0 0
AC_VI L 3 4 2 94 0
AC_VO L 2 3 1 47 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Enable or disable optimized-automation EDCA profile

Enable the optimized low-latency profile for automation use cases to improve performance and efficiency in wireless network environments.

Procedure

Step 1 Enable or disable the optimized-video EDCA profile on a specific radio interface of WGB using one of the options.

Option	Description
Enable optimized-automation EDCA profile	Use the **configure dot11Radio** *radio_slot_id* **profile optimized-automation enable** command. `Device# configure dot11Radio 1 profile optimized-automation enable`
Disable optimized-automation EDCA profile	Use the **configure dot11Radio** *radio_slot_id* **profile optimized-automation disable** command. `Device# configure dot11Radio 1 profile optimized-automation disable`

Step 2 (Optional) Use the **show controllers dot11Radio** *radio_slot_id* command to verify the configuration:

```
Device# show controllers dot11Radio 1

EDCA profile: optimized-automation
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 7 10 12 0 0
AC_BK L 8 10 12 0 0
AC_VI L 7 7 3 0 0
AC_VO L 3 3 1 0 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Configure customized-wmm EDCA profile

Customize the Wi-Fi Multimedia (WMM) profile to optimize traffic queues and improve QoS for specific types of network traffic.

WMM enhances the performance of Wi-Fi networks by prioritizing traffic based on the type of data being transmitted. Configuring a customized WMM EDCA (Enhanced Distributed Channel Access) profile allows you to fine-tune the performance parameters for voice, video, background, and best-effort traffic.

Procedure

Step 1 Use the **configure dot11Radio** *radio_slot_id* **profile customized-wmm enable** command to enable the customized WMM profile.

```
Device# configure dot11Radio 1 profile customized-wmm enable
```

Step 2 Use the **configure dot11Radio** {**0**| **1**|**2**}**wmm** {**be**| **vi**| **vo**| **bk**}{**cwmin** *cwmin_num* |**cwmax** *cwmax_num* | **aifs** *aifs_num* |**txoplimit** *txoplimit_num*} command to configure customized WMM profile parameters.

```
configure dot11Radio 1 wmm vo cwmin 3
```

Parameter descriptions:

- 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)
- aifs—Arbitration Inter-Frame Spacing, <1-15> in units of slot time
- cwmin—Contention Window min, <0-15> 2^n-1, in units of slot time
- cwmax—Contention Window max, <0-15> 2^n-1, in units of slot time
- txoplimit—Transmission opportunity time, <0-255> integer number, in units of 32us

Step 3 (Optional) Disable the customized WMM profile.

Use the **configure dot11Radio** *radio_slot_id* **profile customized-wmm disable** command to disable the customized WMM profile.

```
Device#configure dot11Radio 1 profile customized-wmm disable
```

Configure EDCA parameters using Controller GUI

Configure Enhanced Distributed Channel Access (EDCA) parameters to optimize wireless channel access for voice, video, and other QoS traffic.

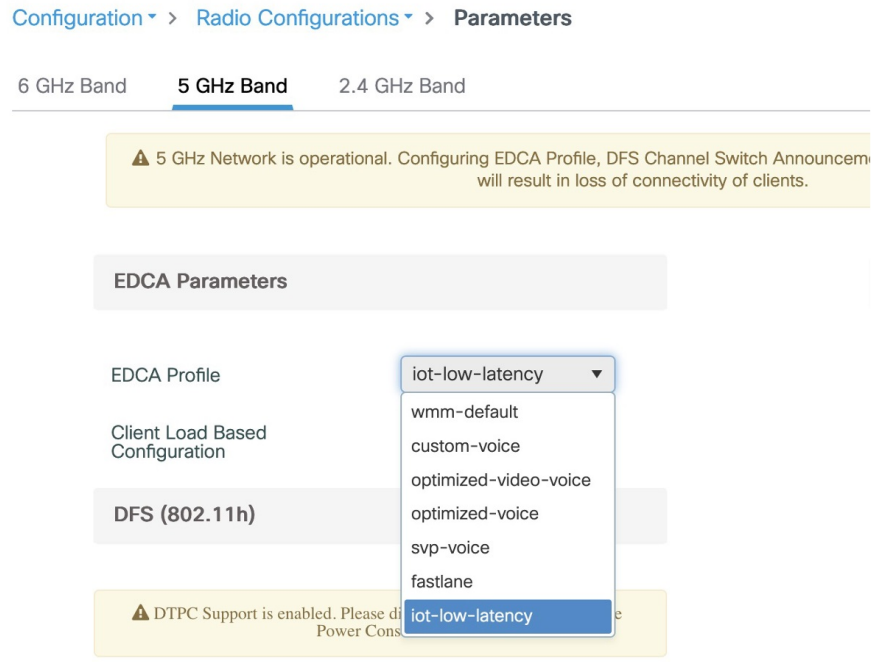
Procedure

Step 1 Navigate to **Configuration** > **Radio Configurations** > **Parameters**.

This page allows you to configure global parameters for 6 GHz, 5 GHz, and 2.4 GHz radios.

Note
You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the **Configuration > Radio Configurations > Network** page to continue.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list.



EDCA parameters provide preferential wireless channel access for voice, video, and other QoS traffic.

Step 3 Click **Apply**.

Configure EDCA parameters using Controller CLI

To optimize wireless network performance for IoT low-latency applications by adjusting Enhanced Distributed Channel Access (EDCA) parameters.

Perform these steps on the command-line interface (CLI) of a Cisco Wireless Controller.

Procedure

Step 1 Use the **configure terminal** command to enter the global configuration mode.

```
Device# configure terminal
```

Step 2 Use the **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **shutdown** command to disable the radio network.

```
Device(config)# ap dot11 5ghz shutdown
```

Step 3 Use the **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency** command to enable the iot-low-latency EDCA profile for the 5 GHz, 2.4 GHz, or 6 GHz network.

```
Device(config)# ap dot11 5ghz edca-parameters iot-low-latency
```

Step 4 Use the **no ap dot11** {**5ghz** | **24ghz** | **6ghz**} **shutdown** command to enable the radio network.

```
Device(config)# no ap dot11 5ghz shutdown
```

Step 5 Use the **end** command to return to privileged EXEC mode.

```
Device(config)# end
```

Step 6 (Optional) Use the **show ap dot11** {**5ghz** | **24ghz** | **6ghz**} **network** command to view the current configuration.

```
Device# show ap dot11 5ghz network

EDCA profile type check                  : iot-low-latency
```

A-MPDU

Aggregation is the process of grouping multiple packet data frames into a single larger frame for transmission, rather than sending them individually. This method enhances efficiency and reduces overhead in wireless communications. Two common aggregation methods are Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU parameters specifically define the size of the aggregated packet and the necessary spacing between aggregated packets, allowing the receiving WLAN station to properly decode the data.

Configure A-MPDU

Before you begin

Configure A-MPDU parameters to optimize the aggregation and transmission of packet data frames, ensuring efficient decoding by WLAN stations.

Procedure

Step 1 Use the **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** *profile-name* command to configure profile-based A-MPDU parameters.

```
Device# ap dot11 5ghz rf-profile Video-Optimized
```

Step 2 Use the **dot11n a-mpdu tx block-ack window-size** *window-size* command to configure transmission block-acknowledgment (block-ack) window size.

```
Device(config-rf-profile)# dot11n a-mpdu tx block-ack window-size 64
```

Note
RF profile level configured value takes preference over globally configured value.

Step 3 Use the **exit** command to return to global configuration mode.

```
Device(config-rf-profile)# exit
```

Step 4 Use the **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** *window-size* command to configure transmission block-acknowledgment window size globally.

```
Device(config)# ap dot11 24ghz dot11n a-mpdu tx block-ack window-size 32
```

Step 5 Use the **wireless tag rf** *rf-tag-name* command to create an RF tag.

```
Device(config)# wireless tag rf Branch-RF-Tag
```

Step 6 Use the **5ghz-rf-policy** *rf-profile-name* command to bind RF tags to RF profiles and to apply them to specific radios.

```
Device(config-wireless-rf-tag)# 5ghz-rf-policy Video-Optimized
```

Step 7 Use the **end** command to return to privileged EXEC mode.

```
Device(config-wireless-rf-tag)# end
```

Step 8 (Optional) Use the **show controllers dot11Radio** *radio_slot_id* command to show the configured A-MPDU length value.

```
Device# show controllers dot11Radio 1

Radio Aggregation Config:
=========================

TX A-MPDU Priority: 0x3f
TX A-MSDU Priority: 0x3f
TX A-MPDU Window:   0x7f
```

SNMP features

The Simple Network Management Protocol (SNMP) on WGB is a functional element that

- facilitates monitoring and management of the WGB device through the SNMP protocol,
- includes roles for information exchange (manager, agent, MIB), and
- supports network health assessment and parameter configuration.

The SNMP framework on WGB includes:

- SNMP Manager: Controls and monitors the activities of network devices using SNMP, typically implemented as a network management system (NMS).
- SNMP Agent: The software component within the managed device that maintains and reports device data.
- SNMP MIB: A collection of managed objects (variables) which can be queried or set by the SNMP manager.

SNMP process

This illustration shows the SNMP process. When an SNMP manager requests data, the agent receives the request and relays it to the subagent, which responds. The agent then sends an SNMP response packet to the manager.

Figure 2: SNMP Process



SNMP versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv2c—The community-string-based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.

- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
  - Message integrity—Ensuring that a packet has not been tampered with in transit.
  - Authentication—Determining that the message is from a valid source.
  - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

Supported SNMP MIB files

The Management Information Base (MIB) is a database containing objects that can be managed on a device. These managed objects, also called variables, can be set or read to provide information about network devices and interfaces. The objects are organized in a hierarchical structure and are grouped in collections identified by object identifiers. Access to MIBs is provided through network management protocols such as SNMP.

The MIB module provides network management information on IEEE 802.11 wireless device association management and data packet forwarding configuration and statistics.

An Object Identifier (OID) uniquely identifies a MIB object on a managed network device. The OID shows the object's location in the MIB hierarchy and provides a way to access the MIB object in a network of managed devices.

Supported OIDs

The list of objects that are supported by the SNMP Management and Information Base (MIB):

- CISCO-DOT11-ASSOCIATION-MIB OIDs are given here.

Table 5: Supported OIDs

OID Object Name	OID	OID Type	OID Description
cDot11ParentAddress	1.3.6.1.4.1.9.9.273.1.1.1	String	Provides the MAC address of the parent access point.
cDot11ActiveWirelessClients	1.3.6.1.4.1.9.9.273.1.1.2.1.1	Gauge	The device on this interface is currently associating with the number of wireless clients.
cDot11ActiveBridges	1.3.6.1.4.1.9.9.273.1.1.2.1.2	Gauge	The device on this interface is currently associating with the number of bridges.
cDot11ActiveRepeaters	1.3.6.1.4.1.9.9.273.1.1.2.1.3	Gauge	The device on the interface is currently associating with the number of repeaters.

OID Object Name	OID	OID Type	OID Description
cDot11AssStatsAssociated	1.3.6.1.4.1.9.9.273.1.1.3.1.1	Counter	When device restarts, the object counts the number of stations associated with the device on the interface.
cDot11AssStatsAuthenticated	1.3.6.1.4.1.9.9.273.1.1.3.1.2	Counter	When the device restarted, it currently counts the number of stations authenticated with the device on the interface.
cDot11AssStatsRoamedIn	1.3.6.1.4.1.9.9.273.1.1.3.1.3	Counter	When the device restarted, the object counts the number of stations roamed from another device to the device on the interface.
cDot11AssStatsRoamedAway	1.3.6.1.4.1.9.9.273.1.1.3.1.4	Counter	This object counts the number of stations roamed away from the device on the interface since device re-started.
cDot11AssStatsDeauthenticated	1.3.6.1.4.1.9.9.273.1.1.3.1.5	Counter	This object counts the number of stations deauthenticated with this device on the interface since device re-started
cDot11AssStatsDisassociated	1.3.6.1.4.1.9.9.273.1.1.3.1.6	Counter	This object counts the number of stations disassociated with this device on the interface since device re-started

OID Object Name	OID	OID Type	OID Description
cd11IfCipherMicFailClientAddress	1.3.6.1.4.1.9.9.273.1.1.4.1.1	String	This is MAC address of the client attached to the radio interface that caused the most recent MIC failure
cd11IfCipherTkipLocalMicFailures	1.3.6.1.4.1.9.9.273.1.1.4.1.2	Counter	When the device restarted, the object counts the number of MIC failures encountered on the radio interface.
cd11IfCipherTkipRemotMicFailures	1.3.6.1.4.1.9.9.273.1.1.4.1.3	Counter	When the device restarted, the object counts the number of MIC failures reported by clients on the radio interface.
cd11IfCipherTkipCounterMeasInvok	1.3.6.1.4.1.9.9.273.1.1.4.1.4	Counter	When the device restarted, the object counts the number of TKIP Counter Measures invoked on the interface.
cd11IfCipherCcmpReplaysDiscarded	1.3.6.1.4.1.9.9.273.1.1.4.1.5	Counter	When the device restarted, the object counts the number of received unicast fragments discarded by replay mechanism on the interface.
cd11IfCipherTkipReplaysDetected	1.3.6.1.4.1.9.9.273.1.1.4.1.6		When the device restarted, the object counts the number of TKIP replay errors detected on this interface.
cDot11ClientRoleClassType	1.3.6.1.4.1.9.9.273.1.2.1.1.3	Counter	The role classification of the client
cDot11ClientDevType	1.3.6.1.4.1.9.9.273.1.2.1.1.4	EnumVal	The device type of the client.

OID Object Name	OID	OID Type	OID Description
cDot11ClientRadioType	1.3.6.1.4.1.9.9.273.1.2.1.1.5	EnumVal	The radio classification of the client.
cDot11ClientWepEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.6	EnumVal	Whether WEP key mechanism is used for transmitting frames of data for the client
cDot11ClientWepKeyMixEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.7	EnumVal	Whether this client is using WEP key mixing
cDot11ClientMicEnabled	1.3.6.1.4.1.9.9.273.1.2.1.1.8	EnumVal	Whether the MIC is enabled for the client
cDot11ClientPowerSaveMode	1.3.6.1.4.1.9.9.273.1.2.1.1.9	EnumVal	The power management mode of the client.
cDot11ClientAid	1.3.6.1.4.1.9.9.273.1.2.1.1.10	Gauge	This is the association identification number of clients or multicast addresses associating with the device.
cDot11ClientDataRateSet	1.3.6.1.4.1.9.9.273.1.2.1.1.11	String	Is a set of data rates at which this client can transmit and receive data
cDot11ClientSoftwareVersion	1.3.6.1.4.1.9.9.273.1.2.1.1.12	String	Cisco IOS software version
cDot11ClientName	1.3.6.1.4.1.9.9.273.1.2.1.1.13	String	Cisco IOS device hostname
cDot11ClientAssociationState	1.3.6.1.4.1.9.9.273.1.2.1.1.14	EnumVal	The object indicates the state of the authentication and association process

OID Object Name	OID	OID Type	OID Description
cDot11ClientVlanId	1.3.6.1.4.1.9.9.273.1.2.1.1.17	Gauge	The VLAN which the wireless client is assigned to when it is successfully associated to the wireless station.
cDot11ClientSubIfIndex	1.3.6.1.4.1.9.9.273.1.2.1.1.18	Integer	This is the ifIndex of the sub-interface which this wireless client is assigned to when it is successfully associated to the wireless station.
cDot11ClientAuthenAlgorithm	1.3.6.1.4.1.9.9.273.1.2.1.1.19	EnumVal	The IEEE 802.1x authentication methods performed between the wireless station and this client during association
cDot11ClientDot1xAuthenAlgorithm	1.3.6.1.4.1.9.9.273.1.2.1.1.21	Octet String	The IEEE 802.1x authentication methods performed between the wireless client and the authentication server.
cDot11ClientUpTime	1.3.6.1.4.1.9.9.273.1.3.1.1.2	Gauge	The time in seconds that this client has been associated with this device
cDot11ClientSignalStrength	1.3.6.1.4.1.9.9.273.1.3.1.1.3	Integer	The device-dependent measure the signal strength of the most recently received packet from the client.

OID Object Name	OID	OID Type	OID Description
cDot11ClientSigQuality	1.3.6.1.4.1.9.9.273.1.3.1.1.4	Gauge	The device-dependent measure the signal quality of the most recently received packet from the client.
cDot11ClientPacketsReceived	1.3.6.1.4.1.9.9.273.1.3.1.1.6	Counter	The number of packets received from this client.
cDot11ClientBytesReceived	1.3.6.1.4.1.9.9.273.1.3.1.1.7	Counter	The number of bytes received from the client.
cDot11ClientPacketsSent	1.3.6.1.4.1.9.9.273.1.3.1.1.8	Counter	The number of packets sent to the client.
cDot11ClientBytesSent	1.3.6.1.4.1.9.9.273.1.3.1.1.9	Counter	The number of bytes sent to the client.
cDot11ClientMsduRetries	1.3.6.1.4.1.9.9.273.1.3.1.1.11	Counter	The counter increases when it successfully transmits an MSDU after one or more retransmissions.
cDot11ClientMsduFails	1.3.6.1.4.1.9.9.273.1.3.1.1.12	Counter	The counter increments when the client fails to transmit an MSDU successfully because the number of transmit attempts exceeds a certain limit.

Configure SNMP parameters

This procedure describes how to configure Simple Network Management Protocol (SNMP) on the WGB. You can enable SNMPv2c or SNMPv3 depending on your network requirements. The steps include setting community strings or usernames, defining authentication and encryption methods, and enabling SNMP functionality on the device.

- Configure all SNMP parameters before enabling the SNMP feature using the CLI command: **configure snmp enabled**.
- All SNMP configurations will be automatically removed when the SNMP feature is disabled.

Procedure

Step 1 Use the **configure snmp v2c community-id length** *length* command to enter the SNMP v2c community ID (SNMP v2c only).

```
Device#configure snmp v2c community-id 50
```

Step 2 Use the **configure snmp version** {**v2c** | **v3**} command to specify the SNMP protocol version.

```
Device# configure snmp version v3
```

Step 3 Use the **configure snmp auth-method** {**md5** | **sha**} command to specify the SNMP v3 authentication protocol (SNMP v3 only).

```
Device# configure snmp auth-method md5
```

Step 4 Use the **configure snmp v3 username length** *length* command to enter the SNMP v3 username (SNMP v3 only).

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

Step 5 Use the **configure snmp v3 password length** *length* command to enter the SNMP v3 user password (SNMP v3 only).

```
Device# configure snmp v3 password length 12
```

The valid range for *length* is 8 to 64 characters.

Step 6 Use the **configure snmp encryption** {**des** | **aes** | **none**} command to specify the SNMP v3 encryption protocol (SNMP v3 only).

```
Device#configure snmp encryption des
```

Encryption values are **des** or **aes**. Use **none** if a v3 encryption protocol is not needed.

Step 7 Use the **configure snmp secret length** *length* command to enter the SNMP v3 encryption passphrase (SNMP v3 only).

```
Device#configure snmp secret length 12
```

The valid range for *length* is 8 to 64 characters.

Step 8 Use the **configure snmp enabled** command to enable SNMP functionality on the WGB.

```
Device#configure snmp enabled
```

To configure SNMP **v2c**, repeat Step 1, Step 2 and Step 8.

To configure SNMP **v3**, repeat Step 2 through Step 8.

Step 9 (Optional) Use the **configure snmp disabled** command to disable SNMP configuration.

```
Device# configure snmp disabled
```

SNMP configuration examples

Configuring SNMP v2c:

```
Device#configure snmp v2 community-id 25
Device#configure snmp version v2c
Device#configure snmp enabled
```

Configuring SNMP v3 (security level AuthPriv):

```
Device#configure snmp auth-method md5
Device#configure snmp v3 username length 32
Device#configure snmp v3 password length 25
Device#configure snmp secret length 12
Device#configure snmp encryption aes
Device#configure snmp version v3
Device#configure snmp enabled
```

Configuring SNMP v3 (security level AuthNoPriv):

```
Device#configure snmp auth-method md5
Device#configure snmp v3 username length 32
Device#configure snmp v3 password length 32
Device#configure snmp encryption none
Device#configure snmp version v3
Device#configure snmp enabled
```

Verifying SNMP

Use the **show snmp** command to verify the SNMP configuration.

SNMP version v3

```
Device# show snmp

SNMP: enabled
Version: v3
Community ID: test
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
```

SNMP version v2c

```
Device# show snmp

SNMP: enabled
Version: v2c
Community ID: test
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
```

QoS ACL classification and marking

Quality of Service (QoS) ACL classification and marking identify network traffic using access control list (ACL) rules and assign a traffic class or priority value.

- Classification uses ACLs to match traffic flows based on parameters such as source or destination IP address, protocol type, port numbers, or other header fields. This step identifies the type of traffic being forwarded, such as voice, video, or data.

- Marking occurs after classification. Packets are tagged with specific QoS values, such as DSCP, IP precedence, or CoS, which indicate their priority level. These markings guide QoS policies such as queuing, policing, or shaping across the network..

Starting with Cisco Unified Industrial Wireless Software Release 17.14.1, you can classify packets from two wired ports and assign them to different access control driver queues based on your configuration.

In addition to TCP and UDP, the WGB supports ethertype-based and DSCP-based classification. The WGB classifies packets and assigns them to access control queues according to the field environment to meet jitter and latency requirements.

Rule-based traffic classifications

A rule-based traffic classification is a network management technique that:

- uses custom rules to classify incoming Ethernet packets by criteria such as 802.1p, DSCP, and protocol type,
- assigns classified packets to priority queues on the wireless side for QoS enforcement, and
- ensures critical services receive higher priority, reducing latency and optimizing network performance.

Rule configuration criteria

You can configure mapping rules using the following parameters:

- Ethernet type (for example, Profinet)
- Transport layer port numbers or port ranges
- DSCP values
- Source and destination IP addresses
- Protocol types

Packet classification and assignment

As incoming packets arrive at the Ethernet port, WGB applies the defined rules to:

- Identify critical services or traffic flows
- Classify packets based on predefined criteria
- Assign packets to the appropriate access control queues on the wireless network

Benefits of rule-based mapping

By using customized rule-based classification and mapping, you can:

- Enforce QoS policies effectively
- Prioritize critical applications and services
- Reduce latency for time-sensitive traffic
- Improve overall network performance and user experience

QoS and ACL traffic classification methods

Traffic classification is the process of distinguishing one type of network traffic from another by examining packet fields. It is enabled only when QoS is active. During classification, the device performs a lookup and assigns a QoS label to the packet. The QoS label defines the QoS actions to be applied and identifies the output queue for forwarding.

- Classification relies on fields across packet layers
- Packets are grouped into service classes based on Ethertype, DSCP, or TCP/UDP ports, and consistently treated within those classes.
- The data plane records rule hits for analysis, while the control plane configures data forwarding.

Layer 2 classification fields

Layer 2 Ethernet frames use the Ethertype field (2 bytes) to carry classification information. This field normally indicates the type of data encapsulated in the frames.

Layer 3 classification fields

Layer 3 IP packets carry classification information in the Type of Service (ToS) field (8 bits). It has:

- IP precedence values that range from 0–7, and
- DSCP values that range from 0–63.

Layer 4 classification fields

Layer 4 TCP segments or UDP datagrams use the source or destination port fields for classification. These port numbers allow devices to classify traffic based on applications or services.

Traffic assignment to service classes

The system assigns traffic to a specific service class based on Ethertype, DSCP, or UDP/TCP port (or port range). Packets within a service class are treated consistently. WGBs classify packets from wired ports and map them to different driver queues according to user configuration.

Data plane role in classification

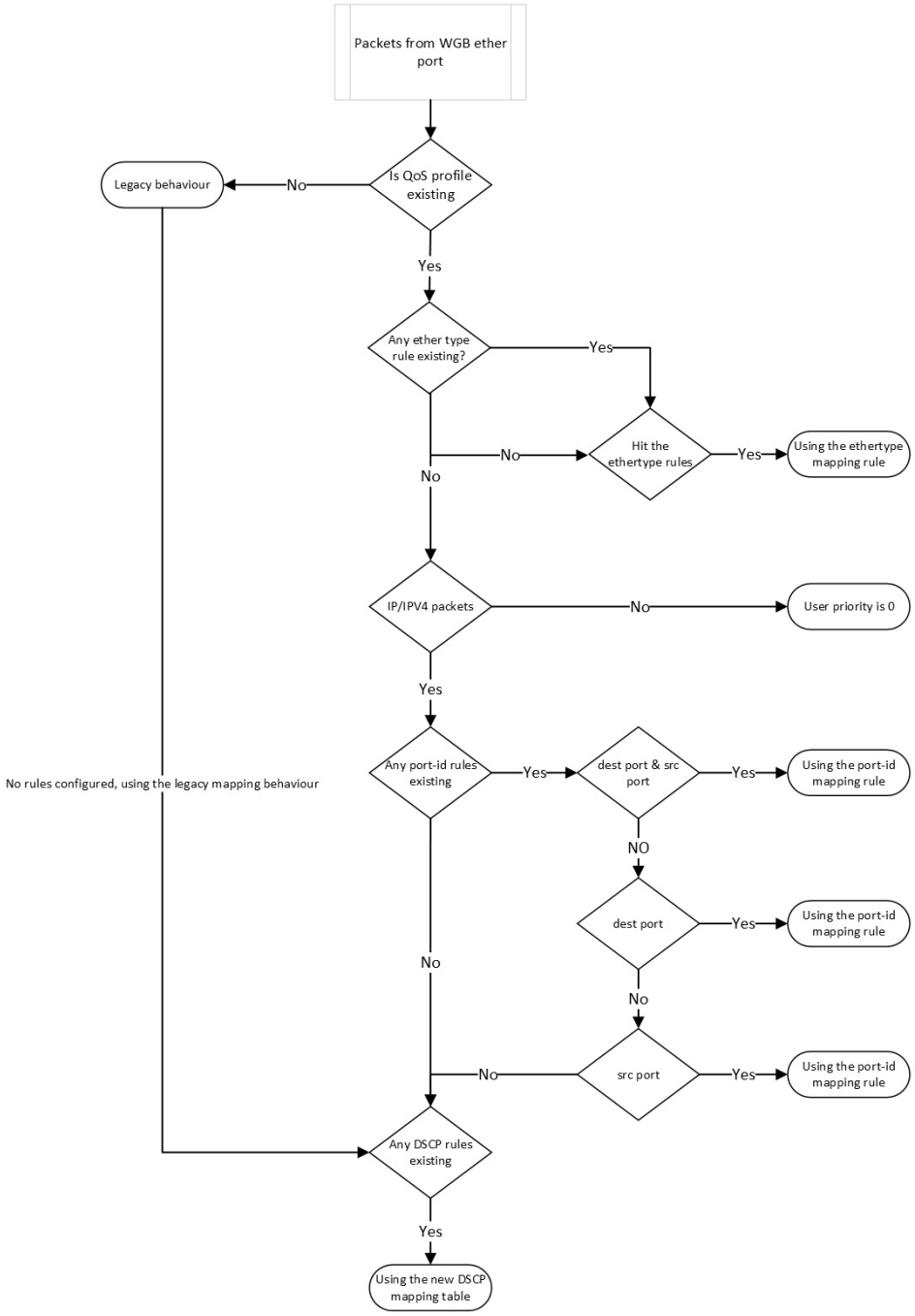
Data plane statistics provide counters showing how many times each rule is matched by traffic. These counters help administrators analyze rule effectiveness and optimize performance.

Control plane role in classification

The control plane is responsible for managing and configuring how data is forwarded through the network.

The following flowchart illustrates how packets from a WGB Ethernet port are classified and mapped to QoS rules based on existing profiles, Ethertype, port identifiers, and DSCP values.

Figure 3: Flowchart of traffic flows from WGB ethernet port



Legacy QoS mapping behavior

Summary

Access points assign traffic priority by retrieving VLAN-based TCI values, applying a fixed priority of 6 for Profinet, and using DSCP-to-dot1p mapping for IP and IPv6 traffic.

Workflow

Access points determine traffic priority based on ethertype using the following rules:

1. Retrieve TCI Priority: Access points retrieve the Tag Control Information (TCI) priority from the VLAN element for the specified ethertype 0x8100.
2. Assign TCI Priority for Profinet: For ethertype 0x8892 (profinet), access points assign the TCI priority as 6.
3. Set DSCP Priority for IP and IPv6: For ethertype 0x0800 (IP) and 0x86DD (IPv6), access points set the DSCP priority according to the default dscp2dot1p mapping table.

How Access Points assign QoS priorities

Summary

Access points assign QoS priorities based on protocol type and configured rules, with defaults applied for non-IP traffic or when no rules are set.

Workflow

Here's how the process of enabling QoS on access points works:

1. The access point determines the priority for an ethertype QoS mapping of 0x8892 (profinet) based on the configuration setting.
2. For ethertypes 0x0800 (IP) and 0x86DD (IPv6), the access point assigns priority according to mapping rules that consider either the port or DSCP:
   - The access point checks the UDP/TCP port (or port range) rule.
   - The access point checks the DSCP rule.
3. The access point assigns a user priority value of 0 to packets that are not IPv4/IPv6.
4. If no rule configuration is present, the QoS profile defaults to the legacy mapping behavior.



Note If 802.1p priority exists, it overrides any customised rule.

Configure QoS Mapping Profile

This procedure allows you to define the different classification rules for configuring WGB QoS mapping.

Procedure

Step 1 Use the **config wgb qos-mapping** *profile-name* **enable** command to enable the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile enable
```

Step 2 Use the **config wgb qos-mapping** *profile-name* **add ethtype hex** *hex-number* **priority** *priority* command to add a mapping rule based on Ethernet type.

```
Device# configure wgb qos-mapping demo-profile add ethtype hex 8892 priority 5
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule to it.

You can delete the rules based on ethernet type using the **config wgb qos-mapping** *profile-name* **delete ethtype hex** *hex-number*

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

Step 3 Use the **config wgb qos-mapping** *profile-name* **add** [**srcport** *number* | **dstport** *number* | **range** *start-number ending-number*] **priority** *priority* command to add a mapping rule based on port ID or range.

```
Device# config wgb qos-mapping voice-profile add dstport 5004 priority 6
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule.

You can delete rules based on port-id/range using the **config wgb qos-mapping** *profile-name* **delete** [**srcport** *number* | **range** *start-number ending-number* [**dstport** *number* | **range** *start-number ending-number*]]

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

Step 4 Use the **config wgb qos-mapping** *profile-name* **add dscp** *number* **priority** *priority* command to add a mapping rule based on DSCP value.

```
Device# configure wgb qos-mapping demo-profile add dscp 63 priority 4
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule.

You can delete a mapping rule based on DSCP value using the **config wgb qos-mapping** *profile-name* **delete dscp** *number* **priority** *priority* command.

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

After deleting the DSCP mapping rule, the rules are reset to the default values of the DSCP mapping.

Step 5 Use the **config wgb qos-mapping** *profile-name* **disable** command to disable the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile disable
```

When disabled, the profile is cleared from the datapath but retained in the WGB configuration file. If the profile does not exist, a warning is issued and no new profile is created.

Step 6 (Optional) Use the **config wgb qos-mapping** *profile-name* **delete** command to delete the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile delete
```

When deleted, the profile is removed from both the datapath and the WGB configuration.

Verify Quality of Service Map

To verify the QoS mapping configuration on the Control Plane, run the **show wgb qos-mapping**.

```
Device# show wgb qos-mapping

Number of QoS Mapping Profiles: 2
====================================
Profile name : qos1
Profile status : active
Number of Rules: 8
Rules:
L4 srcport : 31000-31100, dstport : 6666-7777, priority : 7
L4 srcport : 23000, dstport : N/A, priority : 3
L4 srcport : N/A, dstport : 20000-20100, priority : 5
L4 srcport : N/A, dstport : 2222, priority : 2
L4 srcport : 12300-12500, dstport : N/A, priority : 6
IPv4/IPv6 dscp: 43, priority : 1
Ethernet type : 0x8892, priority : 0
L4 srcport : 8888, dstport : 9999, priority : 4

Profile name : qos2
Profile status : inactive
Number of Rules: 8
Rules:
L4 srcport : 31000-31100, dstport : 6666-7777, priority : 2
L4 srcport : 23000, dstport : N/A, priority : 6
L4 srcport : N/A, dstport : 20000-20100, priority : 4
L4 srcport : N/A, dstport : 2222, priority : 7
L4 srcport : 12300-12500, dstport : N/A, priority : 3
IPv4/IPv6 dscp: 43, priority : 0
Ethernet type : 0x8892, priority : 1
L4 srcport : 8888, dstport : 9999, priority : 5
```

To verify the WGB QoS mapping configuration on the Data Plane, run the **show datapath qos-mapping rule**.

```
Device# show datapath qos-mapping rule

Status: active
QoS Mapping entries
======= dscp mapping =======
Default dscp2dot1p Table Value:
[0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1
[16]->2 [17]->2 [18]->2 [19]->2 [20]->2 [21]->2 [22]->2 [23]->2
[24]->3 [25]->3 [26]->3 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5
[48]->6 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7

active dscp2dot1p Table Value:
[0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1
[16]->7 [17]->2 [18]->2 [19]->2 [20]->2 [21]->2 [22]->2 [23]->2
[24]->3 [25]->3 [26]->3 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5
```

```
[48]->6 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7
```

To verify the WGB QoS mapping statistics on Data Plane, run the **show datapath qos-mapping statistics** command.

```
Device# show datapath qos-mapping statistics

======= pkt stats per dscp-mapping rule =======
dscp up pkt_cnt
16 7 0
```

To clear the WGB QoS mapping statistics on Data Plane, run the **clear datapath qos-mapping statistics** command.

Note The command clears packet count statistics per rule on data-plane.

Packet Capture: TCP dump utilities

TCP dump utilities are network packet analyzers that

- captures packets transmitted over network interfaces,
- displays and saves packet data for monitoring and troubleshooting, and
- enables in-depth analysis of wired network traffic on WGBs.

TCP Dump on WGB chapter provides information on how to enable TCP dump through the WGB wired interface on the Catalyst IW9165E.

Purpose of TCP dump utility

TCP dump on a WGB monitors and troubleshoots network communications, ensuring the WGB relays frames correctly between the wired clients and the wireless networks.

The TCP dump utility

- displays captured packets in real time on the WGB terminal, and
- capture packets to storage.

Note The TCP dump utility does not support the simultaneous capture of packets to storage and printing them on the WGB terminal.

Packet capture modes

The WGB packet capture utility supports the following modes and behaviors:

- Default: Displays captured packets with header in the real time on the WGB terminal
- Verbose: Parses and prints real-time packets on the WGB terminal, displaying the headers and prints the data of each packet, including its link-level header, in hexadecimal format.

Note Reformat the verbose output for text2pcap compatibility.

In default or verbose mode, the WGB terminal can print a maximum of 1000 packet entries.

- Capture: Captures packets to a file storage instead of printing them in real time. Use the **show pcap** command to view the captured internal wired packets.

Note Every round of Packet Capture (PCAP) clears the existing PCAP file.

Before any new PCAP session, transfer the current PCAP file to an external server to prevent it from being overwritten.

PCAP stops automatically when the PCAP file reaches a size of 100 MB.

Protocol packet capture capabilities

You can capture packets from an AP either using a default or custom filter through the WGB wired port and then upload them to an external server.

The default filter captures three main protocol packets such as IP, TCP, or UDP.

A custom filter captures specific packets that are relevant for troubleshooting specific issues or monitoring certain types of network activity.

You can use different protocol filters to capture packets for debugging. For instance, include the given protocols in your filter expression:

- Transmission Control Protocol, Internet Control Message Protocol (ICMP) and ICMPv6
- Profinet with IP proto 0x8892
- Address Resolution Protocol (ARP)
- Internet Group Management Protocol (IGMP)
- User Datagram Protocol
- Dynamic Host Configuration Protocol (DHCP) with port 67 or port 68 and DHCPv6 with port 546 or port 547
- Common Industrial Protocol (CIP) with TCP port 44818
- Domain Name System (DNS) with port 53
- Simple Network Management Protocol with port 161 or port 162.

Note The protocols listed represent only a portion of the PCAP capabilities.

Filter expressions for packet captures

The filter expression for a PCAP comprises at least one primitive. Primitives usually consist of qualifiers followed by an identifier. The identifier can be a name or a number.

There are three kinds of qualifiers.

- Type: Specifies the type of the identifier. The type can be a port, a host, a network, or a range of ports.

  For example: port 20

- Dir: Specifies that the capture is for only packets with a given transfer direction.

  For example: src x.x.x.x and port ftp-data or dst x.x.x.x and port ftp

- Proto: Limits the capture to a specific protocol.

  For example: tcp port 21.

The filter expressions can be combined using the logical operators AND, OR, and NOT to create more specific and complex filters.

Note When constructing filter expressions, it is important to understand the order of operations and use parentheses to group expressions when necessary to ensure the correct interpretation.

Enable wired packet captures

This procedure enables packet capture (PCAP) on a WGB to monitor wired traffic. It allows you to capture packets by protocol (IP, TCP, UDP), apply verbose output for detailed analysis, save packet data to PCAP files, and use custom filters (including VLAN) to analyze specific traffic across native and non-native VLANs.

Procedure

Step 1 Enable PCAP using one of the options given here:

Option	Description

Run PCAP with the default filter	Use the **debug traffic wired** [**0**| **1**]{**ip**	**tcp**	**udp**}[**verbose**	**capture]** command.
				`Device# configure wgb mobile station interface dot11Radio 1 dot11v-bss-transition enable`
				[**0**| **1**] specifies the wired interface number. If not selected, capture packets from all the wired interface.
				`Device# debug traffic wired 1 ip`
				`APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)`
				`1 08:35:50.529851 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 13721, seq 1, length 64`
				`2 08:35:50.534813 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 13721, seq 1, length 64`
				This option is the default and captures packets with IP protocol headers.
				`Device# debug traffic wired 1 udp verbose`

Option	Description
	APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:25:59.696990 IP6 fe80::322c:712c:5787:f246.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit 0x0000: 3333 0001 0002 fc58 9a16 e428 86dd 6001 0x0010: 7b92 006d 1101 fe80 0000 0000 0000 322c 0x0020: 712c 5787 f246 ff02 0000 0000 0000 0000 0x0030: 0000 0001 0002 0222 0223 006d 00a6 010c 0x0040: d064 0008 0002 ffff 0006 001e 0034 0011 0x0050: 0015 0016 0017 0018 001f 0038 0040 0043 0x0060: 0052 0053 005e 005f 0060 0001 000a 0003 0x0070: 0001 fc58 9a16 e428 0014 0000 0027 0013 0x0080: 0006 4150 4643 3538 0439 4131 3604 4534 0x0090: 3238 0000 0300 0c00 0000 0100 0000 0000 0x00a0: 0000 00 The verbose option captures detailed information from UDP protocol packets. Device# debug traffic wired 1 tcp capture % Writing packets to "/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
Run PCAP with the custom filter	Use the **debug traffic wired** [**0**| **1**] **filter** *expression* [**verbose** | **capture]** command. Enable only one PCAP process at a time. Do not use unsupported characters like " ` $ ^ & | \ > < ? ; and ~ in the filter expressions. Device# debug traffic wired 0 filter icmp APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 10:38:59.948729 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 16204, seq 1, length 64 2 10:38:59.954308 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 16204, seq 1, length 64 This option is the default and captures packets with IP protocol headers. Device# debug traffic wired 1 filter icmp verbose APXXXX.XXXX.XXXX##reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 17:13:30.706493 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 986, seq 1, length 64 0x0000: fc58 9a17 afd4 f8e4 3b9d 7322 0800 4500 0x0010: 0054 57a0 4000 4001 889e c0a8 6cc8 c0a8 0x0020: 6c51 0800 940c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637 17:13:30.710567 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 986, seq 1, length 64 0x0000: f8e4 3b9d 7322 fc58 9a17 afd4 0800 4500 0x0010: 0054 9102 0000 4001 8f3c c0a8 6c51 c0a8 0x0020: 6cc8 0000 9c0c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637

Option	Description

	The verbose option captures detailed information from UDP protocol packets.
	`Device# debug traffic wired 1 filter icmp capture`
	`% Writing packets to "/tmp/pcap/APXXXX.XXXX.XXXX_capture.pcap0"`
	`APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)`
	The capture option saves TCP packet information to a PCAP file.

Run PCAP in multiple VLANs using custom filter	Use the **debug traffic wired** [**0**| **1**][**filter** *expression* |**ip** } command.
	Note
	Some custom filters miss traffic in non-native VLANs. For example, the custom filter command **debug traffic wired 0 filter icmp** fails to capture downlink ICMP traffic in non-native VLANs
	`Device#debug traffic wired 0 filter "icmp or (vlan and icmp)"`
	`1 12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64`
	`2 12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1, length 64`
	Add VLAN to the filter expression to capture bidirectional traffic from a wired client on a non-native VLAN.
	`Device#debug traffic wired 0 ip`
	`1 12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64`
	`2 12`
	Use the default IP filter to capture all IP traffic, including native and non-native VLANs.

Step 2 To upload the packets to an external server, use the command given here: Use the **copy pcap** *file-name.pcap0* {**tftp**| **sftp**}*://server-ip* [*directory*][*file-name*] command to upload the packets to an external server.

```
Device# copy pcap APXXXX.XXXX.XXXX_capture.pcap0 scp://iot@209.165.200.213:/capture/wgb_sniffer.pcap
copy ""/pcap/APXXXX.XXXX.XXXX_capture.pcap0"" to
"scp://iot@209.165.200.213:/capture/wgb_dhcp_sniffer_0_46_29.pcap" (Y/N)Y
iot@209.165.200.213 password:
APXXXX.XXXX.XXXX_capture.pcap0 0% 0 0.0KB/s --:-- ETA
APXXXX.XXXX.XXXX_capture.pcap0 100% 2530 916.5KB/s 00:00
```

Note
Complete the PCAP process and save the packets to a file before uploading. Use a TFTP, SFTP, or SCP server to transfer the PCAP file to an external server.

Disable wired packet captures

Procedure

Step 1 Use the **no debug traffic wired** [*0-3*]{**ip** | **tcp** | **udp**}[**verbose** | **capture**] command to disable PCAP with the default filter.

```
Device# no debug traffic wired 1 ip verbose
```

Step 2 Use the **no debug traffic wired** [*0-3*]**filter** *expression* [**verbose** | **capture**] command to disable PCAP with the custom filter.

```
Device# no debug traffic wired 0 filter "icmp or (vlan and icmp)" capture
```

Note
You can also use the **no debug** or **undebug all** command to terminate the capture process.

Verify wired packet capture

- To verify the debug status, use the **show debug** command.

```
Device#show debug
traffic:
  wired tcp debugging is enabled
```

- To view the captured internal wired packets stored in the file, use the **show pcap** command.

Note After capturing packets to the file, use the **show pcap** command to view them.

```
Device#show pcap
reading from file /pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type EN10MB (Ethernet)
1  00:00:00.000000 IP 0.0.0.0 > 224.0.0.1: igmp query v2
2  09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920, seq
 1, length 64
3  09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920, seq
1, length 64
4  09:41:49.904914 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 29920, seq
 2, length 64
5  09:41:49.909009 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 29920, seq
2, length 64
```

- To filter and view the basic content of captured packets sequentially, run the **show pcap [filter** *expression***]** command.

```
Device#show pcap filter "src 209.165.200.189”
reading from file /pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type EN10MB (Ethernet)
 1  09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920,
seq 1, length 64
 2  09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920, seq
 1, length 64
```

- To filter and view the detailed content of a specific packet, run the **show pcap [filter** *expression***][detail** *no***]** command.

```
Device#show pcap filter "src 209.165.200.189" detail 2
2024-04-25 09:41:49.904914
000000 18 59 f5 96 af 74 00 50 56 85 8a 0a 08 00 45 00
000010 00 54 14 6c 40 00 40 01 b7 9d 64 16 53 72 64 16
000020 53 01 08 00 70 81 74 e0 00 02 d4 3e 2b 66 00 00
000030 00 00 50 24 04 00 00 00 00 00 10 11 12 13 14 15
000040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
000050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
000060 36 37
```

Port address translation

Port Address Translation (PAT), also known as Network Address and Port Translation (NAPT), is a network address translation method that:

- translates multiple internal wired client private IP addresses and port numbers
- to unique public IP addresses and port numbers
- before sending packets to the external network.

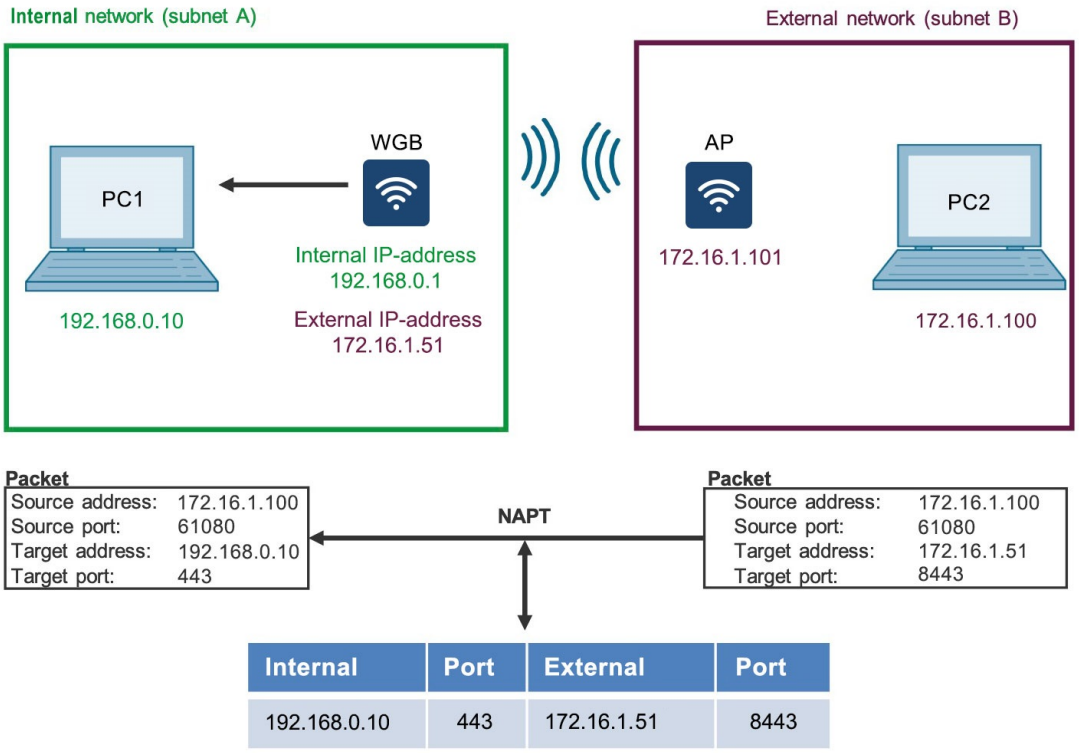
A private IP address is used only within an internal network. A public IP address is globally unique and used on the Internet. NAPT mapping uses both the IP address and the port number. This allows packets from multiple internal hosts to map to the same external IP address with different port numbers. This enables client devices within the internal local subnet to reuse the same IP addresses across different Automated Guided Vehicles (AGVs).

From Release 17.16.1, PAT is supported on the IW9165E Workgroup Bridge (WGB) Access Points (APs) of each AGV.

Note Profinet clients on the AGV must be configured with a unique IP address that belongs to the global subnet.

This image illustrates the concept of Network Address Port Translation (NAPT), demonstrating how a Wireless Gateway Bridge (WGB) translates incoming packets from an external network to an internal host by mapping external IP addresses and ports to internal ones.

Figure 4: NAPT Translation Between Internal and External Networks



Supported protocol

NAPT supports TCP and UDP for communication between devices on the internal and external networks.

Limitations for WGB

- NAT is not supported for incoming packets with an 802.1Q VLAN tag behind the device.
- Multicast traffic is not supported for NAT inside wired clients.
- FTP traffic is supported in active mode. In passive mode, FTP traffic is supported only when the FTP server is located within the NAT inside.
- The TFTP protocol is supported only when the TFTP server resides inside the NAT.
- Application Layer Gateway (ALG) is not supported.

Limitations for uWGB

- Access Control Lists (ACLs) are not supported.
- The NAPT supports only one private LAN as the NAPT inside network.

NAPT rules and mapping tables

A NAPT rule and mapping table is a network translation mechanism that:

- defines how a Workgroup Bridge (WGB) translates internal private addresses and ports to an external, routable address and port,
- maintains a table that maps internal device traffic to corresponding global IP/port pairs, and
- supports both TCP and UDP protocols for address and port translation.

The configuration supports a maximum of 256 IP NAT rules on WGB.

NAPT mapping table

The mapping table is created and managed based on the traffic and NAPT rules.

NAPT uses entries containing the source IP address, source port number, protocol type, destination IP address, and destination port number (TCP or UDP). These entries enable the system to translate addresses, filter packets, and index the NAPT mapping table.

Note The maximum number of mapping entries in NAPT translation table is 4096.

This table shows an example of a NAPT mapping.

Table 6: NAPT Mapping Table

Protocol	Internal Local IP Address and Port	WGB Global IP Address	External Global IP Address and Port
TCP	192.168.0.10: 80	172.16.100.11	172.16.100.11: 61080

Upstream and downstream data flows

Upstream and downstream data flows are types of network traffic flows that:

- use Network Address and Port Translation (NAPT) to translate source or destination addresses,
- allow secure transfer of data between internal and external networks, and
- maintain privacy and integrity of IP addresses.

Downstream data flow using NAPT

Downstream data flow refers to the flow of data from the external network to the AGV's internal network. The gateway (WGB or uWGB) manages communication between the external and internal networks..

When packets arrive with an external IP address and port number, the mapping table is checked to identify the corresponding internal destination.

The packets are then translated and forwarded to the internal network based on the destination IP address and port number.

The diagram illustrates how address and port translation manages both upstream (internal-to-external) and downstream (external-to-internal) traffic flows between private LAN clients and external networks.

Figure 5: Upstream and downstream data flow using NAPT in WGB

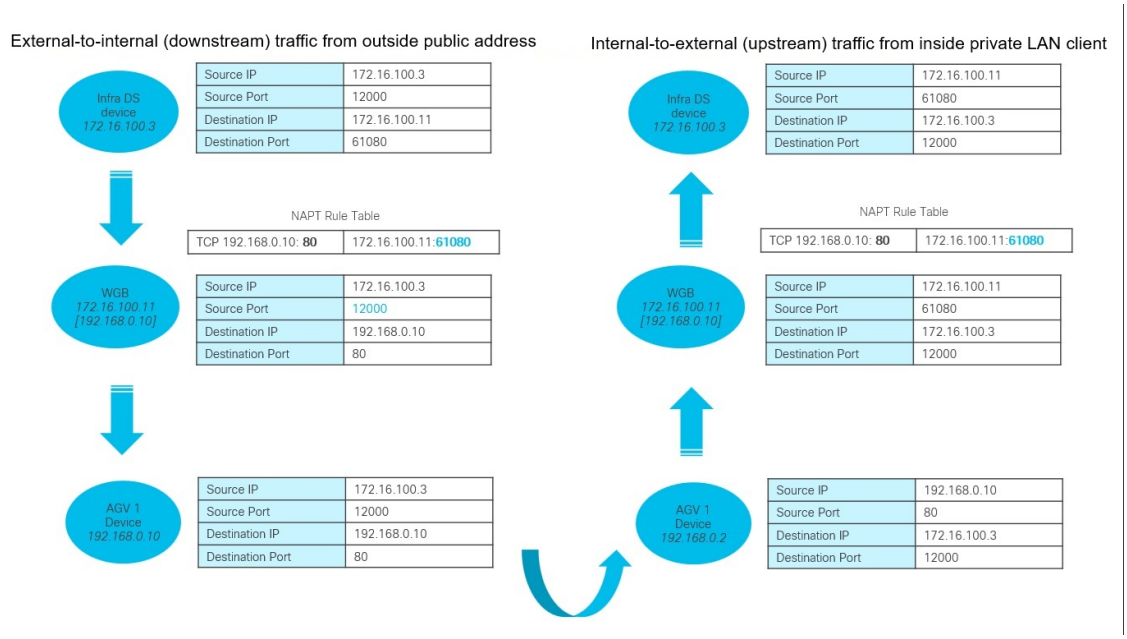
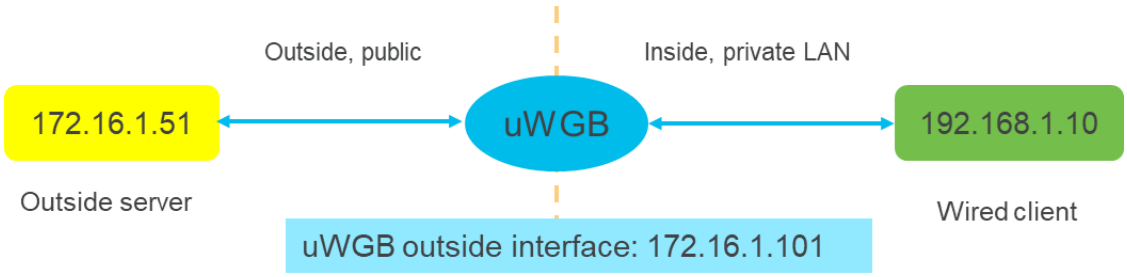


Figure 6: Upstream and downstream data flow using NAPT in uWGB



Upstream data flow using SNAT

Upstream data flow refers to the transfer of packets from internal networks to external networks. The gateway enables communication between the two networks.

All outgoing packets from the internal network are translated to the external network using Source Network Address Translation (SNAT).

For upstream traffic, SNAT replaces the source IP address and port numbers with the gateway's IP address, ensuring that internal IP addresses are not exposed to the external network.

Configure NAPT on WGB

This procedure describes how to configure Source Network Address Translation (SNAT) for upstream data flow and Network Address and Port Translation (NAPT) for downstream data flow.

Complete Steps 1 to 3 to configure upstream data flow using SNAT.

Complete Steps 4 and 5 to configure downstream data flow using NAPT.

Procedure

Step 1 Use the **configure ip nat enable** command to enable NAPT.

```
Device#configure ip nat enable
```

Use the **configure ip nat disable** command to disable the NAPT.

Step 2 Use the **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* command to configure inside IPv4 address and netmask.

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

Step 3 (Optional) Use the **configure ip nat inside port range** *min-port-number max-port-number* command to configure SNAT port range for upstream data flow.

```
Device# configure ip nat inside port range 32000 33000
```

The valid range is 1–65535. The default range is 30000–59999.

Note
Ensure that the SNAT port range and the NAPT port range do not overlap.

Step 4 Use the **configure ip nat outside port range** *min-port-number max-port-number* command to configure NAPT port range for downstream data flow.

```
Device# configure ip nat outside port range 34000 62000
```

The valid range for outside port numbers is 1025–65535. Do not use reserved ports 1233, 1234, or 20000.

Note
Ensure the NAPT and SNAT port ranges do not overlap.

Step 5 Use the **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command to configure the NAPT mapping rule for downstream data flow.

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address is the internal wired client network IP address.

inside-port-number is the internal wired client network TCP or UDP port number.

Outside port number must be within the configured NAPT range.

Step 6 (Optional) Use the **show ip nat configuration** command to view the current NAPT configuration.

```
Device# show ip nat configuration

IP NAT Configuration are:
===================================
Status: enabled
inside interface ip/netmask: 192.168.0.1/255.255.255.0
SNAT port range: 10000 - 20000
NAPT port range: 61000 - 65535
The number of ip nat rules: 1
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61080           192.168.0.10       80             tcp
```

Step 7 (Optional) Use the **show ip nat tranlations** command to view the current NAPT translation entries from the NAPT rule table.

```
Device# show ip nat translations
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.0.10, 41278, 172.16.1.51, 22000) => (172.16.1.101, 30004, 172.16.1.51, 22000) [forward] exp:
 290
(172.16.1.51, 22000, 172.16.1.101, 61080) => (172.16.1.51, 22000, 192.168.0.10, 41278) [reverse] exp:
 290
===================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.0.10, 80, 172.16.100.3, 443) => (172.16.100.11, 30000, 172.16.100.3, 443) [forward] exp:
138
(172.16.100.3, 443, 172.16.100.11, 30000) => (172.16.100.3, 443, 192.168.0.10, 80) [reverse] exp:
138
```

In the output, 'forward' refers to the log details of data packets processed by the WGB, including the source, destination, and translation information.

'Reverse' refers to the log details of return traffic, ensuring that responses from the destination reach the original source by reversing the traffic direction. It ensures the response from the destination correctly reaches back to the source by reversing the direction of the original traffic.

Manage uWGB in NAPT deployment

Follow this procedure to manage uWGB in a NAPT deployment.

Before you begin

Ensure that all uWGB wired clients are in the private LAN.

Procedure

Step 1 Use the **configure dot11Radio 1 mode uwgb** *mac_address* **ssid-profile** *test_ssid* command to configure radio mode to uWGB.

```
Device# configure dot11Radio 1 mode uwgb FC:58:9A:17:0D:52 ssid-profile testssid
```

You can choose any unique MAC address, or use the optional method given below to calculate a unique MAC address.

Note
Ensure that the MAC address does not conflict with existing devices on the network to prevent connectivity issues.

To calculate the unique MAC address, add the offset value 0x12 to the base MAC address.

To find the base MAC address, use the **show controllers dot11Radio** *interface* command, as shown in Step 2.

Use the formula: base MAC address + offset = unique MAC address.

Note
Verify that the offset value is 0x12 or greater. For example, adding 0x12 to FC:58:9A:17:0D:40 results in FC:58:9A:17:0D:52.

Step 2 (Optional) Use the **show controllers dot11Radio 1** command to find the base MAC address.

```
Device#show controllers dot11Radio 1
wifi1     Link encap:Ethernet  HWaddr FC:58:9A:17:0D:40
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9109 errors:70 dropped:59043 overruns:0 frame:0
          TX packets:27920 errors:13 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:2699
          RX bytes:913806 (892.3 KiB)  TX bytes:5399794 (5.1 MiB)
```

Step 3 (Optional) Use the **show wgb dot11 associations** command to verify the uWGB is in the WGB state.

```
Device#show wgb dot11 associations
Uplink Radio ID            : 1
Uplink Radio MAC           : FC:58:9A:17:0D:52
SSID Name                  : SSID_NAME
Connected Duration         : 56 hours, 37 minutes, 11 seconds
Parent AP MAC              : B0:B8:67:3D:5E:D6
Uplink State               : CONNECTED
Auth Type                  : PSK
Key management Type        : WPA2
Uclient mac                : FC:58:9A:17:0D:52
Current state              : WGB
Uclient timeout            : 60 Sec
Dot11 type                 : 11ac
Channel                    : 157
Bandwidth                  : 20 MHz
Current Datarate (Tx/Rx)   : 156/144 Mbps
Max Datarate               : 156 Mbps
RSSI                       : 35
IP                         : 172.16.1.101/24
Default Gateway            : 172.16.1.1
IPV6                       : ::/128
Assoc timeout              : 100 Msec
Auth timeout               : 100 Msec
Dhcp timeout               : 60 Sec'
```

Step 4 Configure NAPT to enable end-to-end traffic flow for uWGB wired clients.

Configure NAPT on uWGB

This procedure describes how to configure Source Network Address Translation (SNAT) for upstream data flow and Network Address and Port Translation (NAPT) for downstream data flow.

Follow Step 1 through Step 4 to configure support for upstream data flow using SNAT.

Follow Step 5 and Step 6 to to configure support for downstream data flow using NAPT.

Procedure

Step 1 Use the **configure ip nat enable** command to enable NAPT.

```
Device#configure ip nat enable
```

Note
Use the **configure ip nat disable** command to disable the NAPT.

Step 2 (Optional) Use the **configure ip nat inside port range** *min-port-number max-port-number* command to configure SNAT port range for upstream data flow.

```
Device# configure ip nat inside port range 32000 33000
```

The valid range is 1025–65535. The default range is 30000–59999.

Note
The SNAT port range is the source port that the uWGB uses when sending traffic from internal network to the external network.

Ensure that the SNAT port range and the NAPT port range do not overlap.

Step 3 Use the **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* command to configure the gateway IPv4 address for the internal wired client on the uWGB.

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

Step 4 Use the **configure interface nat-outside address ipv4 static** *static-ip-address static-netmask gateway-ip-address* command to configure external IPv4 address on the uWGB.

```
Device# configure interface nat-outside address ipv4 static 172.16.1.101 255.255.255.0 172.16.1.1
```

static-ip-address is the uWGB own public address

gateway-ip-address is the uWGB external IP address.

The outside port number is automatically generated for upstream data flow.

The configuration supports the internal-to-external traffic flow.

Step 5 Use the **configure ip nat outside port range** *min-port-number max-port-number* command to configure NAPT port range on the uWGB to receive traffic from the external network to the internal network.

```
Device# configure ip nat outside port range 34000 62000
```

The valid range for outside port numbers is 1025–65535. Do not use reserved ports 1233, 1234, or 20000.

Note
Ensure the NAPT and SNAT port ranges do not overlap.

Step 6 Use the **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command to configure the NAPT mapping rule for downstream data flow.

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address is the internal wired client network IP address.

inside-port-number is the internal wired client network TCP or UDP port number.

Outside port number must be within the configured NAPT range.

Step 7 (Optional) Use the **show ip nat configuration** command to view the current NAPT configuration.

```
Device# show ip nat configuration

IP NAT Configuration are:
===================================
Status: enabled
inside interface ip/netmask: 192.168.1.1/255.255.255.0
SNAT port range: 30000 - 59999
NAPT port range: 60000 - 65000
outside proxy ip/netmask/gateway: 172.16.1.101/255.255.255.0/172.16.1.1
The number of ip nat rules: 2
```

```
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61001           192.168.1.10       20001          udp
1        61002           192.168.1.10       20002          tcp
```

Step 8 (Optional) Use the **show ip nat tranlations** command to view the current NAPT translation entries from the NAPT rule table.

```
Device#show ip nat translations

ICMP:
    src_ip    dst_ip    port     =>       src_ip    dst_ip    port      direction    expiry_time
(172.16.1.1, 172.16.1.101, 30257) => (172.16.1.1, 192.168.1.10, 267) [reverse] exp: 272
(192.168.1.10, 172.16.1.1, 11) => (172.16.1.101, 172.16.1.1, 30001) [forward] exp: 272
====================================
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.1.10, 20000, 172.16.1.51, 35200) => (172.16.1.101, 61001, 172.16.1.51, 35200) [reverse] exp:
 214
(192.168.1.10, 51184, 172.16.1.51, 22000) => (172.16.1.101, 30001, 172.16.1.51, 22000) [forward] exp:
 161
(172.16.1.51, 35200, 172.16.1.101, 61001) => (172.16.1.51, 35200, 192.168.1.10, 20000) [forward] exp:
 214
(172.16.1.51, 22000, 172.16.1.101, 30001) => (172.16.1.51, 22000, 192.168.1.10, 51184) [reverse] exp:
 161
====================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.1.10, 44155, 172.16.1.51, 23000) => (172.16.1.101, 30002, 172.16.1.51, 23000) [forward] exp:
 238
(172.16.1.51, 23000, 172.16.1.101, 30002) => (172.16.1.51, 23000, 192.168.1.10, 44155) [reverse] exp:
 238
====================================
```

In the output, 'forward' refers to the log details of data packets processed by the uWGB, including the source, destination, and translation information.

'Reverse' refers to the log details of return traffic, ensuring that responses from the destination reach the original source by reversing the traffic direction. It ensures the response from the destination correctly reaches back to the source by reversing the direction of the original traffic.

Delete NAPT mapping rule

This procedure describes how to delete NAPT configuration entries. You can remove a specific NAPT mapping rule by specifying the inside and outside parameters. You can also delete a rule by its rule ID or clear all NAPT rules from the configuration. Choose the method based on whether you want to remove a specific rule or reset the entire NAPT configuration.

Procedure

Delete NAPT mapping rule using one of the options given here:

Option	Description
Delete a NAPT mapping rule	Use the **configure ip nat rule delete inside ip** *inside- ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command. `Device#configure ip nat rule delete inside ip 192.168.1.10 port 80 outside port 61080 protocol tcp`
Delete the NAPT mapping rule as per the rule-id	Use the **configure ip nat entry delete** *rule-id* command. `Device# configure ip nat entry del 0` **Note** You can use the **show ip nat configuration** command to view the rule-id.
Delete all the NAPT mapping rules	Use the **configure ip nat entry delete all** command. `Device# configure ip nat entry delete all`

Delete NAPT IP address

This procedure explains how to delete the configured NAT IP addresses. You can remove the gateway IPv4 address assigned to the internal wired client. Alternatively, you can delete the external IPv4 address configured on the NAT outside interface.

Note To remove all the NAPT configuration, you should also delete the IP address and interface.

Procedure

Delete the NAPT IP address using one of the options given here:

Option	Description
Delete gateway IPv4 address for the internal wired client	Use the **configure ip nat address delete** command. `Device#configure ip nat address delete`
Delete the external IPv4 address	Use the **configure interface nat-outside address delete** command. `Device#configure interface nat-outside address delete`

AAA user authentications

AAA user authentication is a network management mechanism that:

- controls access to network resources through user authentication,
- assigns differentiated privilege levels to users, and
- manages usernames and passwords centrally on the AAA server.

From Release 17.15.1, AAA-based user management and authentication are supported on IW9165E WGB.

The AAA server assigns privilege levels (0–15) via Authorization-Reply messages. Only levels 1 (view user) and 15 (management user) are supported. Levels 2–14 are reserved and must not be assigned.

If a user is added without a privilege level, WGB will assign the lowest privilege level to that user.

Features of AAA-based user management and authentication

AAA-based user management and authentication includes these features:

- Provides multiple-user support
- Stores usernames and passwords on the AAA server
- Authenticates users with AAA
- Supports differentiated user privileges
- Restricts CLI access based on user privileges



Note Similar to a Cisco Router or Switch, the Workgroup Bridge (WGB) can also create and store usernames and passwords locally.

Configure AAA Server

Before you begin

- You can add a secondary AAA server (RADIUS or TACACS+) before adding a primary AAA server. Once the primary AAA server is added, clients connect to the primary AAA server.
- When both primary and secondary RADIUS servers are configured, the WGB attempts to connect with the primary RADIUS server three times before switching to the secondary RADIUS server.
- For the TACACS+ server, the connection attempt is done only once with the primary TACACS+ server. If the primary TACACS+ server fails to respond, the secondary TACACS+ server is used.



Note The WGB AAA RADIUS server configuration command is officially supported starting from the 17.15.1 release.

If you downgrade the image from release 17.15.1 or later to 17.14.1 or earlier, or upgrade from 17.14.1 or earlier to 17.15.1 or later, the configured RADIUS server port resets to zero. Reconfigure the RADIUS server port.

Procedure

Add or remove a AAA server (RADIUS or TACACS+).

Option	Description
Configure a AAA server	Use the **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**} **add** {**ipv4** | **ipv6**} *ip-address* **port** *port-number* **secret** *secret-string* command. `Device# configure radius authentication primary add ipv4 10.10.10.5 port 100 secret radiusSecret123` **Note** Do not use unsupported characters in secret-string parameters. These characters include the vertical bar (|), semicolon (;), dollar sign ($), less than (<), greater than (>), ampersand (&), caret (^), grave accent (`), backslash (), carriage return (\r), and double quotation marks (“”).
Remove a AAA server	Use the **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**} **delete** command. `Device# configure radius authentication primary delete`

Enable or disable RADIUS authentication for login user

Procedure

Step 1 Enable or disable AAA RADIUS authentication for the login user using one of the options.

Option	Description
Enable AAA RADIUS authentication for the login user	Use the **config ap management aaa radius enable** command. `Device# config ap management aaa radius enable`
Disable AAA RADIUS authentication for the login user	Use the **config ap management aaa radius disable** command. `Device# config ap management aaa radius disable`

Step 2 (Optional) Use the **show running-config | include aaa** command to verify the AAA server (RADIUS or TACACS+) configuration.

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
```

.

Enable or disable TACACS+ authentication for login user

Procedure

Step 1 Enable or disable AAA RADIUS authentication for the login user using one of the options.

Option	Description
Enable AAA TACACS+ authentication for the login user	Use the **config ap management aaa tacplus enable** command. `Device# config ap management aaa tacplus enable`
Disable AAA TACACS+ authentication for the login user	Use the **config ap management aaa tacplus disable** command. `Device# config ap management aaa tacplus disable`

Step 2 (Optional) Use the **show running-config | include aaa** command to verify the AAA server (TACACS+) configuration.

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

AAA authentication configuration example

When AAA RADIUS authentication is enabled, using the show running-config command generates this sample output.

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
.
```

When AAA TACACS+ authentication is enabled, using the show running-config command generates this sample output.

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

Verification and monitoring

Verify the WGB and uWGB configuration

Perform these tasks to verify WGB and uWGB related show configurations.

Procedure

Step 1 Check whether the AP is in WGB or uWGB mode using one of the options.

Option	Description

WGB	Use the **show run** command.
	`Device#show run`
	`AP Name : APFC58.9A15.C808`
	`AP Mode : WorkGroupBridge`
	`CDP State : Enabled`
	`Watchdog monitoring : Enabled`
	`SSH State : Disabled`
	`AP Username : admin`
	`Session Timeout : 300`
	
	`Radio and WLAN-Profile mapping:-`
	`==========`
	`Radio ID Radio Mode SSID-Profile SSID`
	`Authentication`
	`----------`
	`1 WGB myssid demo`
	`OPEN`
	
	`Radio configurations:-`
	`==========`
	`Radio Id : NA`
	`Admin state : NA`
	`Mode : NA`
	`Radio Id : 1`
	`Admin state : DISABLED`

Option	Description
	Mode : **WGB** Dot11 type : 11ax Radio Id : NA Admin state : NA Mode : NA
uWGB	Use the **show run** command. Device#show run AP Name : APFC58.9A15.C808 AP Mode : WorkGroupBridge CDP State : Enabled Watchdog monitoring : Enabled SSH State : Disabled AP Username : admin Session Timeout : 300 Radio and WLAN-Profile mapping:- ========== Radio ID Radio Mode SSID-Profile SSID Authentication --- 1 UWGB myssid demo OPEN Radio configurations:- ========== Radio Id : NA Admin state : NA Mode : NA Radio Id : 1 Admin state : DISABLED Mode : **UWGB** Uclient mac : 0009.0001.0001 Current state : WGB UClient timeout : 0 Sec Dot11 type : 11ax Radio Id : NA Admin state : NA Mode : NA

Step 2 Check information about wireless clients associated with the WGB or uWGB using one of the options.

Option	Description
WGB	Use the **show wgb dot11 associations** command. Device#show wgb dot11 associations Uplink Radio ID : 1 Uplink Radio MAC : 00:99:9A:15:B4:91 SSID Name : roam-m44-open Parent AP Name : APFC58.9A15.C964 Parent AP MAC : 00:99:9A:15:DE:4C Uplink State : CONNECTED Auth Type : OPEN Dot11 type : 11ax Channel : 100 Bandwidth : 20 MHz

Option	Description
	Current Datarate (Tx/Rx) : 86/86 Mbps Max Datarate : 143 Mbps RSSI : 53 IP : 192.168.1.101/24 Default Gateway : 192.168.1.1 IPV6 : ::/128 Assoc timeout : 100 Msec Auth timeout : 100 Msec Dhcp timeout : 60 Sec
uWGB	Use the **show wgb dot11 associations** command. Device#show wgb dot11 associations Uplink Radio ID : 1 Uplink Radio MAC : 00:09:00:01:00:01 SSID Name : roam-m44-open Parent AP MAC : FC:58:9A:15:DE:4C Uplink State : CONNECTED Auth Type : OPEN Uclient mac : 00:09:00:01:00:01 Current state : UWGB Uclient timeout : 60 Sec Dot11 type : 11ax Channel : 36 Bandwidth : 20 MHz Current Datarate (Tx/Rx) : 77/0 Mbps Max Datarate : 143 Mbps RSSI : 60 IP : 0.0.0.0 IPV6 : ::/128 Assoc timeout : 100 Msec Auth timeout : 100 Msec Dhcp timeout : 60 Sec

Syslog

Syslogs are a category of protocols that send event data logs to a centralized location for storage and analysis. These are widely used for monitoring and troubleshooting network devices by capturing event messages. The term Syslog may also refer to the protocol itself or the system that implements it.

- Protocol Type: Syslog is a standardized protocol commonly used for logging system events.
- Transport Protocol: Currently, Syslog supports only UDP mode for data transmission.
- Debug Log Collection: When the debug command is enabled on a WGB, it collects debug logs and sends them to the Syslog server.
- Log Categorization: Logs sent to the Syslog server from WGB are categorized under the "kernel facility" and logged at the "warning level."

Enable or disable the WGB syslog

Perform this task to configure the syslog functionality on a Workgroup Bridge (WGB). This allows you to enable or disable logging to a specific host, ensuring proper monitoring and debugging.

Procedure

Step 1 Enable or disable WGB syslog using one of the options.

Option	Description
Enable WGB syslog	Use the **logging host enable** *server_ip* **UDP**command. `Device# logging host enable 192.168.1.200 udp`
Disable WGB syslog	Use the **logging host disable** command. `Device# logging host disable`

Step 2 (Optional) Use the **show running-config** command to view current syslog configuration.

```
Device# show running-config
```

Radio Statistics Commands

The **debug wgb dot11 rate**command displays debugging information related to data rates negotiated. It helps troubleshoot connectivity, performance, or roaming issues by showing how the WGB selects and uses data rates when communicating with the access point.

```
Device# debug wgb dot11 rate

[*03/13/2023 18:00:08.7814]                MAC    Tx-Pkts    Rx-Pkts
Tx-Rate(Mbps)                    Rx-Rate(Mbps)  RSSI   SNR Tx-Retries
[*03/13/2023 18:00:08.7814] FC:58:9A:17:C2:51        0         0      HE-20,2SS,MCS6,GI0.8
 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
[*03/13/2023 18:00:09.7818] FC:58:9A:17:C2:51        0         0      HE-20,2SS,MCS6,GI0.8
 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
```

In this example, FC:58:9A:17:C2:51 is the parent AP radio MAC.

The **show interfaces dot11Radio** *slot-id***statistics** command displays detailed statistics for a wireless radio interface. It provides information such as transmitted and received packets, errors, retries, signal quality, and other performance metrics. This is useful for monitoring the health of the radio interface, identifying connectivity issues, and troubleshooting wireless performance.

```
Device# show interfaces dot11Radio 1 statistics

Dot11Radio Statistics:
        DOT11 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                              TRANSMITTER
Host Rx K Bytes:        965570/0      Host Tx K Bytes:       1611903/0
Unicasts Rx:            379274/0      Unicasts Tx:           2688665/0
Broadcasts Rx:         3166311/0      Broadcasts Tx:               0/0
Beacons Rx:          722130099/1631   Beacons Tx:          367240960/784
Probes Rx:           588627347/2224   Probes Tx:            78934926/80
Multicasts Rx:         3231513/0      Multicasts Tx:           53355/0
Mgmt Packets Rx:     764747086/1769   Mgmt Packets Tx:     446292853/864
Ctrl Frames Rx:        7316214/5      Ctrl Frames Tx:              0/0
RTS received:                0/0     RTS transmitted:             0/0
Duplicate frames:            0/0     CTS not received:            0/0
MIC errors:                  0/0     WEP errors:            2279546/0
```

```
FCS errors:                  0/0        Retries:                896973/0
Key Index errors:            0/0        Tx Failures:              8871/0
                                        Tx Drops:                    0/0

Rate Statistics for Radio::
[Legacy]:
6 Mbps:
 Rx Packets:     159053/0            Tx Packets:      88650/0
                                     Tx Retries:       2382/0
9 Mbps:
 Rx Packets:          43/0           Tx Packets:         23/0
                                     Tx Retries:         71/0
12 Mbps:
 Rx Packets:           1/0           Tx Packets:        119/0
                                     Tx Retries:        185/0
18 Mbps:
 Rx Packets:           0/0           Tx Packets:          5/0
                                     Tx Retries:        134/0
24 Mbps:
 Rx Packets:         235/0           Tx Packets:      20993/0
                                     Tx Retries:       5048/0
36 Mbps:
 Rx Packets:           0/0           Tx Packets:        781/0
                                     Tx Retries:        227/0
54 Mbps:
 Rx Packets:         133/0           Tx Packets:       9347/0
                                     Tx Retries:       1792/0

[SU]:
M0:
 Rx Packets:           7/0           Tx Packets:          0/0
                                     Tx Retries:          6/0
M1:
 Rx Packets:        1615/0           Tx Packets:      35035/0
                                     Tx Retries:       3751/0
M2:
 Rx Packets:       15277/0           Tx Packets:     133738/0
                                     Tx Retries:      22654/0
M3:
 Rx Packets:       10232/0           Tx Packets:       1580/0
                                     Tx Retries:      21271/0
M4:
 Rx Packets:      218143/0           Tx Packets:     190408/0
                                     Tx Retries:      36444/0
M5:
 Rx Packets:      399283/0           Tx Packets:     542491/0
                                     Tx Retries:     164048/0
M6:
 Rx Packets:     3136519/0           Tx Packets:     821537/0
                                     Tx Retries:     329003/0
M7:
 Rx Packets:     1171128/0           Tx Packets:     303414/0
                                     Tx Retries:     154014/0


Beacons missed: 0-30s 31-60s 61-90s 90s+
                     2      0      0    0
```

The **show wgb dot11 uplink latency** command displays latency statistics for the Workgroup Bridge (WGB) uplink connection to the access point (AP). It helps measure the time taken for frames to traverse from the WGB to the AP, providing insight into wireless link performance and potential delay issues.

```
AP# show wgb dot11 uplink latency

Latency Group Total Packets Total Latency Excellent(0-8) Very Good(8-16) Good (16-32 ms)
Medium (32-64ms) Poor (64-256 ms) Very Poor (256+ ms)
        AC_BK             0             0              0               0               0
              0               0                    0
        AC_BE          1840       4243793           1809              10              14
              7               0                    0
        AC_VI             0             0              0               0               0
              0               0                    0
        AC_VO            24         54134             24               0               0
              0               0                    0
```

The **show wgb dot11 uplink** command displays information about the Workgroup Bridge (WGB) uplink to the access point (AP). It provides details such as the associated SSID, BSSID, channel, signal strength, data rates, authentication type, and overall status of the uplink connection. This is useful for verifying connectivity and monitoring the WGB's wireless link to the AP.

```
AP# show wgb dot11 uplink

HE Rates: 1SS:M0-11 2SS:M0-11
Additional info for client 8C:84:42:92:FF:CF
RSSI: -24
PS  : Legacy (Awake)
Tx Rate: 278730 Kbps
Rx Rate: 410220 Kbps
VHT_TXMAP: 65530
CCX Ver: 5
Rx Key-Index Errs: 0
              mac     intf TxData TxUC TxBytes TxFail TxDcrd TxCumRetries MultiRetries
MaxRetriesFail RxData RxBytes RxErr                 TxRt(Mbps)                  RxRt(Mbps)
  LER PER stats_ago
8C:84:42:92:FF:CF wbridge1   1341 1341  184032      0      0          543           96
          0    317   33523     0 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8 (458) 27272
   0  1.370000
Per TID packet statistics for client 8C:84:42:92:FF:CF
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s)
       0      35    1314            0             8
       1       0       0            0             0
       2       0       0            0             0
       3       0       0            0             0
       4       0       0            0             0
       5       0       0            0             0
       6     182      24            1             0
       7       3       3            0             0
Rate Statistics:
Rate-Index    Rx-Pkts    Tx-Pkts Tx-Retries
         0         99          3          0
         4          1          1          9
         5         21         39         35
         6         31        185         64
         7         26        124         68
         8         28        293         82
         9         77        401        151
        10         32        140         97
        11          2        156         37
```

Configure event logging

For WGB field deployment, event logging collects useful information such as WGB state changes and received or transmitted packets. This information provides a log history to help analyze issues, particularly during roaming.

You can configure the WGB trace filter for packet types such as probe, auth, assoc, eap, dhcp, icmp, and arp.

The product supports four types of events.

- Basic event: covers most WGB basic-level information messages.
- Detail event: covers the basic event and additional debug-level messages.
- Trace event: records WGB trace events if enabled.
- All event: bundles trace events and detail events.

The log format is [*timestamp* | *module* | *level* | *event log string*].

Note Starting from UIW Release 17.17.1, we recommend using the commands mentioned in the "Configure remote server" procedure to obtain more comprehensive diagnostic information.

Procedure

Step 1 Use the **config wgb event trace** {**enable** | **disable**}command to enable or disable WGB trace.

```
Device# config wgb event trace enable
```

Step 2 (Optional) Use the **show wgb event** [**basic** | **detail** | **trace** | **all**] command to manually dump event log messages to memory and to display WGB logging.

```
Device# show wgb event all

[*08/16/2023 08:18:25.167578] UP_EVT:4 R1 IFC:58:9A:17:B3:E7] parent_rssi: -42 threshold:
-70
[*08/16/2023 08:18:25.329223] UP_EVT:4 R1 State CONNECTED to SCAN_START
[*08/16/2023 08:18:25.329539] UP_EVT:4 R1 State SCAN_START to STOPPED
[*08/16/2023 08:18:25.330002] UP_DRV:1 R1 WGB UPLINK mode stopped
[*08/16/2023 08:18:25.629405] UP_DRV:1 R1 Delete client FC:58:9A:17:B3:E7
[*08/16/2023 08:18:25.736718] UP_CFG:8 R1 configured for standard: 7
[*08/16/2023 08:18:25.989936] UP_CFG:4 R1 band 1 current power level: 1
[*08/16/2023 08:18:25.996692] UP_CFG:4 R1 band 1 set tx power level: 1
[*08/16/2023 08:18:26.003904] UP_DRV:1 R1 WGB uplink mode started
[*08/16/2023 08:18:26.872086] UP_EVT:4 Reset aux scan
[*08/16/2023 08:18:26.872096] UP_EVT:4 Pause aux scan on slot 2
[*08/16/2023 08:18:26.872100] SC_MST:4 R2 reset uplink scan state to idle
[*08/16/2023 08:18:26.872104] UP_EVT:4 Aux bring down vap - scan
[*08/16/2023 08:18:26.872123] UP_EVT:4 Aux bring up vap - serv
[*08/16/2023 08:18:26.872514] UP_EVT:4 R1 State STOPPED to SCAN_START
[*08/16/2023 08:18:26.8727091 SC_MST:4 R1 Uplink Scan Started.
[*08/16/2023 08:18:26.884054] UP_EVT:8 R1 CH event 149
```

It might take a long time to display the output of the show wgb event command in the console. Interrupting printing with Ctrl+C does not affect the log dump to memory.

Step 3 (Optional) Use the **clear wgb event** [**basic** | **detail** | **trace** | **all**] command to erase WGB events in memory.

```
Device# clear wgb event all
```

Step 4 (Optional) Use the **copy event-logging flash** command to save all event logs to WGB flash.

```
Device# copy event-logging flash
```

The package file includes four separate log files, each for a different log level.

Step 5 (Optional) Use the **copy event-logging upload**[**tftp** | **sftp** | **scp**] ://*ip-address* [*dir*][*/filename.tar.gz*] command to save event logs to a remote server.

```
Device# copy event-logging upload
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz

Starting upload of WGB config
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz ...
It may take a few seconds. If longer, please cancel command, check network and try again.
##################################################################### 100.0%
Config upload completed.
```

Configure remote server

This task configures the log transfer settings on the device. The log transfer settings define the transfer protocol (TFTP or SFTP), authentication credentials (for SFTP), the remote server IP address, and an optional server path. This setup ensures that event logs and system logs are securely uploaded to a remote server for storage, monitoring, or troubleshooting.

Procedure

Step 1 Use the **transfer upload mode** {**delete** | **sftp** | **tftp**} command to select the protocol for log transfer.

```
Device# transfer upload mode tftp
```

Step 2 Use the **transfer upload credential add** *username* **password** *password* command to configure the username and password.

```
Device# transfer upload credential add Cisco password Cisco123
```

Step 3 Use the **transfer upload server-ip add** *remote-server-ip* command to configure the remote server IP address.

```
Device# transfer upload server-ip add 192.168.71.11
```

Step 4 (Optional) Use the **transfer upload server-ip add** *remote-server-ip* **path** *remote-server-path* command to configure the remote server path.

```
Device# transfer upload server-ip add 192.168.71.11 path /upload/wgb
```

These static configurations are persistent and remain effective even after a device reload.

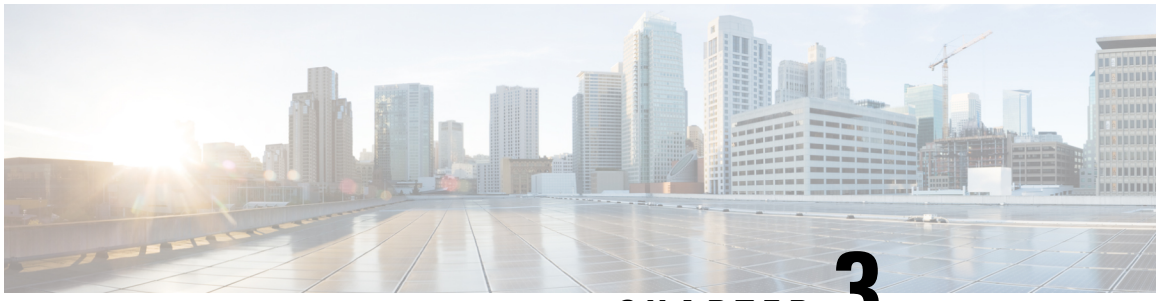
Step 5 Use the **transfer upload start** command to collect event logs and transfer them to the remote server.

```
Device# transfer upload start
```

After configuring the remote server, the device collects and transfers these types of data:

- Core files to support troubleshooting.
- Syslog files to monitor system events and activities.
- WGB or uWGB running configuration to back up settings.

- Radio reset history to identify potential connectivity issues.
- Event logging data to track system performance and incidents.



CHAPTER 3

Manage the Workgroup Bridges through Web UI

- Workgroup Bridge, on page 97
- Access the Cisco Workgroup Bridge Web UI, on page 98
- Monitor the client details and configurations, on page 98
- Configure and authenticate wireless profiles, on page 99
- Configure a static route for NAT wired client access to the WebUI in uWGB mode, on page 103
- Configure WGB and uWGB radio modes, on page 104
- Set IP address, on page 106
- Modify the RSSI threshold, on page 107
- Create NAT rules, on page 108
- Manage firmware images, on page 109
- Import or export a configuration file, on page 111

Workgroup Bridge

Workgroup Bridge (WGB) is an Access Point (AP) mode that:

- provides wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP,
- connects a wired network to a wireless segment by learning wired clients' MAC addresses on the Ethernet interface and reporting them to the wireless controller using Internet Access Point Protocol (IAPP) messages through an infrastructure AP, and
- establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

For more details on WGB, see the chapter WGB.

Table 7: Feature History Table

Feature	Release Information	Feature Description
Manage the Workgroup Bridges through Web UI	IOS XE 17.18.1	This feature enables you to configure the IW916X WGB through the Web UI.

Cisco Web UI is a browser-based graphical user interface (GUI) that simplifies device setup, monitoring, and troubleshooting, making it particularly helpful for users unfamiliar with the Command-Line Interface (CLI).

Access the Cisco Workgroup Bridge Web UI

This procedure describes how to access the Cisco Workgroup Bridge (WGB) Web UI dashboard by connecting a wired client, verifying connectivity, and logging in with the appropriate credentials.

Before you begin

- Ensure your WGB switch has a wired client and is reachable on the 192.168.0.x network.
- Configure the wired client and switch to access the Cisco WGB Web UI at its default IP address (192.168.0.10).
- Perform these steps to access the Cisco WGB Web UI dashboard.

Procedure

Step 1 Access the Cisco WGB Web UI using a browser. Enter the IP address 192.168.0.10. Log in with the default credentials:

- username—Cisco
- password—Cisco

The Cisco WGB Web UI redirects you to its homepage. Ensure that the wired client and the Cisco WGB switch are on the 192.168.0.x network by verifying the client IP address.

Step 2 Ping 192.168.0.10 from the client to verify connectivity.

Step 3 Update the explicit login credentials.

Step 4 Log in using the new credentials to access the Cisco WGB Web UI.

Monitor the client details and configurations

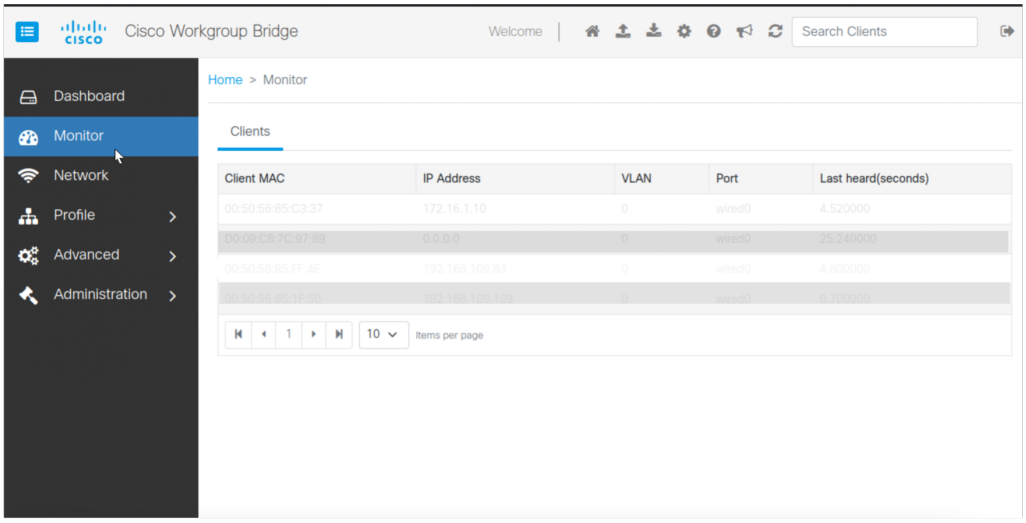
You can track live activity and device connectivity to troubleshoot issues and ensure a seamless network. Monitor client details, such as MAC address, IP address, VLAN information, port, and last heard time (in seconds), to achieve this.

This procedure describes how to monitor client details.

Procedure

Step 1 From Cisco WGB Web UI, choose **Monitor** to view the client details.

Step 2 Choose a number from the **Items per page** drop-down to set how many client entries appear on each page.



Configure and authenticate wireless profiles

A wireless profile is a pre-configured set of network settings that enables devices to connect to a wireless network automatically and securely.

- Allows devices to connect automatically without manual reconfiguration.
- Stores network details such as SSID, security type, encryption method, and passphrase.
- Minimizes credential entry errors and ensures secure, consistent connections.
- Simplifies distribution and management of network settings across multiple devices.
- Enables easy switching between saved networks (for example, home, office, or public Wi-Fi).

Configuring secure wireless access using 802.1X authentication

To configure secure wireless access using 802.1X authentication, complete these tasks:

Create a WLAN

This procedure describes how to create a WLAN.

You can create Wireless Local Area Network (WLAN) to provide wireless connectivity within a specific area, enabling devices to connect to the network without physical cables. WLANs enhance mobility by allowing users to move freely within the network's coverage area while maintaining connectivity. They reduce the need for extensive cabling, simplifies setup, and lower costs.

Before you begin

Configure Extensible Authentication Protocol (EAP), if you access multiple SSID.

Procedure

Step 1 Choose **Profile** > **WLAN** .

Step 2 Click **Create** .

Step 3 Select **Authentication** in **WLAN Profile Configurations** .

The **Authentication** types are:

- **Open** : It provides access to networks without a password.
- **OWE** : Opportunistic Wireless Encryption (OWE) provides automatic encryption for open networks without a password.
- **PSK** : Pre-Shared Key (PSK) secures networks using a shared password for authentication and encryption.
- **SAE** : Simultaneous Authentication of Equals (SAE) secures networks with strong password-based authentication and encryption.
- **EAP** : Extensible Authentication Protocol (EAP) supports various authentication methods.

  You can configure EAP in WLAN either in **Default EAP Profile** or **EAP Profile List** . For details on EAP Profile configuration, see Create EAP profile , on page 101 .

  To select the **EAP Profile List** , you need to provide t **Username** , **Password** , and **Key Management** information. For more details, see Map EAP profile to SSID, on page 102 .

Step 4 Update the required **Key Management** details based on **Authentication** .

The **Key Management** types are:

- **dot11r** : 802.11r (Fast Transition)
- **dot11w** : 802.11w (Protected Management Frames)
- **WPA2** : secures Wi-Fi with AES encryption.
- **WAP3** : enhances Wi-Fi with stronger encryption and password security.

Step 5 Click **Update & apply to device** .

Create 802.1X profile

You can use a 802.1X Profile to define authentication settings for IEEE 802.1X, enabling secure, controlled, and authenticated network access for users and devices.

Perform these steps to create 802.1X profile.

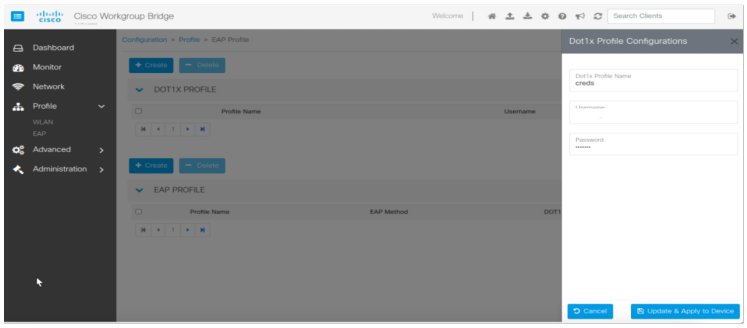
Procedure

Step 1 Choose **Profile** > **EAP**.

Step 2 Click **Create** in **DOT1x PROFILE** area.

Step 3 Enter **Dot1x Profile Name, Username** and **Password**.

Step 4 Click **Update & Apply to Device**.



EAP profiles and SSID maps

You can use EAP profiles to define secure authentication methods (example: Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)) for validating users or devices on a wireless network. Similarly, you can configure SSID maps to associate network names (SSIDs) with specific policies, VLANs, or EAP profiles. Together, they ensure secure access, proper segmentation, and efficient network management.

Create EAP profile

To securely authenticate users and devices in networks, EAP is required as it provides robust access control and data protection. EAP is essential for IIoT ecosystems that require scalable and secure device authentication. It offers flexibility and multiple authentication methods, which are critical for network security and safeguarding sensitive data.

Before you begin

Configure 802.1x profile. For more details see, Create 802.1X profile, on page 100.

Perform these steps to create EAP profile.

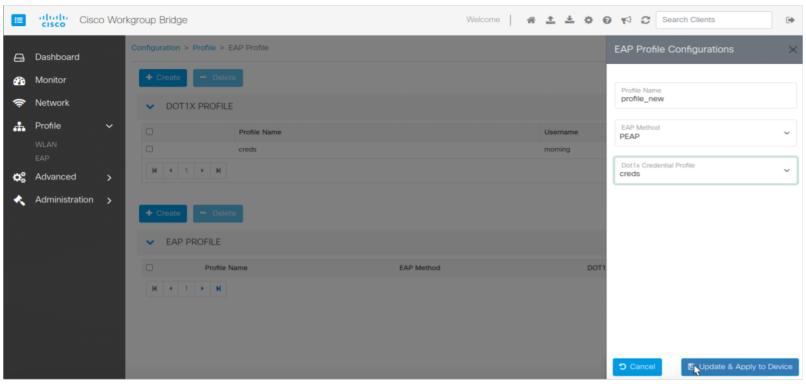
Procedure

Step 1 Choose **Profile > EAP**.

Step 2 Click **Create** in **EAP PROFILE** area.

Step 3 Update the **Profile Name, EAP Method** and **Dot1x Credential Profile** in **EAP Profile Configurations** .

Step 4 Click **Update & Apply to Device**.



Map EAP profile to SSID

Mapping the Extensible Authentication Protocol (EAP) to an Service Set Identifier (SSID) provides secure and authenticated access for devices connecting to the wireless network.

Perform these steps to map EAP profile to SSID.

Procedure

Step 1 Choose **Profile** > **WLAN**.

Step 2 Click **Create**.

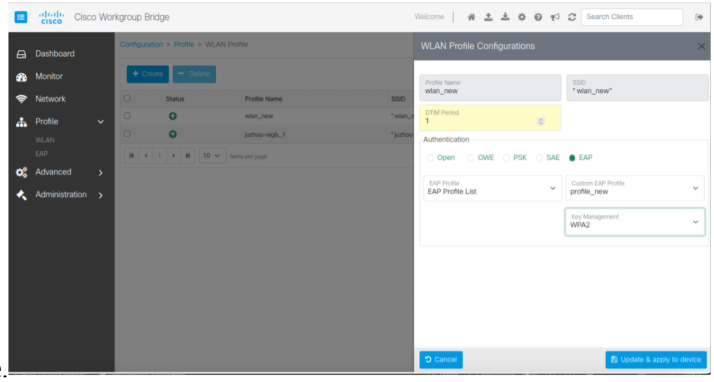
Step 3 Update **Profile Name** and **DTIM Period**.

Step 4 Select **EAP** in **Authentication**.

Step 5 Select the **Profile Name** provided while creating the EAP in **EAP Profile** from the drop-down.

Step 6 Select **Key Management** from the drop-down.

Step 7 Click **Update & apply to device**.



Map the SSID to the uplink radio

This procedure describes how to map SSID to uplink radio.

You can map a Service Set Identifier (SSID) to an uplink radio to enable proper traffic routing and ensure connectivity to the upstream network.

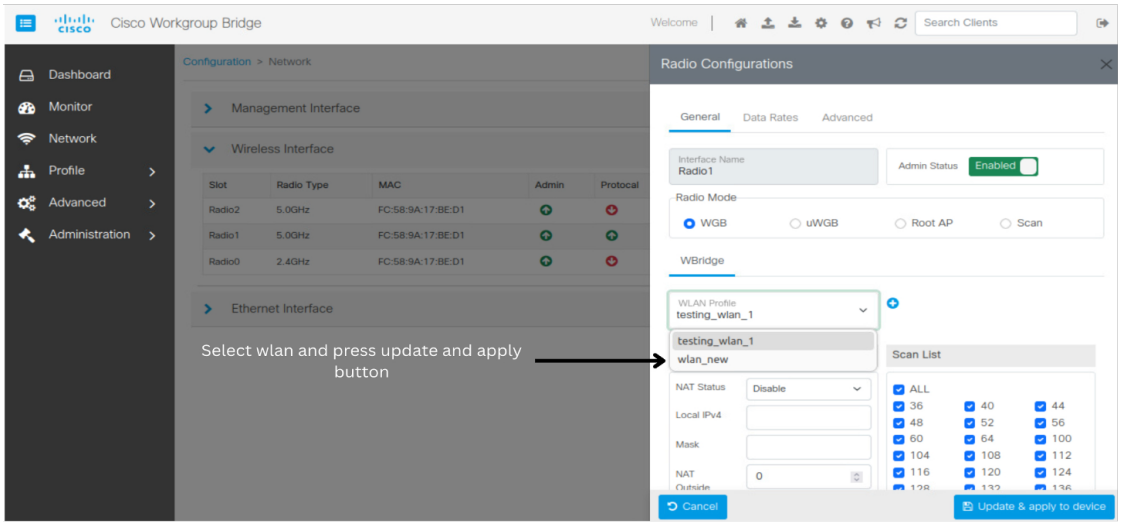
Procedure

Step 1 From the **Network** page, choose the desired uplink radio in **Wireless Interface.**

Step 2 Select the WLAN to be mapped from the **WLAN Profile** drop-down.

Step 3 Select **WGB** in **Radio Mode** .

Step 4 Click **Update & apply to device** .



Configure a static route for NAT wired client access to the WebUI in uWGB mode

This procedure describes how to configure a static route for NAT wired client access to the WebUI in uWGB mode.

You can add a route to the NAT wired client to access the WebUI in uWGB mode via private LAN port.

Run these commands on the Linux client.

Procedure

Step 1 `sudo ifconfig ens192 172.16.1.10 netmask 255.255.255.0`

ens192 —NAT wired client interface.

`172.16.1.10` —IP address of NAT wired client.

Step 2 `sudo ip route add 172.16.1.0/24 dev ens192`

Step 3 `sudo ip route add 192.168.109.0/24 via 172.16.1.11 dev ens192`

The Cisco WGB Web UI for uWGB can be accessed from the NAT wired client.

`172.16.1.11` —Configure WGB LAN port in **WLAN** > **Radio Configuration** > **uWGB mode** > **NAT** .

`192.168.109.0` —Outside network IP address.

After configuring uWGB mode, access the Cisco WGB Web UI using the IP address 172.16.1.11 from the NAT wired client.

Create a NAT rule to access uWGB mode. For details on NAT rules creation, see Create NAT rules, on page 108 .

Configure WGB and uWGB radio modes

The radio mode on the Cisco IoT Workgroup Bridge (IW916x) can be configured to operate in one of two distinct modes: WGB or uWGB. The mode selection depends on the type of Root Access Point (RAP) in the network infrastructure and is designed to ensure compatibility and seamless connectivity.

- WGB mode: Standard Workgroup Bridge operation for connecting non-wireless devices to a wireless network.
- uWGB mode: Universal Workgroup Bridge operation for enhanced compatibility with specific network infrastructures.

Configure the radio in WGB mode

This procedure describes how to configure WGB mode.

You can optimize network configurations and improve operational efficiency by switching to WGB mode. In this mode, the WGB uses Cisco's proprietary protocol extensions for enhanced performance and features. This mode is ideal for Cisco infrastructure deployments. If the Root Access Point (RAP) is a Cisco Access Point, setting the Radio Mode to WGB enables full use of Cisco-specific enhancements.

Procedure

Step 1 From Cisco WGB Web UI, choose **Network** .

Step 2 Select a desired radio from the list of available **Wireless Interface** .

Step 3 Select **WGB** in **Radio Mode** > **Radio Configurations** .

The radio modes can be changed to any mode like **WGB** , **uWGB** , **Root AP** or **Scan** mode.

Configure uWGB mode on the radio

This procedure describes how to configure the device to operate in uWGB mode for interoperability in mixed-vendor environments and to access or manage the WebUI in uWGB mode.

You can optimize network configurations and enhance operational efficiency by switching to uWGB mode. In this mode, the WGB uses standard protocols to provide universal compatibility. This functionality allows seamless integration with non-Cisco Access Points (APs). This mode ensures interoperability in mixed-vendor environments. Setting the Radio Mode to uWGB provides universal compatibility and reliable connectivity if the Root Access Point (RAP) is a non-Cisco AP.

Once configuration is complete, use the WGB private LAN port address of the NAT wired client to access the WebUI in uWGB mode. For more details about NAPT on uWGB, refer to NAPT on uWGB .

Before you begin

To access or manage the WebUI in uWGB mode, configure the device with Network Address port translation (NAPT).

Procedure

Step 1 From Cisco WGB Web UI, choose **Network** .

Step 2 Select a desired radio from the list of available **Wireless Interface** .

Step 3 Select **uWGB** in **Radio Mode** > **Radio Configurations** .

The radio modes can be changed to any mode like **WGB** , **uWGB** , **Root AP** or **Scan** mode.

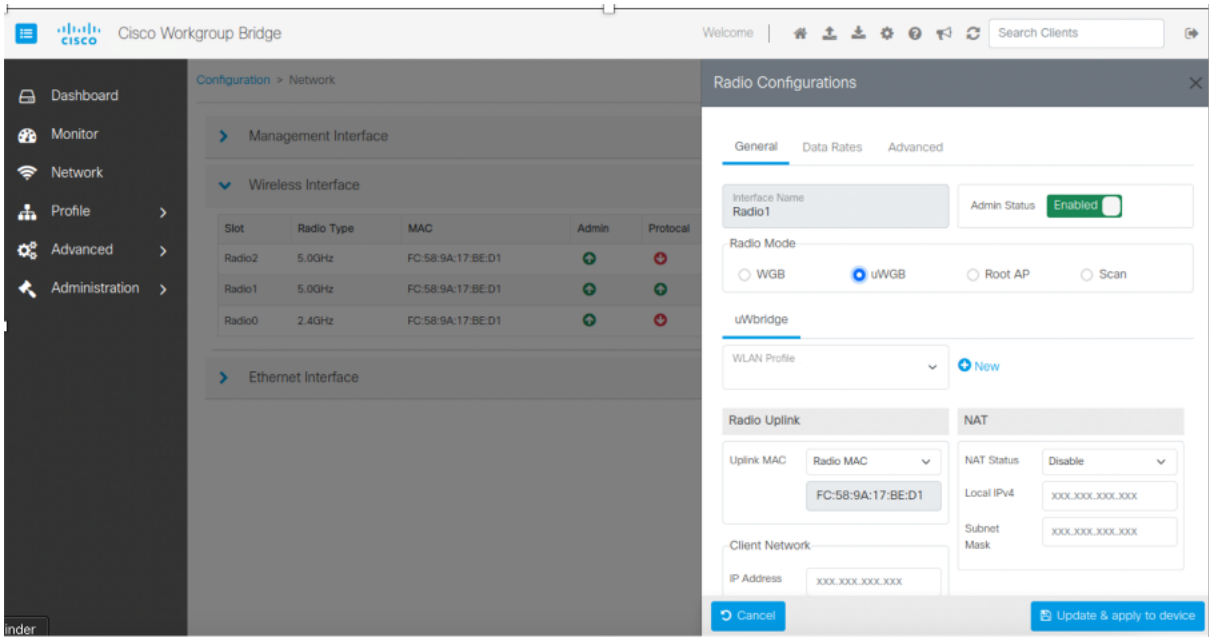
Step 4 Choose **Radio MAC** from drop-down.

Enter client MAC.

Step 5 Choose **NAT Status** from **NAT** drop-down.

Step 6 Enter the IP address of the NAT wired client in the **Local IPv4** field to access the web UI.

Step 7 Click **Update & apply to device** .



Set IP address

The IP address used for accessing Cisco WGB Web UI can be set as either static or through DHCP to enhance the operational efficiency. With this approach, you can switch from static IP to dynamic IP and dynamic IP to static IP.

Switch from static IP to dynamic IP

This procedure describes how to change a static IP address to a dynamic IP address.

You can switch from a static IP to dynamic IP allocation to enable automatic IP address assignment. This change simplifies network management by removing the need for manual configuration and by reducing the risk of IP conflicts. It also helps conserve IP resources, as addresses are assigned dynamically only when devices are connected.

Procedure

Step 1 Choose **Network** > **Management Interface** .

Step 2 Select **auxiliary-client** .

Step 3 Change **Static** to **DHCP** from **IPv4 Type** drop-down.

Step 4 Click **Update & apply to device** .

Switch from dynamic IP to static IP

This procedure describes how to change a dynamic IP address to a static IP address.

You can switch from dynamic IP to static IP allocation to assign a fixed IP address to a device. This ensures consistent network identification, improves reliability for devices like servers or printers, and simplifies tasks such as port forwarding or troubleshooting by keeping the IP address unchanged.

Procedure

Step 1 Choose **Network > Management Interface.**

Step 2 Select **auxiliary-client** in **Interface** .

Step 3 Change **DHCP** to **Static** in the **IPv4 Type** drop-down.

Step 4 Update:

- **Static IP Address** : specify the manually assigned IP.
- **Network Mask** : specify the network and host portions of an IP address.
- **Gateway IP** : specify the IP address of the router that interconnects networks.
- **DNS1 IP** : specify the IP address of the primary DNS server.

Modify the RSSI threshold

This procedure describes how to modify the RSSI threshold.

The Received Signal Strength Indicator (RSSI) measures the power of a wireless signal and is used to evaluate connection quality and strength in wireless networks.

You can set an RSSI threshold to define the minimum signal strength required for maintaining a reliable and optimal wireless connection.

Procedure

Step 1 Choose **Network** .

Step 2 Choose the desired **Radio Type** in the **Wireless Interface** .

Step 3 Choose **Mobility** and **RSSI** threshold to optimize wireless network performance and ensure seamless connectivity for devices.

Step 4 Select **Advanced** in **Radio Configurations** .

Step 5 Update **RSSI Threshold** from drop-down in the **Mobility**.

The RSSI Threshold values are:

- -30 dBm to -50 dBm: Excellent signal strength (ideal for most applications).

- -50 dBm to -60 dBm: Good signal strength (suitable for reliable connectivity).
- -60 dBm to -70 dBm: Fair signal strength (may experience minor connectivity issues).
- -70 dBm to -80 dBm: Weak signal strength (likely to experience performance issues).
- Less than -80 dBm: Very poor signal strength (connectivity may fail or be highly unreliable).

The default RSSI threshold value is -70 dBm.

Step 6 Modify these parameters in the **Antenna** drop-down to optimize signal strength, quality, coverage, and performance in wireless networks:

- **Antenna Number** : optimizes signal reception and coverage.
- **Antenna Gain** : measured in dBi, indicates an antenna's ability to focus signals, with higher values signifying stronger, more directional transmission.

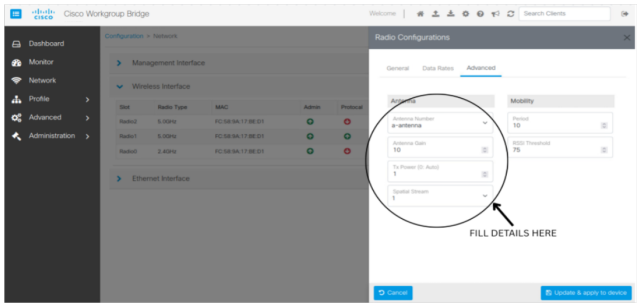
  In **Antenna Gain** field, you can:

  - Enter a value
  - Use the in-field arrows to select a value.

  Values range from 2 dBi to 12 dBi.
- **Tx Power** : maintains signal quality without interference.

  Values range from 1 dBm to 30 dBm.
- **Spatial Stream** : Improves throughput and performance.

  Values range from 1 to 8.



Create NAT rules

This procedure describes how to create NAT rules.

You can use Network Address Translation (NAT) rules to convert private IP addresses into a single public IP address, allowing multiple devices on your network to share one public IP for internet access. This helps conserve public IP addresses and improves security by hiding internal IPs from external networks.

NAT also lets you set rules to control and manage traffic, guaranteeing only authorized data flows between your private and public networks, making it an essential tool for efficient and secure network management.

Procedure

Step 1 From **Network** page, choose the desired uplink radio in **Wireless Interface** .

Step 2 Set the **NAT Outside Port Min** and **NAT Outside Port Max** values in **Radio Configurations > NAT** .

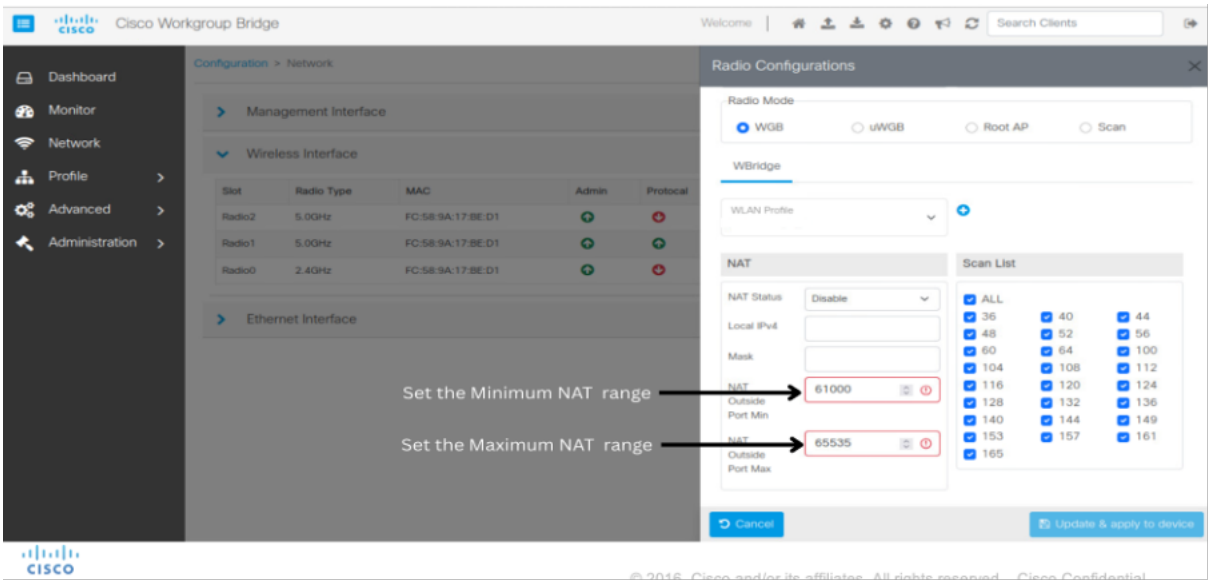
Both **NAT Outside Port Min** and **NAT Outside Port Max** values for NAT port ranges must fall within the range of 1 to 65535.

Step 3 From Cisco WGB Web UI, choose **Advance > NAT** .

Step 4 Click **Create** and update these values:

- **Global port**: Specify 443 as the external (public-facing) port for communication.
- **Local IP**: Specify the internal (private) IP address of the device being mapped.
- **Local Port**: Specify the type of traffic, such as TCP or UDP, to be translated.
- **Traffic Type**: Specify the type of traffic, such as TCP or UDP, to be translated.

Step 5 Click **Update & Apply to Device** .



Manage firmware images

You can efficiently maintain and update device operations by reloading images, activating backups, performing factory resets, upgrading firmware, or importing and exporting configurations.

Reload the firmware image

This procedure describes how to reload the currently running firmware image.

You can reload the currently running firmware image to apply changes or address potential software issues.

Procedure

Step 1 Choose **Administration** > **Firmware** .

Step 2 Click **Reboot** in **Running Software** .

Load a backup image

This procedure describes how to load the back up firmware image.

You can load a backup image to restore the device to a previous stable state or recover from firmware-related issues.

Procedure

Step 1 Choose **Administration** > **Firmware** .

Step 2 Click **Activate** in **Backup Software** .

Perform a factory reset

This procedure describes how to factory reset the device.

You can perform a factory reset to restore the device to its default settings, clearing all configurations and customizations.

Procedure

Step 1 Choose **Administration** > **Firmware** .

Step 2 Click **Clear Configuration** .

Note
After selecting **Clear Configuration** , the WGB goes to Day 0 scenario.

Upgrade the firmware image

This procedure describes how to upgrade the currently running firmware image.

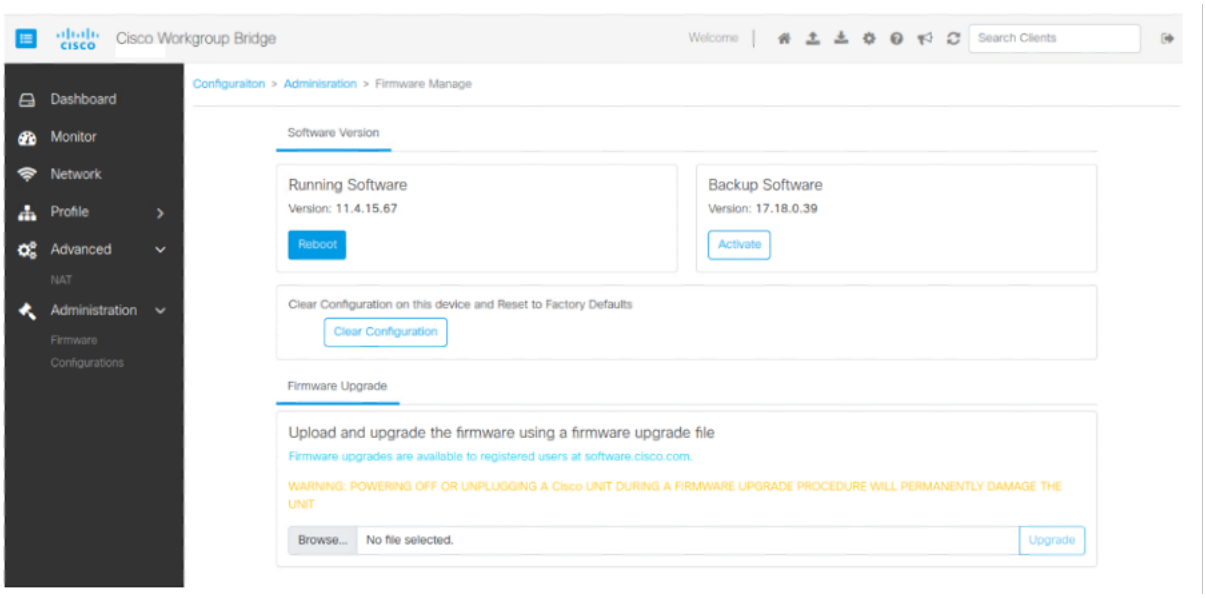
You can upgrade the firmware image to access new features, enhancements, or bug fixes for improved device performance.

Procedure

Step 1 Choose **Administration > Firmware > Browse** .

Step 2 Select the required image.

Step 3 Click **Upgrade** and wait for 180 seconds for the image to reboot and open the Web UI.



Import or export a configuration file

This procedure describes how to import or export a configuration file.

You can import or export a configuration file to back up current settings or to restore settings when needed.

Procedure

Step 1 Choose **Administration > Configurations**.

Step 2 Click **View detail** to check the current configurations in Cisco WGB.

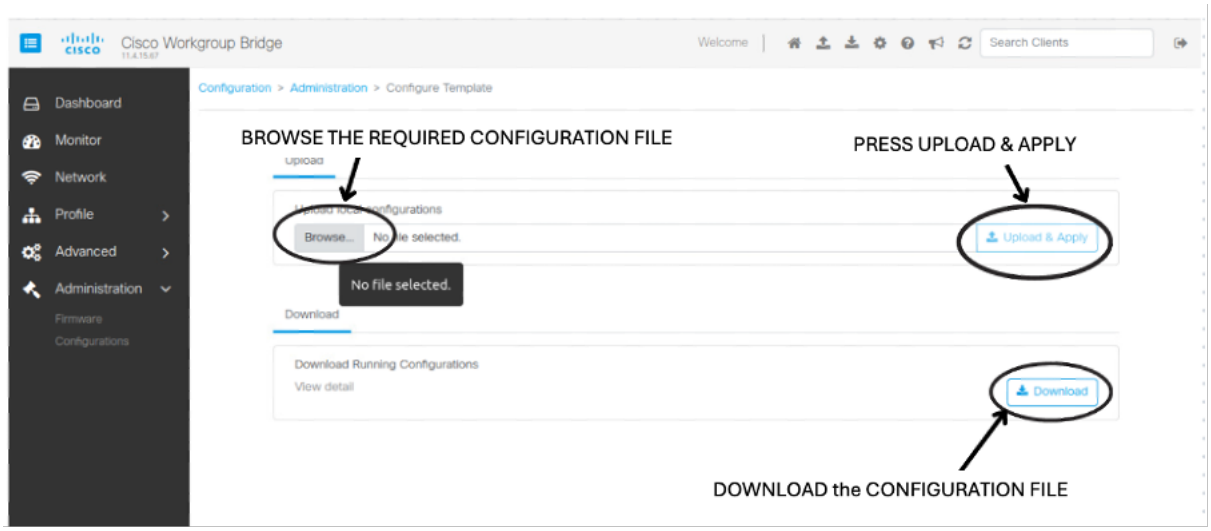
Step 3 Click **Download** to download the configuration.

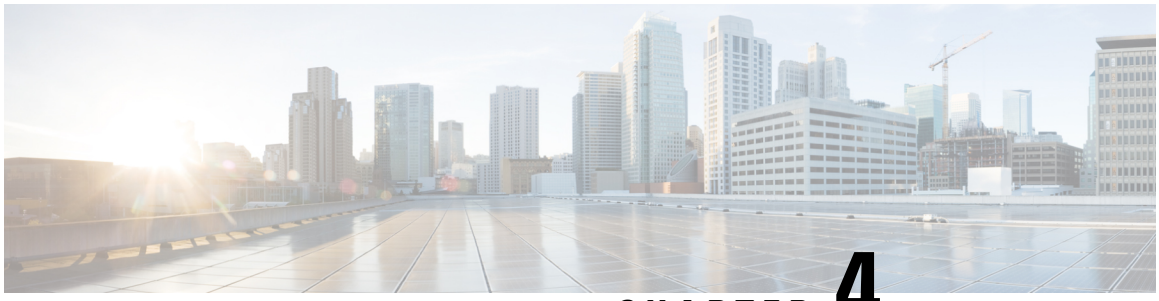
Step 4 Upload the desired configuration to import it later when needed.

Step 5 Click **Upload & Apply** .

Note
The desired configuration file must be of .txt format only.

When you download the configuration, the file is saved to your browser.


Cisco Workgroup Bridge
Welcome
Search Clients
Dashboard
Monitor
Network
Profile
Advanced
Administration
Firmware
Configurations
Configuration > Administration > Configure Template
BROWSE THE REQUIRED CONFIGURATION FILE
PRESS UPLOAD & APPLY
Upload
Browse...
No file selected.
Upload & Apply
No file selected.
Download
Download Running Configurations
View detail
Download
DOWNLOAD the CONFIGURATION FILE



CHAPTER 4

Control and Provisioning of Wireless Access Points

- Overview, on page 113
- Indoor deployment, on page 118
- AFC support for 6 GHz standard power mode, on page 124
- Verify AFC status on an AP, on page 125
- GNSS support, on page 125
- Antenna disconnection detection, on page 126
- Troubleshooting, on page 127

Overview

CAPWAP is an IEEE standard protocol that enables a wireless LAN controller to manage multiple APs. It also allows Wireless LAN Controllers (WLCs) to exchange control and data plane information over a secure communication tunnel.

- Operates at Layer 3 and requires IP addresses on both APs and WLCs.
- Establishes tunnels on UDP ports 5246 (control) and 5247 (data) for IPv4 and IPv6, with DTLS encryption for security.
- Allows centralized management of the wireless network and supports secure communication between APs and controllers.

CAPWAP Protocol

CAPWAP uses DTLS to secure the control channel, encrypting all management and control traffic between the AP and WLC. The data channel is disabled by default. To enable CAPWAP data encryption, a DTLS license is required on the WLC and additional configuration is necessary on the AP.

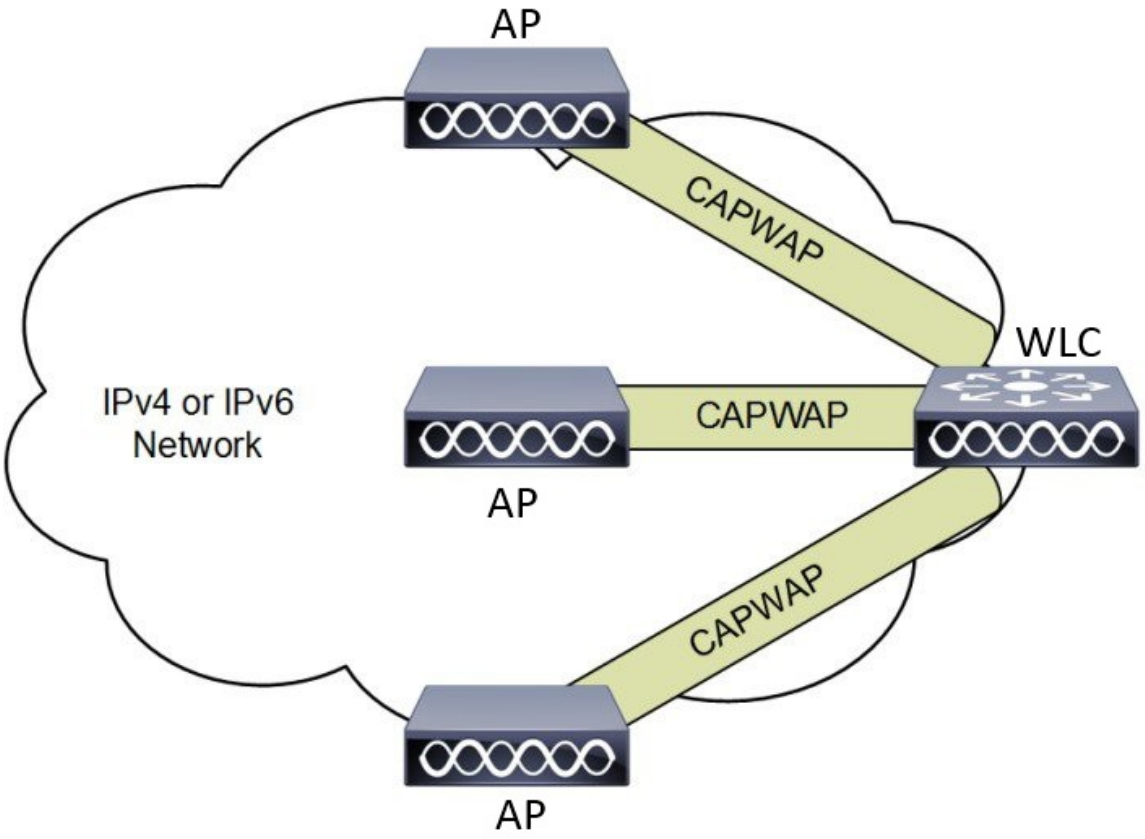
- DTLS ensures encrypted communication to prevent eavesdropping or tampering.
- If an AP does not support DTLS data encryption, only the control plane is secured.
- If an AP supports Data DTLS, it enables data DTLS after receiving configuration from the controller and performs a DTLS handshake on port 5247.
- All data traffic between the AP and controller is encrypted after successful DTLS session establishment.

- The IW9165E uses the IETF standard CAPWAP to communicate between the controller and other APs on the network.

CAPWAP APs Connected to a WLC

This figure shows CAPWAP APs connected to a wireless LAN controller, illustrating the secure communication tunnel established between the APs and the WLC using CAPWAP and DTLS encryption.

Figure 7: CAPWAP APs connected to a WLC



Provisioning certificates on Lightweight Access Points

Certificate provisioning on a Lightweight Access Point (LAP) consists of several coordinated steps involving the LAP, controller, and certificate authority (CA).

Summary

The following actors and components participate in the certificate provisioning process:

- LAP: Initiates the certificate request and installs the signed certificate.

- Controller: Acts as a CA proxy and validates certificates during the JOIN process.
- CA: Signs the certificate request forwarded by the controller.

This process ensures secure communication by provisioning and validating device certificates on the LAP.

Workflow

These stages describe the certificate provisioning workflow on a Lightweight Access Point (LAP):

1. **Certificate Request** : The LAP sends a certificate request to the controller to get a signed X.509 certificate.
2. **CA Proxy** : The controller acts as a CA proxy to facilitate the signing of the certificate request by the CA.
3. **Certificate Installation and Reboot** : Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically.
4. **JOIN Request** : After the reboot, the LAP sends the LSC device certificate to the controller as part of the JOIN request.
5. **JOIN Response and Validation** : The controller sends the new device certificate and validates the inbound LAP certificate with the new CA root certificate as part of the JOIN response.

What's next

Use LSC provisioning functionality to configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for the controller and AP.

Understanding CAPWAP connectivity On AP

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol that enables APs to discover, join, and communicate securely with wireless controllers, supporting both split and local MAC operation modes.

- Facilitates secure discovery and connection between APs and controllers using DTLS.
- Supports two operational modes: **Split MAC** and **Local MAC** .
- Enables centralized management of configuration, firmware, and user data traffic through control and data channels.

CAPWAP connectivity and operation details

CAPWAP connectivity involves a discovery phase, secure connection establishment, and management of AP configuration and data through dedicated channels.

- APs initiate a discovery phase by sending discovery request messages to locate a controller.
- Controllers respond with discovery responses, after which a secure DTLS connection is established.
- APs send CAPWAP join requests and receive join responses to complete the joining process.
- Controllers manage AP configuration, firmware, and control/data transactions post-join.

CAPWAP join process

This section describes the CAPWAP join process between an access point and a wireless LAN controller.

1. Enable CAPWAP on the AP.
2. AP sends discovery request to controller.
3. Controller replies with discovery response.
4. AP sends join request; controller sends join response.
5. Secure DTLS connection is established for CAPWAP control and data messages.

CAPWAP communication between the access point and the wireless LAN controller is established over two logical channels, each serving a distinct function:

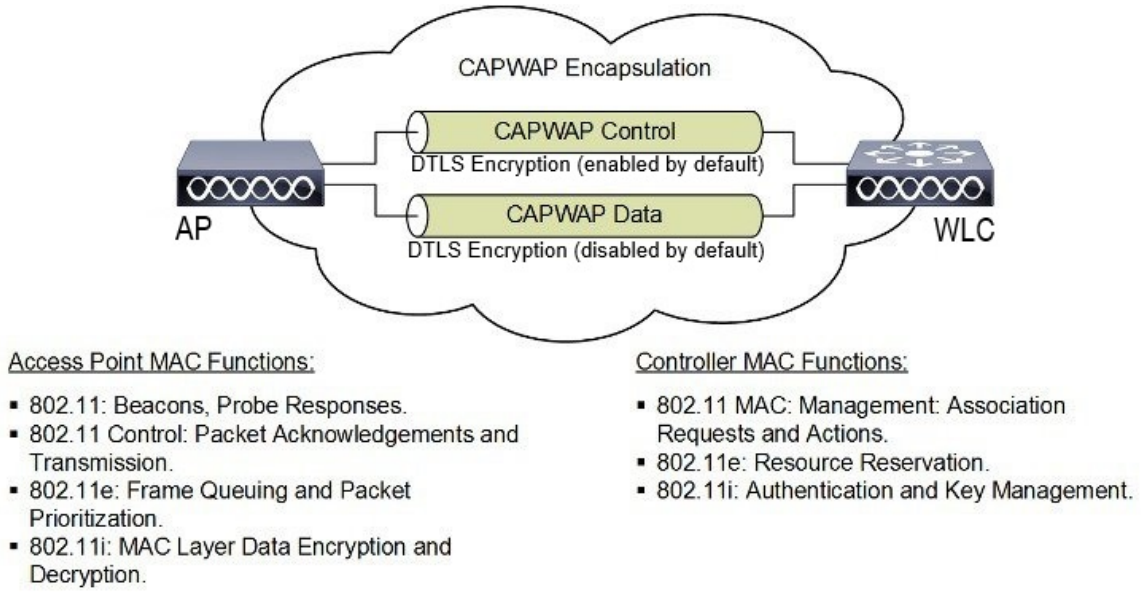
- Control Channel: Used for configuration messages, image downloads, and client key exchanges. APs must acknowledge each message before sending the next.
- Data Channel: Used for encapsulation and tunneling of user data traffic between APs and WLCs, enabling centralized policy enforcement and QoS.

Table 8: CAPWAP Operation Modes Comparison

Attributes	Split MAC	Local MAC
MAC Function Distribution	802.11 protocol split between AP and WLC	All MAC functions performed at AP
Data Frame Handling	Encapsulated and exchanged between WLC and AP	Locally bridged or tunneled as Ethernet frames
Management Frame Processing	Partially at AP, partially at WLC	Entirely at AP

Tip In either mode, the AP processes Layer 2 wireless management frames locally before forwarding them to the controller.

Figure 8: Split MAC Architecture



Example: CAPWAP Join and Data Flow

For example, when a new AP is powered on, it sends a CAPWAP discovery request to locate a controller. After receiving a discovery response, the AP establishes a secure DTLS connection, sends a join request, and upon acceptance, the controller manages the AP's configuration and data traffic through CAPWAP channels.

Reset button settings

The reset button on the IW9165E device allows users to perform different reset actions based on how long the button is pressed.

- Pressing the reset button for less than 20 seconds performs a full reset.
- Pressing the reset button for more than 20 seconds and less than 60 seconds performs a full factory reset (clears the FIPS flag).
- The LED turns blinking red after the boot loader receives the reset signal.

Reset button operation details

To perform a reset, ensure you press the device's reset button before powering on the device. The LED will indicate the reset status by turning blinking red after the boot loader receives the reset signal.

Ethernet port usage on CAPWAP mode

The Catalyst IW9165E supports up to a 3.6 Gbps PHY data rate with two 2x2 multiple input and multiple output (MIMO) and two ethernet ports (2.5G mGig and 1G).

Catalyst IW9165E have below internal port mapping rules:

- Wired0 – One mGig (2.5 Gbps) ethernet ports with 802.3af, 802.3at, 802.3bt PoE support.

Note The wired0 port is used as CAPWAP uplink port in the AP local/Flexconnect mode.

- Wired1 – 1Gig ethernet Lan Port.

Note Starting from 17.14.1 release, RLAN feature is not supported in the wired1 port.

Indoor deployment

The indoor deployment mode for the IW9165E defines how the access point (AP) operates within supported regulatory domains, with specific default settings and frequency usage rules.

- Supports both indoor and outdoor deployment for regulatory domains -B (USA), -E (EU), -A (Canada), and -Z (Australia, New Zealand).
- By default, AP deployment mode is set to indoor.
- For the -B domain, outdoor and indoor frequencies are the same.

Support for 6G power modes

The following table summarizes the support for 6G power modes based on AP deployment and 6G deployment modes.

Table 9: Radio 6G power mode support table

AP Deployment Mode	6G Deployment Mode	Low Power Indoor support	Standard Power support
Indoor AP	Outdoor	No	Yes

Note Outdoor mode can be used indoors, but indoor mode cannot be used outdoors because 5150–5350 MHz channels are indoor-only in -E countries.

For more information about configuring AP deployment mode on the Wireless Controller, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Verify indoor deployment

This procedure describes how to verify whether the indoor deployment is enabled or not on the WLC and AP.

This procedure helps you determine the indoor deployment status on both the Wireless LAN Controller (WLC) and Access Point (AP).

Procedure

Step 1 Run the **show ap name** *ap-name* **config general | inc Indoor** command on the WLC.

- When indoor mode is enabled, the show command provides the following output:

```
Device# show ap name ap-1 config general | inc Indoor
AP Indoor Mode         : Enabled
```

- When indoor mode is disabled, the show command provides the following output:

```
Device# show ap name ap-1 config general | inc Indoor
AP Indoor Mode         : Disabled
```

Step 2 Run the **show controllers Dot11Radio** *interface* command on the AP to check the indoor deployment status.

- When indoor mode is enabled, the show command provides the following output:

```
Device# show controllers Dot11Radio 1
                                    …
Radio Info Summary:
 ======================
Radio: 5.0GHz
Carrier Set:  (-Ei)( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

Note
In the command output, **-Ei** indicates the indoor mode is enabled.

- When indoor mode is disabled, the show command provides the following output:

```
Device# show controllers Dot11Radio 1
                                    …
Radio Info Summary:
 ======================
Radio: 5.0GHz
Carrier Set:  (-E)( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

Note
In the command output, **-E** indicates that indoor mode is disabled.

The CLI output also shows the supported channels.

AP Radio Slot

The Cisco Catalyst IW9165E provides one dedicated 2x2 5GHz Wi-Fi radio and a Dual Band (XOR) radio that serves both 5 GHz and 6 GHz 2x2 radio bands.

- Supports dedicated 5GHz Wi-Fi radio and Dual Band (XOR) radio for 5 GHz and 6 GHz bands.
- Allows switching between 5G and 6G bands.
- Admin state is disabled by default; Slot 2 XOR radio is fixed to 5G by default.

AP Radio Slots

To switch between 5G and 6G bands on the Catalyst IW9165E, use the following CLI command:

- `ap name <ap-name> dot11 dual-band band 6ghz/5ghz`

Note By default, admin state is disabled. Slot 2 XOR radio is fixed to 5G.

Table 10: AP Wi-Fi radio architecture modes

Mode	5 GHz Slot 1	5/6 GHz Slot 2
5G + 5G	5GHz 2x2:2SS (20/40/80 MHz)	5G 2x2:2SS (20/40/80/160 MHz)
5G + 6G	5GHz 2x2:2SS (20/40/80 MHz)	6G 2x2:2SS (20/40/80/160 MHz)

Supported fixed domains and country codes

The ROW regulatory domain simplifies the domain management of the manufacturing process for all the country codes that do not have a specific domain mapped.

Supported Fixed Domains

Domain	Country Codes
A	CA (Canada)
B	US (United States of America)

Domain	Country Codes
E	

Domain	Country Codes
	• AT (Austria) • AT (Austria) • BE (Belgium) • BG (Bulgaria) • HR (Croatia) • CY (Cyprus) • CZ (Czech Republic) • DK (Denmark) • EE (Estonia) • FI (Finland) • FR (France) • DE (Germany) • GR (Greece) • HU Hungary) • IS (Iceland) • IE (Ireland) • IT (Italy) • LV (Latvia) • LI (Liechtenstein) • LT (Lithuania) • LU (Luxembourg) • MT (Malta) • NL (Netherlands) • NO (Norway) • PL (Poland) • PT (Portugal) • RO (Romania) • SK (Slovak Republic) • SI (Slovenia) • ES (Spain) • SE (Sweden), and

Domain	Country Codes
	• CH (Switzerland).
F	ID (Indonesia)
Q	JP (Japan)
Z	• AU (Australia) and • NZ (New Zealand).

Catalyst IW9165 supported country codes (ROW)

Domain	Country Codes
ROW	• CL (Chile) • KR (Korea, Republic of) • GB (United Kingdom), and • VN (Vietnam).

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

Radio antenna settings

The Catalyst IW9165E radio antenna settings define how external antennas are connected and configured for optimal wireless performance.

- The device supports four external antennas with RP-SMA (f) connectors.
- Radio 1 connects to antenna ports 1 and 2; Radio 2 connects to antenna ports 3 and 4.
- The IW9165E is compatible with Self Identifiable Antenna (SIA) antennas for the 6G band, with ports 1 and 3 supporting SIA antennas.

Supported antenna types and port assignments

The Catalyst IW9165E supports a range of external antennas and provides specific port assignments for each radio. SIA antennas are supported on select ports for the 6G band.

- Four external antennas with RP-SMA (f) connectors
- Radio 1: Antenna ports 1 and 2
- Radio 2: Antenna ports 3 and 4

- SIA antennas supported on ports 1 and 3 for the 6G band
- Compatible SIA antennas: IW-ANT-OMV-2567-N and IW-ANT-OMH-2567-N

Comparison of antenna gain values for each slot is shown in this table.

Table 11: Antenna gain (dBm)

5 GHz Slot 1	5 GHz Slot 2	6 GHz Slot 2
3 4 7 8 10 13 15	3 4 7 8 10 13 15	7

Note A power cycle is mandatory after the first installation of the SIA antenna.

For more information on antennas, see the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Hardware Installation Guide .

This example demonstrates how to verify the SIA status on the controller using CLI commands. Run the **show ap config slots** <AP> command to display SIA information.

Device# show ap config slots AP2CF8.9B1C.CE78 Cisco AP Name : AP4C42.1E51.A144 Attributes for Slot 2 SIA Status : Present(RPTNC) SIA Product ID : IW-ANT-OMV-2567-N

AFC support for 6 GHz standard power mode

The 6 GHz Standard Power mode is a regulatory-compliant operational mode for access points (APs) that requires coordination through an Automated Frequency Coordination (AFC) system.

- Standard Power APs must obtain available frequencies and power levels from the AFC system before operation.
- The AFC system determines allowable frequencies and maximum power based on regulatory body data (such as FCC for the U.S.).
- Transmission power is limited to a maximum of 36 dB EIRP, and APs are permitted in UNII-5 and UNII-7 bands in the -B (U.S) domain.

Standard power mode operation and deployment

The Cisco Catalyst IW9165E supports AFC 6 GHz Standard Power mode, enabling APs to operate in outdoor environments with regulatory compliance. The AFC system computes available frequencies and power, and coordinates AP operation to avoid interference.

Table 12: Radio 6 GHz Power Mode Support

AP Deployment Mode	6G Deployment Mode	Low-power Indoor Support	Standard Power Support
Indoor AP	Outdoor	No	Yes

Table 13: 6 GHz Target Power

Max Conducted per Path Power (SP/AFC)		Antenna Gain	Tx x Rx Chains	Max EIRP (SP/AFC)
20-80Mhz	**160Mhz**			
17 dBm	17 dBm	7 dBi	2x2	27 dBm

Verify AFC status on an AP

This procedure describes how to verify the AFC request and response data, as well as the current operating power mode, on an AP using commands.

Procedure

Step 1 Use the **show rrm afc** command to verify the AFC request and response data on the AP.

Example:

```
Device# show rrm afc

Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor axis:
9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

Step 2 Use the **show controllers dot11Radio 2 | i Radio** command to verify the current operating power mode.

Example:

```
Device# show controllers dot11Radio 2 | i Radio
Dot11Radio2     Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

GNSS support

Global Navigation Satellite System (GNSS) is supported on IW9165E. The AP tracks GPS information for devices deployed in the outdoor environment and sends the GNSS information to the wireless controller.

You can use this command to display the GNSS information on the AP:

```
AP# show gnss info
```

You can use these command to display the GPS location of the AP:

```
Controller# show ap geolocation summary
```

```
Controller# show ap name <Cisco AP> geolocation detail
```

Antenna disconnection detection

Antenna Disconnection Detection is a feature that monitors the signal strength delta across antennas on an access point to identify impaired or disconnected antennas.

- Improves performance and reliability by using multiple antennas for better signal reception.
- Detects antenna issues based on signal strength differences exceeding a defined threshold for a specific duration.
- Notifies the system through IAPP messages and controller logs when an antenna issue is detected.

How Antenna Disconnection Detection Works

Multiple antennas on the transmitter and receiver of an access point (AP) enhance performance and reliability by selecting or combining the strongest signals. Detecting an impaired or physically broken antenna is critical to AP reliability.

The Antenna Disconnection Detection feature operates by monitoring the signal strength delta across the antennas on the receiver. If the delta exceeds a defined limit for a specific duration, the antenna is flagged as having issues.

- Improved reception through antenna diversity.
- Critical detection of antenna impairment or breakage.
- Automated notification via IAPP messages and controller logs.

For more information about configuring Antenna Disconnection Detection on the Wireless Controller, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .

Verify Antenna Disconnection Detection on an AP or AP Profile

This procedure describes how to ensure that APs are operating with properly connected antennas. Verifying this configuration can help diagnose connectivity or coverage issues.

Procedure

Step 1 Use the **show ap name***ap-name* **config general** command to verify the configuration on an AP.

Example:

```
Conroller# show ap name AP4C42.1E51.A144 config general

Cisco AP Name   : AP4C42.1E51.A144
================================================
Cisco AP Identifier                             : 8c84.4292.f840
Country Code                                    : Multiple Countries : US,CN,GB,HK,DE,IN,CZ,NZ
Regulatory Domain Allowed by Country            : 802.11bg:-ACE^   802.11a:-ABCDEHNSZ^   802.11
6GHz:-BEZ^
Radio Authority IDs                             : None
AP Country Code                                 : CZ  - Czech Republic
AP Regulatory Domain
802.11bg                                      : -E
802.11a                                       : -E
MAC Address                                     : 8c84.4292.f840
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.33.3
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.33.1
Fallback IP Address Being Used                  :
Domain                                          :
Name Server                                     :
CAPWAP Path MTU                                 : 1485
Capwap Active Window Size                       : 1
```

Step 2 Use the **show ap profile name***ap-profile* **detailed** command to verify th detailed configuration parameters of a specific access point profile on the controller.

Example:

```
Controller# show ap profile name ap-profile detailed

AP Profile Name: ap-profile
.
.
.
AP broken antenna detection:
Status                                                  : ENABLED
RSSI threshold                                          : 40
Weak RSSI                                               : -80
Detection Time                                          : 120
```

Troubleshooting

The document provides use cases to understand the reason for the Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) tunnel break between Access Points (APs) and the Wireless Controller.

For more information, see Troubleshoot Access Point Disassociation from Controller

Note There could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

Feedback request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the Feedback button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

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.