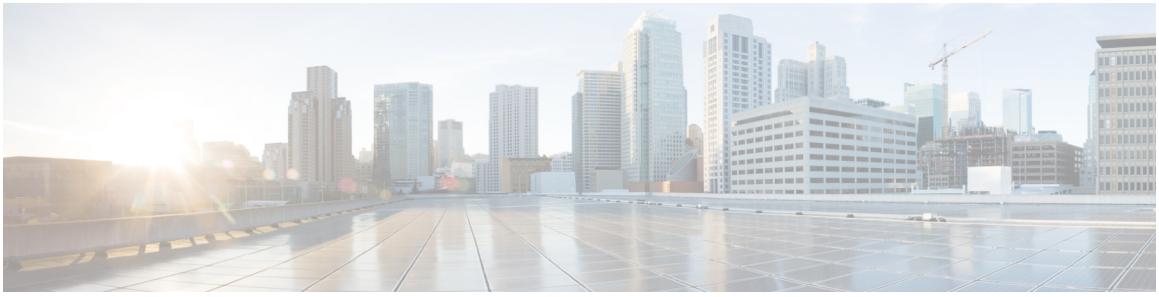


Cisco Catalyst IW9165 Rugged Series Configuration Guide, Release 17.13.x

First Published: 2023-12-15

Last Modified: 2025-05-15

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

Overview of the Access Point 1

Connect to the Access Point Console Port 1

Related Documentation 2

CHAPTER 2 **Workgroup Bridge** 3

Workgroup Bridge 3

WGB mode recommendations 4

uWGB mode recommendations 4

Guidelines to reset the login credentials 5

Configure WLAN and policy profiles for WGB association 6

Upgrade the uWGB image 7

WGB configuration 8

Configure a Dot1X credential 9

Deauthenticate WGB wired client 9

Configure an EAP profile 9

Configure trustpoint manual enrollment for terminal 10

Configure trustpoint auto-enrollment for WGB 12

Configure manual certificate enrollment using TFTP server 13

Configure a PKCS12 or PFX or P12 certificate enrollment using a TFTP server 14

Verify PKCS12 or PFX or P12 certificate enrollment for WGB mode 14

SSID configuration 15

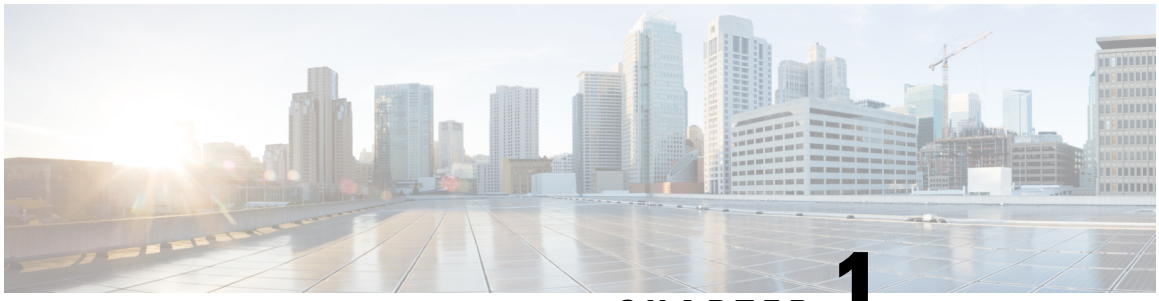
Create an SSID profile 15

Configure radio interface for WGB 16

Configure WGB or uWGB timer 16

uWGB Configuration 17
Configure a Dot1X credential 17
Configure an EAP profile 17
Configure trustpoint manual enrollment for terminal 18
Configure trustpoint auto-enrollment for WGB 20
Configure manual certificate enrollment using TFTP server 21
SSID configuration 22
Create an SSID profile 22
Configuring Radio Interface for uWGB 23
Configure IP address 23
Configure IPv4 address 23
Configure IPv6 address 24
Syslog 24
Conversion between WGB and uWGB modes 25
LED pattern 25
Configure transmission rate with high throughput for WGB 26
Radio Statistics Commands 27
Event Logging 29
802.11v features 30
Configure aux scanning 31
Scanning only mode 31
Aux-Scan handoff mode 32
Layer 2 NAT 33
Configuration Example of Host IP Address Translation 34
Configuration Example of Network Address Translation 36
Native VLAN on Ethernet Ports 36
Low latency profile 37
Configuring WGB optimized-video EDCA Profile 37
Configuring WGB optimized-automation EDCA Profile 37
Configuring WGB customized-wmm EDCA profile 38
Configuring Low Latency Profile on WGB 38
Configure EDCA parameters using Controller GUI 39
Configuring EDCA Parameters (Wireless Controller CLI) 40
Configuring A-MPDU 41

Import and export WGB configuration 41
Verify the WGB and uWGB configuration 42



CHAPTER 1

Introduction

- Overview of the Access Point, on page 1
- Connect to the Access Point Console Port, on page 1
- Related Documentation, on page 2

Overview of the Access Point

The Cisco Catalyst IW9165E Rugged Access Point and Wireless Client (hereafter referred to as *IW9165E*) is designed to add ultrareliable wireless connectivity to moving vehicles and machines. The IW9165E can operate as Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) starting from Cisco Unified Industrial Wireless Software Release 17.12.1, which delivers high availability, low latency, and zero packet loss with seamless handoffs.

Starting from Cisco Unified Industrial Wireless Software Release 17.13.1, the IW9165E can also operate as a Wi-Fi client in Workgroup Bridge (WGB) mode, which allows it to connect to a Cisco access point infrastructure, and Universal WGB (uWGB) mode, which allows it to connect to a third-party access point infrastructure. Both of these modes help bridge the wired clients that are behind the WGB to the access point on the infrastructure side.

This document covers configuration of WGB and uWGB mode specific to the IW9165E access points.

Connect to the Access Point Console Port

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

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

Parameter	Value
Baud rate	115200 bps
Data	Eight bits

Parameter	Value
Parity	No
Stop	One stop bit
Flow Control	No

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

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

   Use these default credentials to log in:

   - Username: Cisco
   - Password: Cisco

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

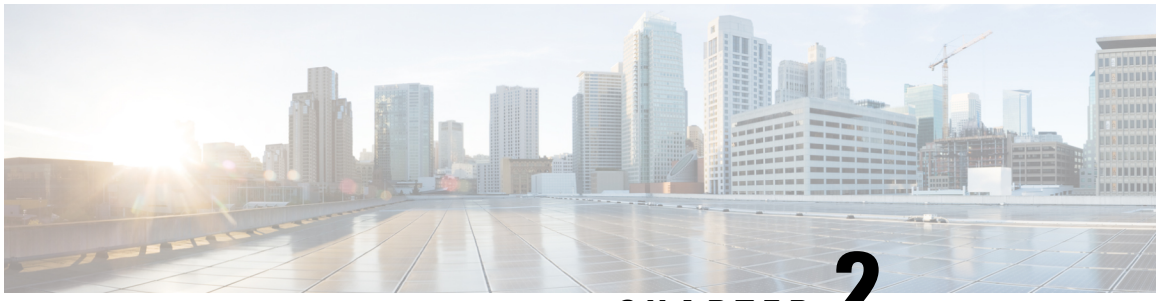
Related Documentation

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 the following 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.



CHAPTER 2

Workgroup Bridge

- Workgroup Bridge, on page 3
- WGB mode recommendations, on page 4
- uWGB mode recommendations, on page 4
- Guidelines to reset the login credentials, on page 5
- Configure WLAN and policy profiles for WGB association, on page 6
- Upgrade the uWGB image, on page 7
- WGB configuration, on page 8
- uWGB Configuration, on page 17
- Configure IP address, on page 23
- Syslog, on page 24
- Conversion between WGB and uWGB modes, on page 25
- LED pattern, on page 25
- Configure transmission rate with high throughput for WGB , on page 26
- Radio Statistics Commands, on page 27
- Event Logging, on page 29
- 802.11v features, on page 30
- Configure aux scanning, on page 31
- Layer 2 NAT, on page 33
- Native VLAN on Ethernet Ports, on page 36
- Low latency profile, on page 37
- Import and export WGB configuration, on page 41
- Verify the WGB and uWGB configuration, on page 42

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 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 APs.
- Speed and duplex settings are automatically negotiated based on the locally connected endpoint's capabilities. These settings cannot be manually configured on the AP's wired 0 and wired 1 interfaces.
- 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 wired client's IP address, 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, and
  - web authentication.
- A WGB cannot associate with a WLAN configured with adaptive 802.11r.

IPv6 and IPv4 support

- The WGB supports IPv6 traffic exclusively for wired clients, even though IPv4 is enabled.
- IPv6 management for the WGB does not function properly, even if the WGB successfully associates with an uplink. IPv6 pings and SSH to the WGB management IPv6 address do not work.

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 1: 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 (*).

Configure WLAN and policy profiles for WGB association

For a WGB to join a wireless network, configure these settings on the WLAN and the related policy profile on the controller.

Follow these steps to configure the Cisco Client Extensions option and set the support for the Aironet IE in the WLAN:

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

   ```
   Device#wlan profile-name
   ```

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

2. Use the **ccx aironet-iesupport** command to configure the Cisco Client Extensions option and set the Aironet IE support on the WLAN.

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

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

Configure WLAN policy profile for WGB

1. Use the **wireless profile policy** *profile-policy* command to enter the wireless policy configuration mode.

   ```
   Device#wireless profile policy profile-policy
   ```

2. Use the **vlan** *vlan-id* command to assign the profile policy to the VLAN.

   ```
   Device#vlan vlan-id
   ```

3. Use the **wgb vlan** command to configure WGB VLAN client support.

   ```
   Device#wgb vlan
   ```

Upgrade the uWGB image

To upgrade the uWGB software image by converting it to WGB mode, performing the upgrade, and reverting it back to uWGB mode. The process requires using TFTP or SFTP protocols for the software download.

Before you begin

The uWGB mode does not support TFTP or SFTP protocols for image upgrades. Therefore, the device must first be converted to WGB mode to enable the image upgrade process.

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 slot_id disable
```

Step 3 Convert uWGB to WGB mode.

Use the **configure Dot11Radio** *slot_id* **mode wgb ssid-profile** *ssid_profile_name* command to reboot the device with the downloaded configuration.

```
Device#configure Dot11Radio slot_id mode wgb ssid-profile ssid_profile_name


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

Note
Replace *ssid_profile_name* with any existing configured SSID profile.

Step 4 When the device reboots, assign a static IP address to the WGB.

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

```
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 view the ICMP ping results to the server.

```
Device#ping server_IP
```

Example:

```
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 upgrade the uWGB software.

```
Device#archive download/reload <tftp | sftp | http >://server_ip /file_path
```

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

```
Device#configure Dot11Radio slot_id mode uwgb wired_client_mac_addr ssid-profile ssid_profile_name
```

WGB configuration

Perform these tasks for WGB configuration:

1. Create an SSID profile.
2. Configure the radio in WGB mode, and associate the SSID profile with the radio.
3. Turn on the radio.

WGB uplink supports various security methods, which includes:

- Open (unsecured)
- Pre-shared key (PSK), and
- Dot1x (LEAP, PEAP, FAST-EAP, and TLS).

Note Ensure that the below configuration order is followed when EAP-TLS security is desired on the WGB:

1. Configure the device username/password, NTP server, hostname, and valid IP address.
2. Create trustpoints and import the certificates using your preferred method.
3. (Optional) Configure the dot1x credentials.
4. Create the EAP profile and map the method, trustpoint name and dot1x credentials (optional).
5. Bind the EAP profile to the SSID profile.
6. Bind the SSID profile to the preferred radio.

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 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 <ssid_prof_name> ssid <ssid name> authentication eap profile
 <eap_prof_name> key-management <key_type>
```

Dot1x FAST-EAP configuration example

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 1 mode wgb ssid-profile demo-FAST
configure dot11radio 1 enable
```

These sections provide detailed information on the WGB configuration procedure.

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

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

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 an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

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

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

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 profile-name trustpoint { default | name trustpoint-name}
```

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

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

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

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 9 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 trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

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.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the 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.

```
Device#configure crypto pki trustpoint ca-server-name 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.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

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

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

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

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

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 in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

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

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 8 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 trustpoint-name 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 PKCS12 or PFX or P12 certificate enrollment for WGB mode

Procedure

Perform this task to ensure that the PKCS12 certificate is successfully downloaded and properly enrolled for WGB mode.

Use the `show crypto pki trustpoint` command to verify the downloaded PKCS12 certificate.

Example:

```
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
```

SSID configuration

Perform these tasks to configure SSID.

Create an SSID profile

Choose one of these authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

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 ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of these authentication protocols to configure an SSID profile using PSK authentication:

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using Dot1x authentication

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 ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configure radio interface for WGB

IW9165E does not have 2.4 GHz radio. You can configure only dot11radio 1 as uplink and operate in WGB mode.

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 ssid-profile-name
```

Enable radio interface for WGB

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

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

Note Use the **configure dot11radio** *slot_id* **disable** command to disable a radio interface.

Configure WGB or uWGB timer

The CLI commands for timer configuration are same for both WGB and uWGB modes. Use these commands to configure timer:

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

  ```
  Device#configure wgb association response timeout response-millisecs
  ```

  The default value is 100 milliseconds, and the valid range is between 100 and 5000 milliseconds.

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

  ```
  Device#configure wgb authentication response timeout response-millisecs
  ```

The default value is 100 milliseconds, and the valid range is between 100 and 5000 milliseconds.

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

  ```
  Device#configure wgb eap timeout timeout-secs
  ```

  The default value is 3 seconds, and the valid range is between 2 and 60 seconds.

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

  ```
  Device#configure wgb bridge client timeout timeout-secs
  ```

  The default timeout value is 300 seconds, and the valid range is between 10 and 1000000 seconds.

uWGB Configuration

The universal WGB is able to interoperate with non-Cisco access points using uplink radio MAC address, thus the universal workgroup bridge role supports only one wired client.

Most WGB configurations apply to uWGB. The only difference is that you configure wired client's MAC address with the following command:

configure dot11 <*slot_id*> **mode uwgb** <*uwgb_wired_client_mac_address*> **ssid-profile** <*ssid-profile*>

The following is an example of Dot1x FAST-EAP configuration:

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 1 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 1 enable
```

The following sections provide detailed information about uWGB configuration:

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

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

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.

3. Attach the SSID profile to the radio.

Procedure

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

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

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 profile-name trustpoint { default | name trustpoint-name}
```

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

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

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

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

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

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

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

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

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

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 9 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 trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

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.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the 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.

```
Device#configure crypto pki trustpoint ca-server-name 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.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

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

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

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

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

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

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

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 ca-server-name key-size key-length
```

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

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

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

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

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 in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

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

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

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

Step 8 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 trustpoint-name certificate
```

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 15
2. Configuring Radio Interface for uWGB, on page 23

Create an SSID profile

Choose one of these authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

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 ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of these authentication protocols to configure an SSID profile using PSK authentication:

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using Dot1x authentication

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 ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configuring Radio Interface for uWGB

IW9165E does not have 2.4 GHz radio. Only slot 1 (dot11radio 1) can be configured as uplink.

- Map a radio interface to a WGB SSID profile by entering this command:

  # **configure dot11radio 1 mode uwgb** *client-mac-address* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  # **configure dot11radio 1** { **enable** | **disable** }

  Example

  ```
  # configure dot11radio 1 disable
  ```

Configure IP address

Configure IPv4 address

- Use the **configure ap address** *ipv4 dhcp* command to configure IPv4 address using DHCP.

  ```
  Device#configure ap address ipv4 dhcp
  ```

- Use the **configure ap address** *ipv4 static ipv4_addr netmask gateway* command to configure the static IPv4 address. By doing so, you can manage the device using a wired interface without an uplink connection.

  ```
  Device#configure ap address ipv4 static ipv4_addr netmask gateway
  ```

Verify current IP configuration

Use **show ip interface brief** command to view the current IP address configuration.

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

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. This configuration allows you to manage the AP through a wired interface without uplink connection.

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

Enable IPv6 auto configuration

Use the **configure ap address ipv6 auto-config enable** command to enable the IPv6 auto configuration on the AP.

```
Device#configure ap address ipv6 auto-config enable
```

Note

- Use the **configure ap address ipv6 auto-config disable** command to disable the IPv6 auto configuration on the AP.
- Use the **configure ap address ipv6 auto-config enable** command to enable IPv6 SLAAC. Note that SLAAC does not apply to CoS of WGB. This command configures IPv6 address with DHCPv6 instead of SLAAC.

Configure IPv6 address using DHCP

Use the **configure ap address** *ipv6 dhcp* command to configure IPv6 address using DHCP.

```
Device#configure ap address ipv6 dhcp
```

Verify current IP configuration

Use the **show ipv6 interface brief** command to verify current IP address configuration.

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

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."

Conversion between WGB and uWGB modes

Conversion from WGB to uWGB mode

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 <radio_slot_id> mode uwgb <WIRED_CLIENT_MAC> ssid-profile
<SSID_PROFILE_NAME>
```

Conversion from uWGB to WGB mode

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 <SSID_PROFILE_NAME>

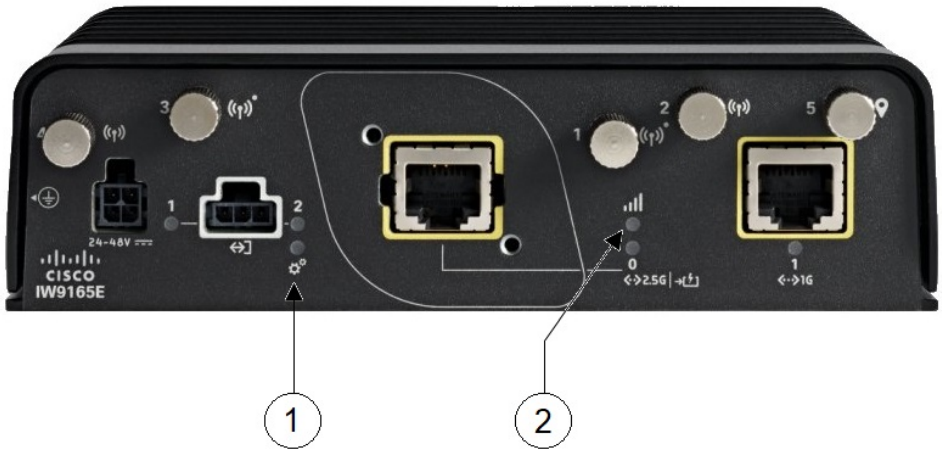
 This command will reboot with downloaded configs.
 Are you sure you want continue? [confirm]
```

LED pattern

There are two LEDs located at the front of AP panel:

- System status LED
- RSSI status LED

Figure 1: IW9165E LEDs



1	System status LED • Blinking Red: Indicates that the WGB is disassociated. • Solid green: Indicates that the WGB is associated with the parent AP.	2	RSSI status LED • Solid green: When the RSSI value is greater than or equal to -71 dBm. • Blinking green: When the RSSI value is between -81 dBm and -70 dBm. • Solid yellow: When the RSSI value is between -95 dBm and -81 dBm. • Off: For all other RSSI values.

Configure transmission rate with high throughput for WGB

When configuring WGB mode for moving deployments, you can manually configure the transmission rate limit using the high throughput (HT) modulation and coding scheme (MCS).

Example of WGB configuration with transmission rate of 802.11n HT m4. m5. rate:

Config dot11radio [**1**|**2**] **802.11ax disable**

Config dot11radio [**1**|**2**] **802.11ac disable**

Config dot11radio [**1**|**2**] **speed ht-mcs m4. m5.**

Note You can configure legacy rate using WGB.

Config dot11radio [**1**|**2**] **speed legacy-rate basic-6.0 9.0 12.0 18.0 24.0**

Both 802.11 management and control frames use legacy rates. The WGB's legacy rates should match or overlap with the AP's legacy rates; otherwise, the WGB association fails.

Use the **debug wgb dot11 rate** command to check WGB Tx MCS rate. Here is an example that shows 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
```

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
```

Event Logging

For WGB field deployment, event logging will collect useful information (such as WGB state change and packets rx/tx) to analyze and provide log history to present context of problem, especially in roaming cases.

You can configure WGB trace filter for all management packet types, including probe, auth, assoc, eap, dhcp, icmp, and arp. To enable or disable WGB trace, use the following command:

#**config wgb event trace** {**enable**|**disable**}

Four kinds of event types are supported:

- **Basic event**: covers most WGB basic level info message
- **Detail event**: covers basic event and additional debug level message
- **Trace event**: recording wgb trace event if enabled
- **All event**: bundle trace event and detail event

The log format is [*timestamp*] *module*:*level* <*event log string*>.

When abnormal situations happen, the eventlog messages can be dumped manually to memory by using the following show command which also displays WGB logging:

#**show wgb event** [**basic**|**detail**|**trace**|**all**]

The following example shows the output of **show wgb event all**:

```
APC0F8.7FE5.F3C0#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
```

Note It might take a long time to display the **show wgb event** command output in console. Using *ctrl+c* to interrupt the printing will not affect log dump to memory.

The following clear command erases WGB events in memory:

#**clear wgb event** [**basic**|**detail**|**trace**|**all**]

To save all event logs to WGB flash, use the following command:

#**copy event-logging flash**

The package file consists of four separate log files for different log levels.

You can also save event log to a remote server by using the following command:

#**copy event-logging upload** <**tftp** | **sftp** | **scp**>**:**`//A.B.C.D[/`*dir*`][/`*filename.tar.gz*`]`

The following example saves event log to a TFTP server:

```
APC0F8.7FE5.F3C0#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.
```

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.

Configure aux scanning

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

Scanning only mode

When slot 2 radio is configured as scanning only mode, slot 1 (5G) radio will always be picked as uplink. Slot 2 (5G) radio will keep scanning configured SSID based on the channel list. By default, the channel list contains all supported 5G channels (based on reg domain). The scanning list can be configured manually or learned by 802.11v.

When roaming is triggered, the algorithm looks for candidates from scanning table and skips scanning phase if the table is not empty. WGB then makes an assocaition to that candidate AP.

Configure scanning only mode

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

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

Manually configure the channel list

Use the **configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **add** command to manually add the channel to the channel list.

```
Device#configure wgb mobile station interface dot11Radio 1 scan <channel> [add|delete]
```

Note Use the **configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **delete** command to manually delete the channel from the channel list.

Configure scanning table timer

Use the **configure wgb scan radio 2 timeout***1500* command to adjust the timer. By default, candidate AP entries in scanning table are automatically removed in 1200 ms.

```
Device#configure wgb scan radio 2 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.

Verify scanning table

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
```

Aux-Scan handoff mode

An Aux-Scan 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 Aux-Scan 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	Aux-Scan only	Aux-Scan 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

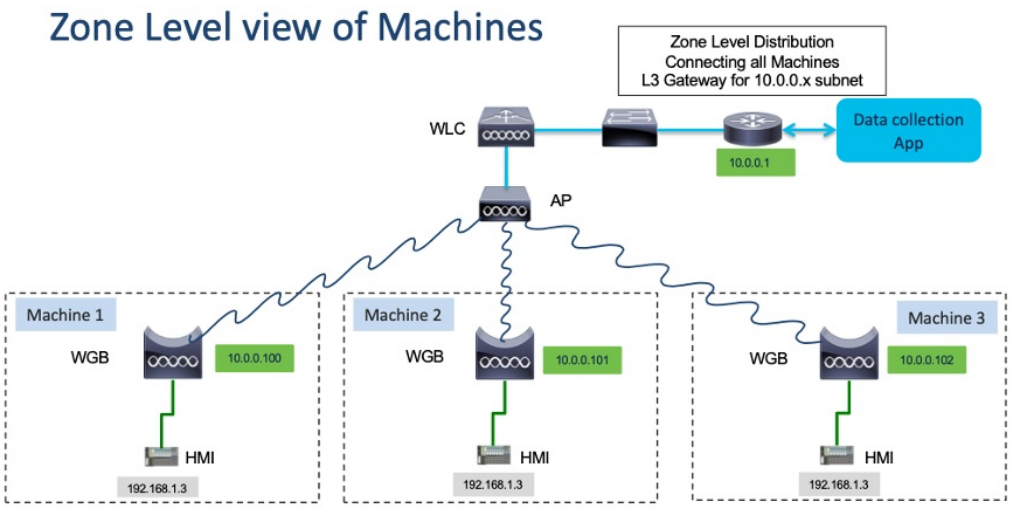
Layer 2 NAT

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:

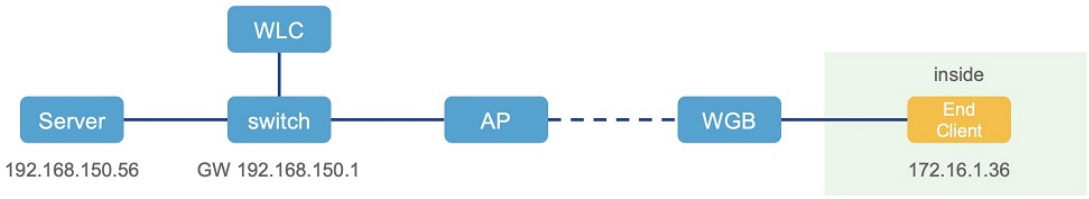
- private-to-public subnet translations
- public-to-private subnet translations

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.



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

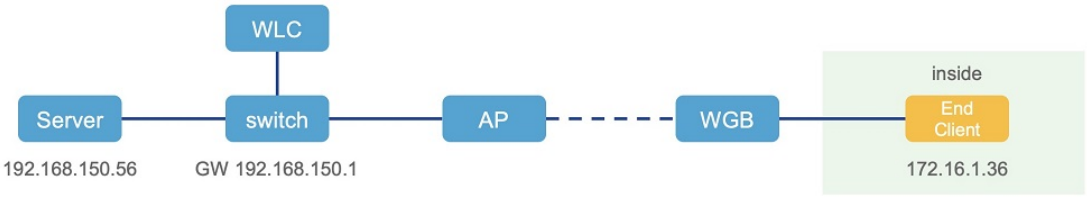
Direction          Original              Substitute            ARP  IP   ICMP UDP  TCP
inside-to-outside  172.16.1.1@2660       192.168.150.1@2660    1    4    4    0    0
inside-to-outside  172.16.1.36@2660      192.168.150.36@2660   3    129  32   90   1
inside-to-outside  172.16.1.56@2660      192.168.150.56@2660   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.

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.

Configuring WGB optimized-video EDCA Profile

To configure optimized low latency profile for video use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-video** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#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
```

Configuring WGB optimized-automation EDCA Profile

To configure optimized low latency profile for automation use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-automation** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#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
```

Configuring WGB customized-wmm EDCA profile

To configure customized Wi-Fi Multimedia (WMM) profile, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile customized-wmm** {**enable** | **disable**}

To configure customized WMM profile parameters, use the following command:

#**configure dot11Radio** {**0**|**1**|**2**} **wmm** {**be** | **vi** | **vo** | **bk**} {**cwmin** <*cwmin_num*> | **cwmax** <*cwmax_num*> | **aifs** <*aifs_num*> | **txoplimit** <*txoplimit_num*>}

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

Configuring Low Latency Profile on WGB

Use the following command to configure low latency profile on WGB:

AP# **configure dot11Radio** <*radio_slot_id*> **profile low-latency** [**ampdu** <*length*>] [**sifs-burst** {**enable** | **disable**}] [**rts-cts** {**enable** | **disable**}] [**non-aggr** <*length*>] [**aggr** <*length*>]

Use the following command to display iot-low-latency profile EDCA detailed parameters:

```
#show controllers dot11Radio 1 | beg EDCA
EDCA config
L: Local C:Cell A:Adaptive EDCA params
  AC   Type  CwMin  CwMax Aifs Txop ACM
AC_BE     L      4      6   11    0   0
AC_BK     L      6     10   11    0   0
AC_VI     L      3      4    1    0   0
AC_VO     L      0      2    0    0   1
AC_BE     C      4     10   11    0   0
AC_BK     C      6     10   11    0   0
AC_VI     C      3      4    2   94   0
AC_VO     C      2      3    1   47   1
```

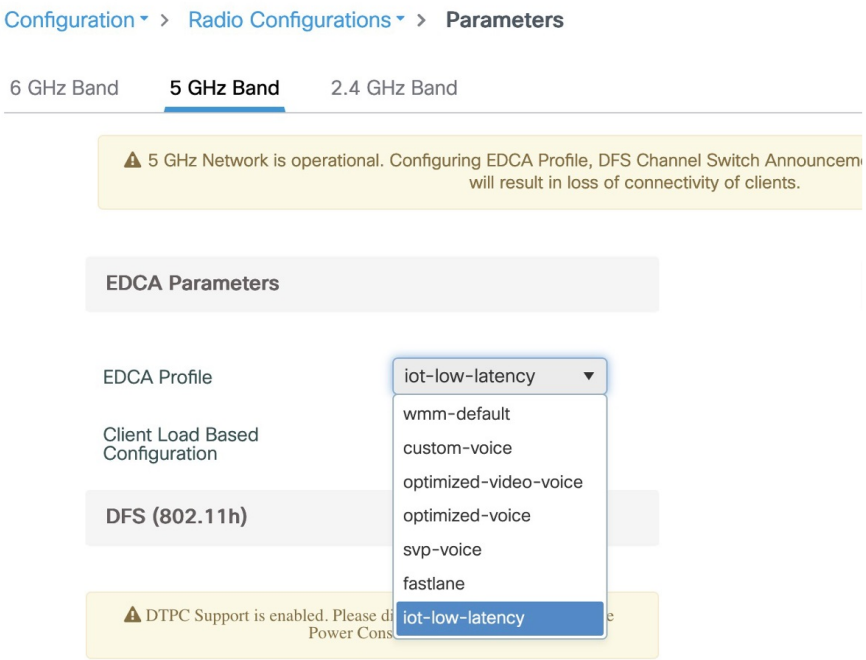
Configure EDCA parameters using Controller GUI

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters**. Using this page, you can 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 before you proceed.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.



Step 3 Click **Apply**.

Configuring EDCA Parameters (Wireless Controller CLI)

Procedure

Step 1 Enters global configuration mode.

configure terminal

Example:

```
Device# configure terminal
```

Step 2 Disables the radio network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

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

Step 3 Enables iot-low-latency EDCA profile for the 5 GHz, 2.4 GHz, or 6 GHz network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency**

Example:

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

Step 4 Enables the radio network.

no ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

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

Step 5 Returns to privileged EXEC mode.

end

Example:

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

Step 6 Displays the current configuration.

show ap dot11 {**5ghz** | **24ghz** | **6ghz**} **network**

Example:

```
Device(config)# show ap dot11 5ghz network
EDCA profile type check                  : iot-low-latency
```

Configuring A-MPDU

Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).

The A-MPDU parameters define the size of an aggregated packet and define the proper spacing between aggregated packets so that the receive side WLAN station can decode the packet properly.

To configure profiled based A-MPDU under 2.4G, 5G and 6G radio, use the following commands:

WLC(config)# **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** <*profile-name*>

WLC(config-rf-profile)# [**no**] **dot11n a-mpdu tx block-ack window-size** <*1-255*>

Global configuration is a special profile which can also be configured bu using the following command:

WLC(config)#[**no**] **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** <*1-255*>

To bind different RF profiles with the radio RF tag, use the following command:

WLC(config)# **wireless tag rf** <*rf-tag-name*>

WLC (config-wireless-rf-tag)# **5ghz-rf-policy** <*rf-profile-name*>

Note RF profile level configured **a-mpdu tx block-ack window-size** value takes preference over globally configured value.

To display configured a-mpdu length value, use the following command:

show controllers dot11Radio <*radio_slot_id*>

```
AP# show controllers dot11Radio 1
Radio Aggregation Config:
=========================

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

Import and export WGB configuration

Export WGB configuration

You can upload the current configuration of an existing WGB to a server and then you can download it for newly deployed WGBs.

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

```
Device#copy configuration upload <sftp:|tftp:> ip-address [directory] [file-name]
```

Import WGB configuration

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

```
Device#copy configuration download <sftp:|tftp:> ip-address [directory] [file-name]
```

Note When you execute the **copy configuration download** command, the AP starts to reboot. The new configuration takes effect only after the reboot.

Verify the WGB and uWGB configuration

Use the **show run** command to check whether the AP is in WGB mode or uWGB mode.

- WGB:

```
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
   Mode               : WGB
   Dot11 type         : 11ax
Radio Id              : NA
   Admin state        : NA
   Mode               : NA
```

- uWGB:

```
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
```

Use the **show wgb dot11 associations** command to view the WGB and uWGB configuration.

- WGB:

```
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
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:

```
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
```

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.