

Workgroup Bridges

- Cisco Workgroup Bridges, on page 1
- Non-Cisco Workgroup Bridges, on page 64
- Cisco Wave 2 Access Points as Workgroup Bridges, on page 65

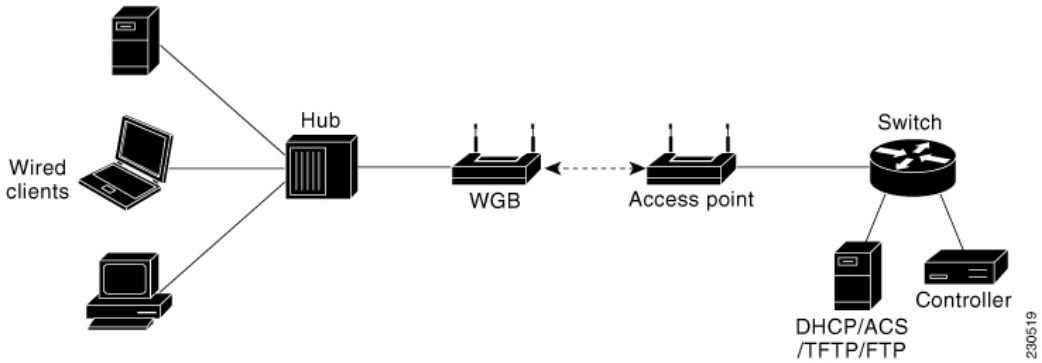
Cisco Workgroup Bridges

A workgroup bridge (WGB) is a Cisco access point that can be configured in a mode that permits it to associate with a wireless infrastructure, providing network access on behalf of wired clients. The WGB mode is supported on autonomous IOS (Wave 1) APs and on some Wave 2 APs.

A Cisco WGB provides information about its wired clients via Internet Access Point Protocol (IAPP) messaging. This enables the wireless infrastructure to know the MAC addresses of the WGB's wired clients. Up to 20 wired clients are supported behind a Cisco WGB.

In 8.10 release, the following APs support WGB operational mode: 2800, 3800, 4800, 1560 and 6300.

Figure 1: WGB Example



Note If the lightweight access point fails, the WGB attempts to associate to another access point.

- The following features are supported for use with a WGB:
  - Guest N+1 redundancy

  - Local EAP
  - Open, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, PEAP, and EAP-TLS authentication modes

- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.
- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must disable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

This section contains the following subsections:

Guidelines and Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with Cisco lightweight access points.
- Per-VLAN Spanning Tree (PVST) and packets are used to detect and prevent loops in the wired and wireless switching networks. WGB transparently bridge STP packets. WGB can bridge STP packets between two wired segments. Incorrect or inconsistent configuration of STP in the wired segments can cause WGB wireless link to be blocked by the connected switch(es) to Access Point or WGB. This could cause WGB to disconnect from AP or AP disconnection to Controller to drop, and wired clients not receiving IP addresses, as STP begins to block switch port in the wired network. If administrator needs to disable bridging of STP between the wired segments by the WGB, we recommend disabling the STP on the directly connected switches in the wireless network.
- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication
- Aironet WGBs are not supported if the parent AP is configured for FlexConnect local switching with local authentication, if the parent AP is a Wave 2 AP (that is, 802.11ac Wave 2 or 802.11ax). For more information, see CSCvh22645.
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- If a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the WGB to a large value using the following Cisco IOS commands on the WGB:

```
configure terminal
```

```
bridge bridge-group-number aging-time seconds
exit
end
```

where *bridge-group-number* is a value between 1 and 255, and *seconds* is a value between 10 and 1,000,000 seconds. We recommend configuring the *seconds* parameter to a value greater than the wired client's idle period.

- When you deauthenticate a WGB record from a controller, all of the WGB wired clients' entries are also deleted.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
  - Idle timeout
- The broadcast forwarding toward wired WGB clients works only on the native VLAN. If additional VLANs are configured, only the native VLAN forwards broadcast traffic.
- A WGB might be unable to connect in PSK with the controller. The output of the **debug client** command on the controller might show the following messages:

  ```
  *osapiBsnTimer: Oct 21 17:40:49.646: [PA] 70:6d:15:95:81:1c 802.1x
  'timeoutEvt' Timer expired for station 70:6d:15:95:81:1c and for message
  = M2

  *Dot1x_NW_MsgTask_4: Oct 21 17:40:49.646: [PA] 70:6d:15:95:81:1c
  Retransmit 1 of EAPOL-Key M1 (length 99) for mobile 70:6d:15:95:81:1c
  ```

  This is observed with a Cisco Wave 1 AP WGB, WPA2-PSK, and controller on Release 8.10.105.0 or a later release. This issue is fixed in autonomous IOS Release 15.3(3)JK1, 15.3(3)JPJ2, and later releases.

  The workaround is to configure PMK ID inclusion in M1 of 4-way handshake messages by entering this command: **config wlan security wpa akm psk pmkid** {**enable** | **disable**} *wlan_id*
- Associating a WGB to a WLAN that is configured for Adaptive 802.11r is not supported.

Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs

Release 8.3 provides an enhancement to broadcast traffic support on multiple 802.1Q VLAN workgroup bridge (WGB) deployments that traverse mesh networks and in Local mode. Specifically, support for WGB downstream broadcasts over multiple VLANs (to differentiate and prioritize traffic); and, bridging of VLAN traffic to wired clients connected to the WGB. Applications for this functionality are commonly found in the transportation and mining industries. For more information, see CSCub87583.

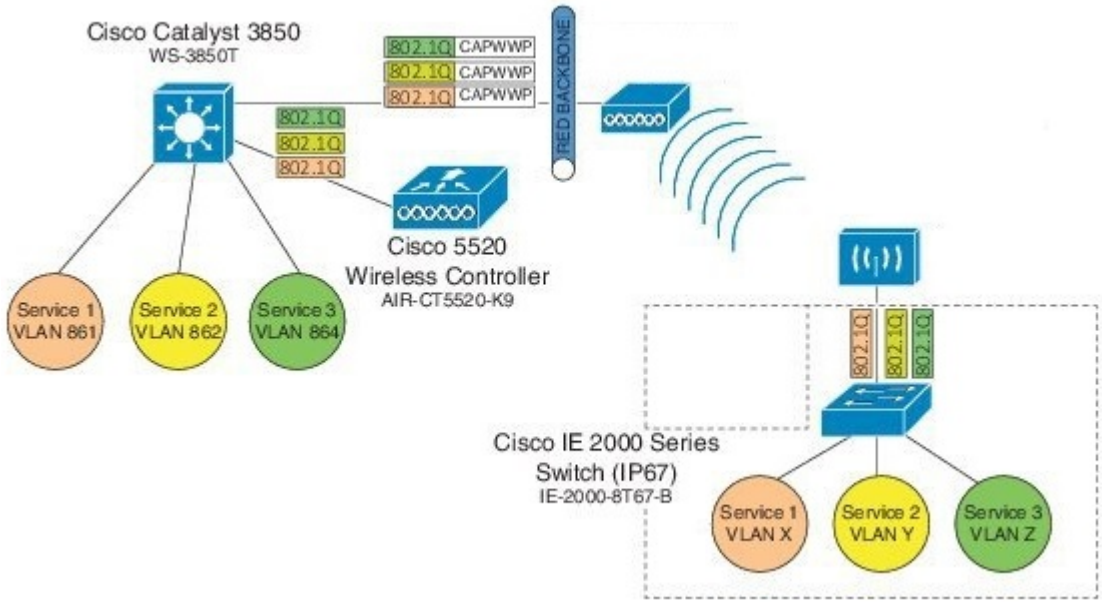
Supported platforms:

- Access point (AP) and WGB support:
  - IW3700 Series

Supported AP mode:

- Local mode
- Bridge mode

Figure 2: Workgroup Downstream Broadcast on Multiple VLAN



Prerequisites

You need to create the dynamic interfaces and bind them to the interface group before you proceed with the configuration.

1. Create the dynamic interfaces, by choosing **CONTROLLER** > **Interfaces** > **New** on controller. Add any dynamic interface that needs to support the downstream broadcast on Multiple VLANs feature into the interface group.
2. Bind the dynamic interfaces with Interface Groups, by choosing **CONTROLLER** > **Interface Groups** > **Add Group** on controller.
3. Bind the Interface Groups to WLAN. Choose **WLAN**. Under the specific WLAN General confirmation tab, choose the proper interface group.

Cisco Wireless Controller Configuration (CLI Only)

To enable or disable the downlink broadcast packet VLAN tagging on a WLAN (new command):

`(Cisco Controller) >`**config wlan wgb broadcast-tagging** {**enable** | **disable**} *wlan-id*

Note This feature is disabled by default.

Note To enable this feature, you need to enable **Broadcast Forwarding** on controller, by choosing **Controller** > **General** and choose **Enabled** from the **Broadcast Forwarding** drop-down list.

Note To enable this feature, you should also configure the AP Multicast Mode to Multicast rather than Unicast, by clicking **Controller** > **General** > **AP Multicast Mode** and choosing **Multicast**, and then assign Multicast Group Address.

WGB Configuration (CLI Only)

You can configure the following on Workgroup Bridges:

- Broadcast Tagging
- Native VLANs

By default, Broadcast Tagging is disabled.

By default, only Native VLAN broadcasts can be forwarded to wired clients in Native VLANs.

You use the no command to disable VLAN configurations on the WGB as shown in the examples below.

Note When you have multiple VLAN configurations on WGB, you need to configure the encryption cipher mode and keys as the following example shows:

```
encryption vlan 861 mode ciphers aes-ccm
encryption vlan 862 mode ciphers aes-ccm
encryption vlan 864 mode ciphers aes-ccm
```

Then, you should configure the encryption cipher mode globally on the multicast or broadcast interface by entering the following command:

```
encryption mode ciphers aes-ccm
```

VLAN Broadcast Tagging Configuration

- To enable broadcast tagging on a VLAN (new command):

  `(WGB) (config)#`**workgroup-bridge unified-vlan-client broadcast-tagging**

- To disable broadcast tagging on a VLAN:

  `(WGB) (config)#`**no workgroup-bridge unified-vlan-client broadcast-tagging**

Note The **no workgroup-bridge unified-vlan-client broadcast-tagging** command will disable **workgroup-bridge unified-vlan-client** as well. Make sure you have **workgroup-bridge unified-vlan-client** configured properly to enable the multiple vlan feature.

Reliable Transmission of Downstream Broadcast and Multicast with Multiple VLAN Support

The support of Workgroup Bridge (WGB) downstream broadcast on multiple VLAN was first introduced in Release 8.3 for IOS AP in local mode and bridge mode. Cisco Wireless Controller Release 8.10.121.0 provides an enhancement for reliable downstream multicast and broadcast for COS AP in local, flexconnect, bridge, and flexconnect+bridge mode, and supports both IOS and COS WGBs. Release 8.10.130.0 provides the enhancement for reliable downstream broadcast for IOS AP in local and bridge mode, and supports both IOS and COS WGBs.

The following sections describe detailed information and configuration guidelines for different platforms. Please see specific section based on your AP and WGB platform and controller software release version:

- For IOS AP and minimum software Release 8.3, refer to Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs, on page 3.
- For COS AP and minimum software Release 8.10.121.0, refer to Reliable WGB Downstream Multicast and Broadcast on Multiple VLANs, on page 6.
- For IOS AP and minimum software Release 8.10.130.0, refer to Reliable WGB Downstream Broadcast for Multiple VLANs, on page 20.

Reliable WGB Downstream Multicast and Broadcast on Multiple VLANs

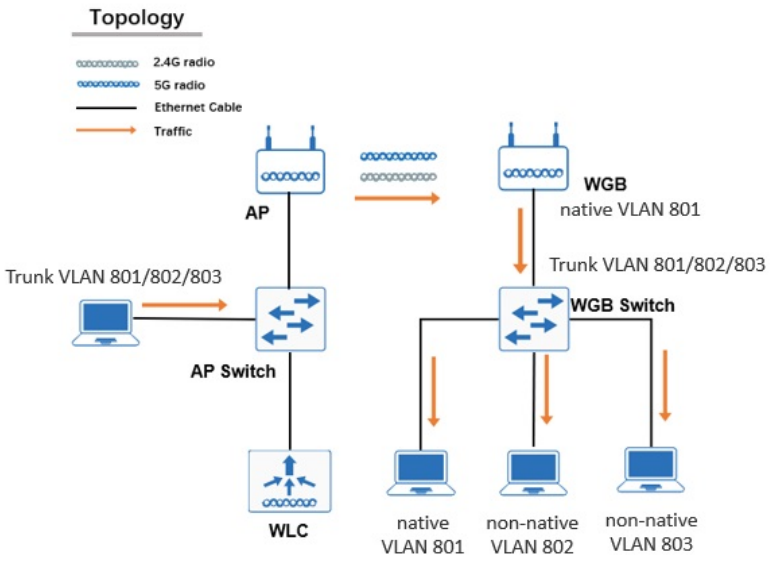
Release 8.10.121.0 provides a software enhancement for downstream multicast and broadcast targeted for WGB with different VLAN wired clients. Such kind of applications include product lines in manufacture field, autopilot in fleet vehicles, and etc. Less loss of broadcast and multicast is required for these deployments.

Legacy multicast or broadcast without 802.11 ACK mechanism's retransmission will lead to packet loss. With reliable downstream multicast and broadcast feature, they can be converted to unicast packet with retransmission.

Note This enhancement is for WGB and its wired clients. It will not impact the non-WGB wireless clients.

As shown in the following figure, a WGB with wired clients of three different VLANs (VLAN 801, 802, and 803) joins the AP wireless network. The broadcast and multicast traffic from AP to WGB will be transmitted to the clients with corresponding VLAN and retransmission will happen if traffic is lost on air.

Figure 3: WGB Bridged Network



- Supported AP platforms:
  - Cisco Catalyst IW6300 Heavy Duty Series Access Points
  - Cisco 6300 Series Embedded Services Access Points
- Supported WGB platforms:
  - Cisco Catalyst Industrial Wireless 6300 Series Access Points
  - Cisco 6300 Series Embedded Services Access Points
  - Cisco Industrial Wireless 3700 Series Access Points
- Supported AP modes:
  - Local
  - Flexconnect
  - Bridge
  - Flexconnect+ bridge

Note Non-native VLAN WGB wired client is not supported by flexconnect+bridge MAP.

The following figures illustrate an example of 802.11 packet forwarding from VLAN 801(0x321). The receiver address changes from FF:FF:FF:FF:FF:FF to the MAC address of WGB Radio (dc:8c:37:35:b2:6f), and the destination address changes from FF:FF:FF:FF:FF:FF to 01:00:5E:80:03:21 (the last two bytes in MAC address represents corresponding VLAN in hexadecimal). The new packet is a 802.11e QoS data.

Figure 4: Normal Broadcast Packet

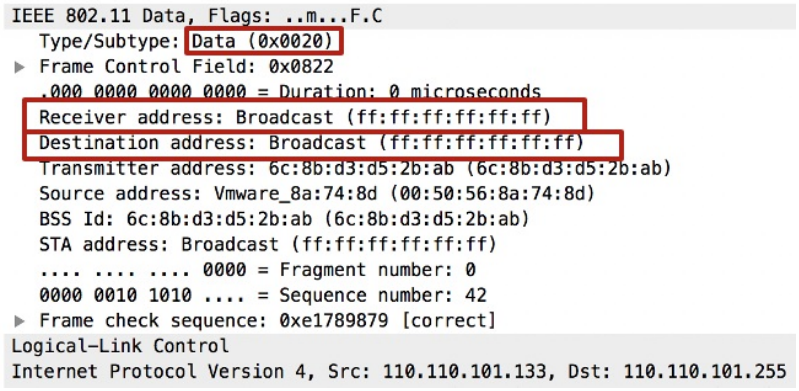
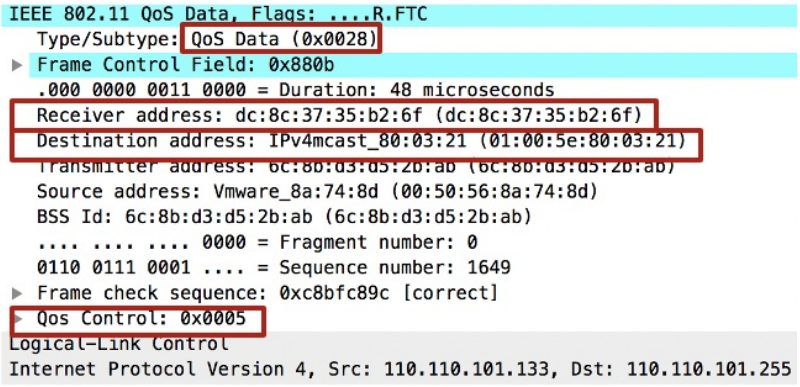


Figure 5: Reliable Broadcast Packet



The following figures illustrate an example of MC2UC packet to 226.6.6.9. The receiver address changes to the MAC address of WGB Radio (dc:8c:37:35:b2:6f), and the destination address is 01:00:5E:06:06:09. The new packet is a 802.11e QoS data.

Figure 6: Normal Multicast Packet

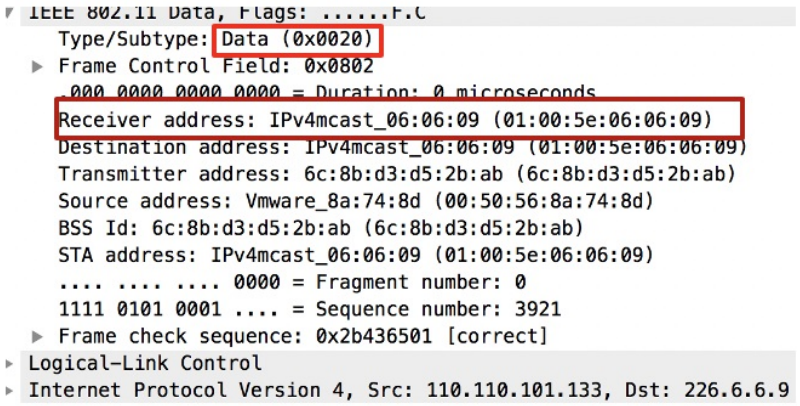
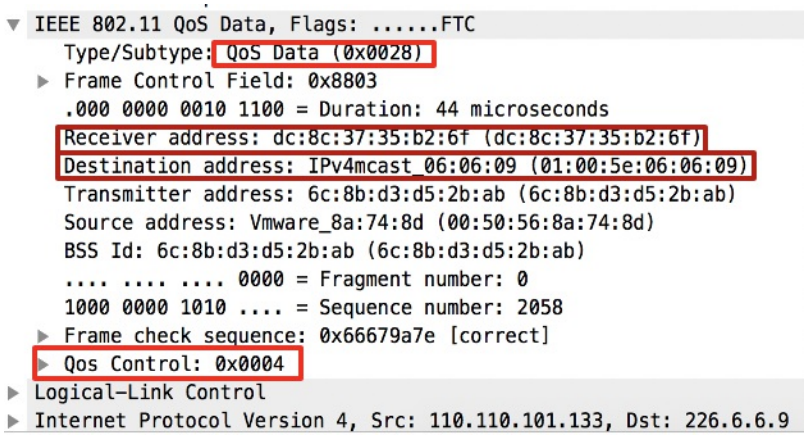


Figure 7: Reliable Multicast Packet



QoS Behavior

The QoS attribute is a new field for reliable broadcast and multicast traffic, which is defined in 802.11e.

- The 802.11e QoS priority of reliable broadcast packets will follow default multicast default priority value from WLAN's QoS configuration.
- The 802.11e QoS priority of reliable multicast packets will follow the original MC2UC behavior.
  - When AP is in local mode, the max priority is video.
  - When AP is in flexconnect mode and WLAN is local switching, the priority will always be 4, which belongs to the Video category.

The following QoS mapping tables show examples for different scenarios.

1. Local Mode AP While MC2UC is Enabled.

   Reliable broadcast will follow multicast default priority, while reliable multicast will follow the original max priority to video.

Table 1: QoS Mapping Table 1 - Local Mode AP While MC2UC is Enabled

Quality of Service (QoS) configured on WLAN	WLAN QoS Parameters Configured on Wireless>QoS>Profiles>platinum			802.11 QoS Data capture on the air QoS Control Priority value	
	Maximum Priority	Unicast Default Priority	Multicast Default Priority	Broadcast	Multicast
Platinum (voice)	Voice	Voice	Voice	Voice	Video
Platinum (voice)	Voice	Voice	Video	Video	Video

Quality of Service (QoS) configured on WLAN	WLAN QoS Parameters Configured on Wireless>QoS>Profiles>platinum			802.11 QoS Data capture on the air QoS Control Priority value	
Platinum (voice)	Voice	Voice	Best effort	Best effort	Best effort
Platinum (voice)	Voice	Voice	background	background	background

2. Flexconnect mode + Local Switching While MC2UC is Enabled.

   Reliable broadcast will follow multicast default priority. Reliable multicast will follow the original MC2UC default priority, UP (User Priority) value is 4, which belongs to Video Category.

Table 2: QoS Mapping Table 2 - Flexconnect mode + Local Switching While MC2UC is Enabled

Quality of Service (QoS) configured on WLAN	WLAN QoS Parameters Configured on Wireless>QoS>Profiles>platinum			802.11 QoS Data capture on the air QoS Control Priority value	
	Maximum Priority	**Unicast Default Priority**	**Multicast Default Priority**	**Broadcast**	**Multicast**
Platinum (voice)	Voice	Voice	Voice	Voice	Video
Platinum (voice)	Voice	Voice	Video	Video	Video
Platinum (voice)	Voice	background	Best effort	Best effort	Video
Platinum (voice)	Voice	background	background	background	Video

3. Local/Flex Mode AP While MC2UC is Disabled.

   Reliable broadcast will follow multicast default priority. As MC2UC is disable, multicast is data packet without QoS attribute.

Table 3: QoS Mapping Table 3 - Local/Flex Mode AP While MC2UC is Disabled

Quality of Service (QoS) configured on WLAN	WLAN QoS Parameters Configured on Wireless>QoS>Profiles>platinum			802.11 QoS Data capture on the air QoS Control Priority value	
	Maximum Priority	**Unicast Default Priority**	**Multicast Default Priority**	**Broadcast**	**Multicast**

Quality of Service (QoS) configured on WLAN	WLAN QoS Parameters Configured on Wireless>QoS>Profiles>platinum			802.11 QoS Data capture on the air QoS Control Priority value	
Platinum (voice)	Voice	Voice	Voice	Voice	\
Platinum (voice)	Voice	Voice	Video	Video	\
Platinum (voice)	Voice	Voice	Best effort	Best effort	\
Platinum (voice)	Voice	Voice	background	background	\

Controller Configuration

Reliable broadcast from AP to WGB is enabled by default. For AP in central switching, broadcast forwarding should be enabled on the controller. For AP in local switching, broadcast forwarding should be disabled on controller.

To support reliable multicast, MediaStream (Multicast to Unicast, MC2UC) should be enabled on controller. MC2UC is for downstream multicast service, by which AP can convert multicast packet to unicast packet and send it to each wireless client. For more information of MC2UC, refer to https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112889-cuwns-vidstrm-guide-00.html.

This section provides the basic MC2UC configuration for AireOS/ME controller.

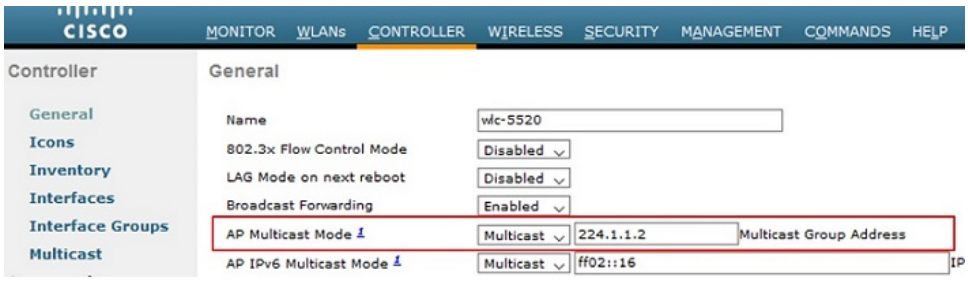
1. Enable WGB VLAN support on controller.

```
(Cisco Controller) > config wgb vlan enable
```

Figure 8:

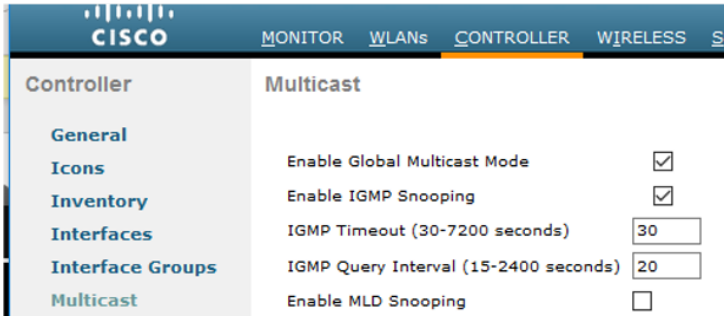
2. Enable multicast on controller. In this example, the multicast group address is 224.1.1.2.

```
(Cisco Controller) > config network multicast global enable
(Cisco Controller) > config network multicast mode multicast multicast_Group_Address
```



3. Enable multicast IGMP snooping. The IGMP timeout value is in the range of 30-7200 seconds. The IGMP query interval is in the range of 15-2400 seconds.

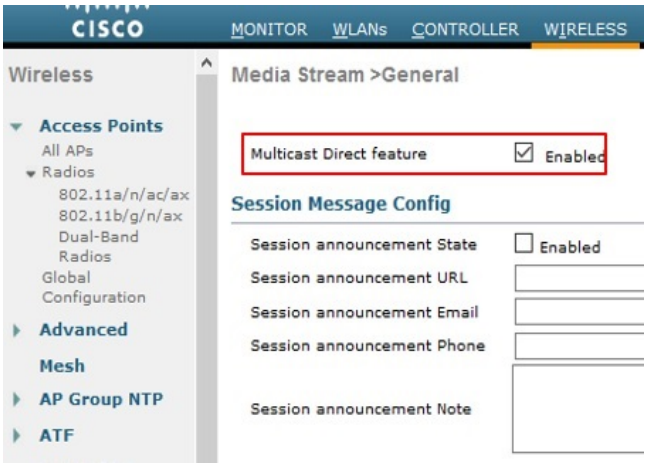
```
(Cisco Controller) > config network multicast igmp snooping enable
(Cisco Controller) > config network multicast igmp timeout time_out_vlaue
(Cisco Controller) > config network multicast igmp query interval Value
```



4. Enable multicast direct globally and set the general settings.

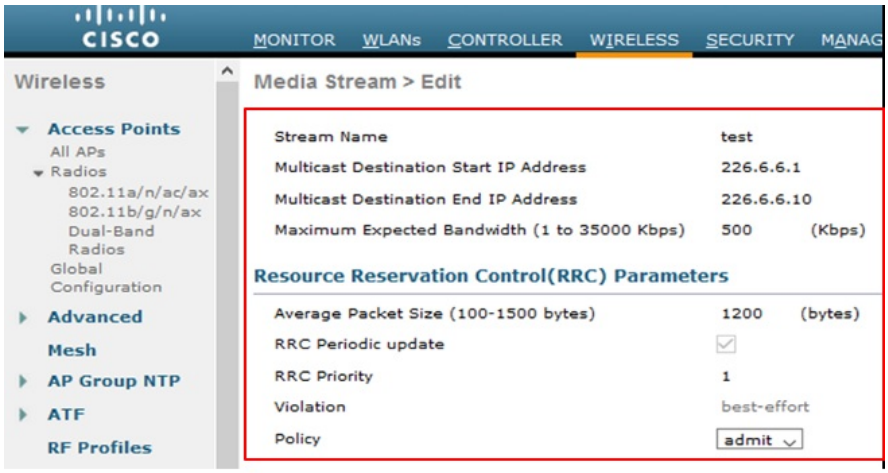
```
(Cisco Controller) >config media-stream multicast-direct enable
```

Note Media Stream Multicast-direct requires Load Based CAC to run. Voice deployment employing Static CAC needs to convert to Load Based CAC.



5. Define Media stream with RRC parameters.

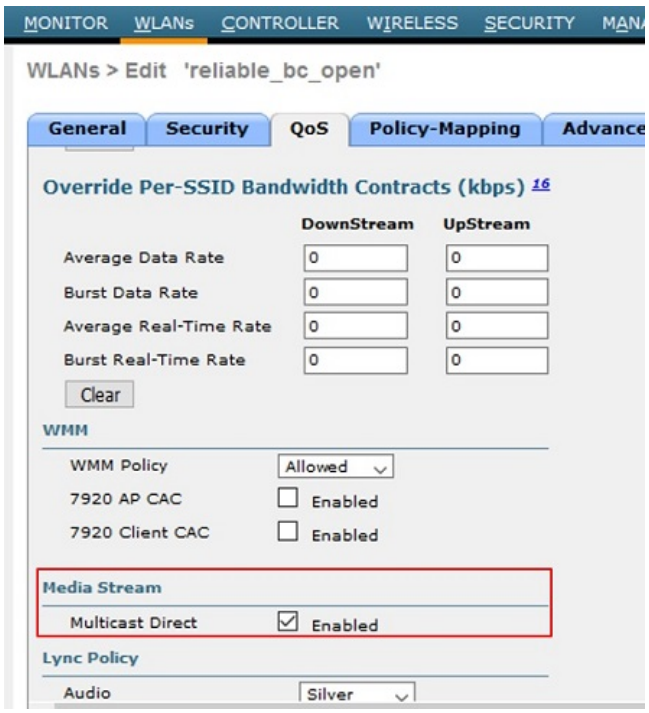
```
(Cisco Controller) >config media-stream add multicast-direct test  226.6.6.1 226.6.6.10
 detail  5000 1200 periodic video 1 fallback
```



6. (Optional) Configure Call Admission Control (CAC) for Media, Voice, and Video under radio. Refer to MC2UC guide for more information.

7. Enable Media Stream Multicast-direct for a WLAN.

```
(Cisco Controller) > config wlan media-stream multicast-direct 1 enable
```



8. Enable MC2UC feature support for WGB.

```
(Cisco Controller) > config media-stream wired-client enable
```

Note Media Stream Multicast-direct for WGB wired client will bypass admission control, which can cause the bandwidth calculation for video to be inaccurate.

9. Use the show command to check the configuration.

```
(Cisco Controller) > show media-stream group summary
```

```
(Cisco Controller) >show media-stream group summary

Stream Name   Start IP                          End IP                            Operation Status
------------ ---------------------------------- ---------------------------------- ----------------
test         226.6.6.1                         226.6.6.10                        Multicast-direct
```

```
(Cisco Controller) > show media-stream group detail test
```

```
(Cisco Controller) >show media-stream group detail test

Media Stream Name.............................. test
Start IP Address............................... 226.6.6.1
End IP Address................................. 226.6.6.10
 RRC Parmmeters
 Avg Packet Size(Bytes)........................ 1200
 Expected Bandwidth(Kbps)...................... 500
 Policy........................................ Admit
 RRC re-evaluation............................. periodic
 QoS........................................... Video
 Status........................................ Multicast-direct
 Usage Priority................................ 1
 Violation..................................... fallback
```

```
(Cisco Controller) > show 802.11a media-stream rrc
```

```
(Cisco Controller) >show 802.11a media-stream rrc


Multicast-direct............................... Enabled
Best Effort.................................... Disabled
Video Re-Direct................................ Enabled
Max Allowed Streams Per Radio.................. Auto
Max Allowed Streams Per Client................. Auto
Max Video Bandwidth............................ 0
Max Voice Bandwidth............................ 75
Max Media Bandwidth............................ 85
Min PHY Rate................................... 6000
Max Retry Percentage........................... 80
```

WGB Configuration

For broadcast traffic, 01:00:5e:80:xx:xx is introduced to transmit the VLAN information between AP and WGB.

- For COS WGB (IW6300 and ESW6300), a new CLI is introduced to forward the packets to the right VLAN when both reliable broadcast 01:00:5e:80:xx:xx and normal broadcast FF:FF:FF:FF:FF:FF are received:

  configure wgb broadcast tagging {**enable**|**disable**}

  WGB will received both FF:FF:FF:FF:FF:FF and 01:00:5e:80:xx:xx packets on the native VLAN. By default, this CLI is disabled. Both FF:FF:FF:FF:FF:FF and 01:00:5e:80:xx:xx packets will be received by the WGB and forwarded to the client. If this CLI is enabled, FF:FF:FF:FF:FF:FF packet will be dropped, and only 01:00:5e:80:xx:xx packet will be forwarded to the correct VLAN client.

- For IOS WGB (IW3702), to support multiple VLAN, the following CLI should be configured on WGB:

  WGB(config)#**workgroup-bridge unified-vlan-client**

  To forward the packet to the right VLAN when both reliable broadcast 01:00:5e:80:xx:xx and normal broadcast FF:FF:FF:FF:FF:FF are received:

  WGB(config)#[**no**] **workgroup-bridge unified-vlan-client broadcast-tagging**

WGB will received both FF:FF:FF:FF:FF:FF and 01:00:5e:80:xx:xx packet on the native VLAN. By default, WGB will forward the normal broadcast (FF:FF:FF:FF:FF:FF) and discard the reliable broadcast (01:00:5e:80:xx:xx). If the CLI is enabled, WGB will forward the reliable broadcast (01:00:5e:80:xx:xx) to corresponding VLAN's wired client and discard the normal broadcast (FF:FF:FF:FF:FF:FF).

Troubleshooting Reliable Broadcast

Follow these steps to troubleshoot reliable broadcast downstream:

Procedure

Step 1 Get MGID VLAN mapping on the controller, using the **show network multicast mgid summary** command.

Example:

```
(Cisco Controller) >show network multicast mgid summary

Layer2 MGID Mapping:
--------------------
InterfaceName vlanId MGID
-------------------------------- ------ ----
management 800 0
vlan827 827 10
vlan801 801 14
vlan802 802 15
vlan804 804 13
vlan901 901 10
vlan902 902 11
vlan903 903 12
Layer2 mDNS MGID Mapping:
-----------------------
Start mDNS Mgid................................. 16447

End mDNS Mgid................................... 20545

Layer3 MGID Mapping:
--------------------

Number of Layer3 MGIDs.......................... 0

Group address VLAN MGID IGMP/MLD
--------------------------------------- ---- ---- --------
```

Step 2 Check packet count on AP.

a) For local mode or flexconnect mode (central switching), use the **show capwap mcast mgid wgb** command.

Example:

```
COS-AP#show capwap mcast mgid wgb
L2MGID for each WGB Client:
           wgbmac mgid vlan-id clientCount rx_bc tx_bc
A0:23:9F:F9:A2:6F   10     827           2     0     0
2C:D0:2D:D3:7F:0F   10     827           2     0     0
```

In above output, **wgbmac** is the RA of the new reliable broadcast packet, and **tx_bc** is new reliable broadcast packets counter send to WGB. You can also check if WGB entry's MGID and VLAN-ID mapping is consistent with controller's Layer2 MGID mapping here.

b) For Flexconnect mode (local switching), use the **show multicast wgb** command.

Example:

```
COS-AP#show multicast wgb
Broadcast to WGB stats:
BG-ID             wgb_mac  wiredCount Vlan_ID tx-bc
    2   2C:D0:2D:D3:7F:0F           2     827     0
    2   A0:23:9F:F9:A2:6F           2     827     0
```

In above output, **wgb_mac** is the RA of the new reliable broadcast packet, and **tx_bc** is new reliable broadcast packets counter send to WGB.

The CLI **clear counters client** can clear the tx-bc of the above show commands.

Step 3 Use debug CLI **debug interface wireless dot11Radio <0/1> wlan <0/15> tx** to check packet sent on the AP radio.

The following debug output shows a reliable downstream broadcast packet to VLAN 802. DA address is 01:00:5e:80:03:22. SA address is 00:50:56:8a:1f:eb.



Step 4 Check client entry and packet count on WGB.

a) For COS WGB, execute **show wgb bridge** and **show wgb statistic packet**.

Example:

```
cos-wgb#show wgb bridge
***Client ip table entries***
              mac vap   port vlan_id         seen_ip confirm_ago fast_brg
00:50:56:8A:04:DA   0 wired0     802 110.110.102.143    0.160000 true
00:50:56:8A:E8:F1   0 wired0     801 110.110.101.197   37.820000 true

cos-wgb#show wgb statistic packet
       Multicast/Unicast Packet statistics
       Multicast Tx : 32
       Unicast Tx : 24
       Multicast Rx : 64
       …
       Rx Broadcast from multiple vlans
       port VLAN_ID rx_bc2mc_cnt
          0     801            4
          0     802           76
```

In above output, **rx_bc2mc_cnt** is the reliable broadcast packet count received on cos WGB. The **clear wgb statistics packet** command can clear the rx_bc2mc_cnt count.

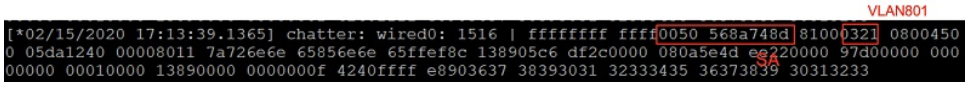
b) For IOS WGB, use the **show bridge** command to trace client entry in WGB.

Example:

```
WGB3702#show bridge
Total of 300 station blocks, 290 free
Codes: P - permanent, S - self
Bridge Group 1:
    Address     Action Interface  Age   RX count  TX count
0050.568a.e8f1 forward   Gi0.801    0        334         0
Bridge Group 82:
0050.568a.04da forward   Gi0.802    0        270         0
0050.568a.1feb forward   Gi0.802    3          1         0
```

Step 5 Debug packet forwarding on WGB.

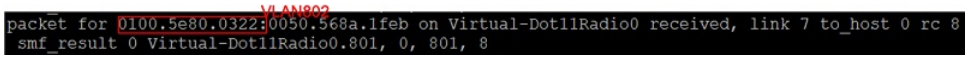
a) For COS WGB, use the **debug interface ethernet 0 tx** command. The following debug output shows that WGB forwards downstream BC2UC packet to VLAN 801.



b) For IOS WGB, use the **debug dot11 forwarding** command to trace how received special multicast packets are recovered to broadcast with right VLAN.

To forward normal broadcast (FF:FF:FF:FF:FF:FF), use the following command:

```
WGB(config)#no workgroup-bridge unified-vlan-client broadcast-tagging
```



To forward reliable broadcast (01:00:5e:80:xx:xx), use the following command:

```
WGB(config)#workgroup-bridge unified-vlan-client broadcast-tagging
```



Use the **debug dot11 events** command to trace how normal broadcast (FF:FF:FF:FF:FF:FF) packets are dropped on native VLAN. When **workgroup-bridge unified-vlan-client broadcast-tagging** is enabled on IOS WGB, the output of **debug dot11 events** will display a line as below:

```
*DEC 24 08:36:05.143: Unified WGB drop original none-tagged bcast pak
```

Troubleshooting Reliable Multicast

Follow these steps to troubleshoot reliable multicast downstream:

Procedure

Step 1 Check MC2UC group on the controller.

a) For local mode or FlexConnect mode (central switching) AP, use the **show network multicast mgid summary** command to get MGID of Layer3 multicast group. Use the **show network multicast mgid detail** <*mgid*> command to verify Mcast-direct status of client.

```
(Cisco Controller) >show network multicast mgid summary

Layer2 MGID Mapping:
--------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       800      0
vlan801                          801      13
vlan802                          802      14
vlan803                          803      15
vlan804                          804      16
vlan901                          901      10
vlan902                          902      11
vlan903                          903      12
Layer2 mDNS MGID Mapping:
-------------------------
Start mDNS Mgid................................ 16447

End mDNS Mgid.................................. 20545



Layer3 MGID Mapping:

--More-- or (q)uit
--------------------
Number of Layer3 MGIDs......................... 1

             Group address                VLAN  MGID  IGMP/MLD
 ---------------------------------------  ----  ----  --------
 226.6.6.8                                802   12353  IGMP
```

```
(Cisco Controller) >show network multicast mgid detail 12353

Mgid.......................................... 12353
Multicast Group Address....................... 226.6.6.8
Vlan.......................................... 802
No of clients................................. 2
Client List...............................
Client MAC         AP Name                          Expire Time (mm:ss)  Multicast-Status           Qos User Priori
ty
-----------------  -------------------------------  -------------------  -------------------------  ---------------
dc:8c:37:35:b2:6f  reliable-AP1                     49:37                Mcast-direct Allowed       4
00:50:56:8a:04:da  reliable-AP1                     49:37                Mcast-direct Pending       0
```

In above output, WGB is dc:8c:37:35:b2:6f, and WGB wired client is 00:50:56:8a:04:da.

b) For flexconnect mode local switching AP, use the **show flexconnect media-stream client summary** and **show flexconnect media-stream client <media-stream-name>** command.

```
(Cisco Controller) >show flexconnect media-stream client summary


Client Mac         Stream Name          Multicast IP     AP-Name                  VLAN   Type
-----------------  -------------------  ---------------  -----------------------  -----  ----------------
00:13:ef:f1:0d:6e      -                224.0.0.252      reliable-AP1             801    Multicast Only
00:50:56:8a:04:da      -                224.0.0.252      reliable-AP1             801    Multicast Only
00:50:56:8a:e8:f1      -                224.0.0.252      reliable-AP1             801    Multicast Only
```

```
(Cisco Controller) >show flexconnect media-stream client test

Media Stream Name.............................. test
IP Multicast Destination Address (start)..... 226.6.6.1
IP Multicast Destination Address (end)....... 226.6.6.10

Client Mac         Multicast IP     AP-Name                  VLAN   Type

00:50:56:8a:e8:f1  226.6.6.8        reliable-AP1             801    Multicast Direct
```

In above output. WGB wired client is 00:50:56:8a:e8:f1. Multicast group IP address is 226.6.6.8.

Step 2 Check media stream group on AP.

a) For flexconnect mode (local switching), use the **show multicast media-stream client group** and **show multicast media-stream client group <group-address>** commands.

```
reliable-AP1#show multicast  media-stream client group

Media stream Clients for All Groups:
Index           Client ToUc-count Group-Addr Sub-If MC2UC
    0 00:50:56:8A:E8:F1        627  226.6.6.8 aprlv4  true
```

```
reliable-AP1#show multicast  media-stream client group 226.6.6.8

Media stream Clients for 226.6.6.8
Group-Addr           Client ToUc-count Sub-If Vlan MC2UC
 226.6.6.8 00:50:56:8A:E8:F1          0 aprlv4  801  true
```

In above output. WGB wired client is 00:50:56:8a:e8:f1. Multicast group IP address is 226.6.6.8. VLAN: 801.

b) For local mode or flexconnect mode (central switching), use the **show capwap mcast mgid clients** command.

```
reliable-AP1#show capwap mcast mgid clients
mgid  type           client slot vap
   13 mc2uc DC:8C:37:35:B2:6F    1   7
   14 mc2uc DC:8C:37:35:B2:6F    1   7
12435 mc2uc DC:8C:37:35:B2:6F    1   7
12436 mc2uc DC:8C:37:35:B2:6F    1   7
MGID for each Client:
        client             ip   port  mgid
DC:8C:37:35:B2:6F 110.110.101.187 aprlv7 12435
                                        12436
```

Step 3 Use the **debug interface wireless dot11Radio <0/1> wlan <0/15> tx** command to check packet sent on the AP radio.

```
[*02/19/2020 08:30:00.2519] chatter: aprlv4: 1512 | 01005e06 06080050 568a1feb 08004500 05da771c 00002011 61596e6e 66
21e206 0608f060 138905c6 33f70000 00005e4c f64c0002 d90a0000 00000000 00010000 13890000 00000098 9680ffff e8903637 38
393031 32333435 36373839 30313233 34353637
```

The above output shows a downstream MC2UC packet to multicast group 226.6.6.8. SA is 00:50:56:8a:1f:eb, and DA is 01:00:5e:06:06:08.

Step 4 Check client entry and packet count on WGB.

a) For COS WGB, use the **show wgb bridge** and **show wgb statistic packet** commands.

```
Rx Broadcast from multiple vlans
port VLAN_ID rx_bc2mc_cnt
   0       8            0
   0     207            0
   0     800      1037744
   0     801       354185
   0     802       441969
```

```
cos-wgb#show wgb statistic packet

   Multicast/Unicast Packet  statistics
 Multicast Tx      : 36304
 Unicast Tx        : 8856
 Multicast Rx      : 31272
 Unicast Rx        : 10005
 Multicast Bridge  : 0
 Unicast Flood     : 1149
```

b) For IOS WGB, use the **show bridge** command to trace client entry in WGB.

```
Bridge Group 1:

    Address       Action    Interface       Age   RX count   TX count
0011.1111.1111    forward   Gi0.207           P          0          0
6c8b.d383.b3b8    forward   Vi0.801           4         16          0
0050.568a.e8f1    forward   Gi0.801           0         30          0
```

Step 5 Debug packet forwarding on WGB.

a) For COS WGB, use the **debug interface ethernet 0 tx** command.

```
[*02/14/2020 23:46:34.3250] chatter: wired0: 1512 | 01005e06 06080050 568a1feb 08004500 05da1a26 00002011 be4f6e6e 66
21e206 0608d495 138905c6 baba0000 0bde5e4c f8a7000d 51ce0000 0b000000 00010000 13890000 00000098 9680ffff e8903637 38
393031 32333435 36373839 30313233 34353637
                                  DA                SA
```

The above output shows that WGB forwards downstream MC2UC packet to multicast group 226.6.6.8. SA is 00:50:56:8a:1f:eb, and DA is 01:00:5e:06:06:08.

b) For IOS WGB, use the **debug dot11 forwarding** command.

```
packet for 0100.5e06.0608:0050.568a.1feb on Virtual-Dot11Radio0 received, link 7 to_host 0 rc 8 smf_result 0 Virtual-
Dot11Radio0.801, 0, 801,
                   DA          SA
```

The above output shows that WGB forwards downstream MC2UC packet to multicast group 226.6.6.8. SA is 00:50:56:8a:1f:eb, and DA is 01:00:5e:06:06:08.

Reliable WGB Downstream Broadcast for Multiple VLANs

Release 8.10.130.0 provides an enhancement for the Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs, on page 3 feature, which was first introduced in Release 8.3. Legacy broadcast without 802.11 ACK mechanism's may have more chance to cause packet loss over the air. With reliable downstream broadcast feature, broadcast packet can be converted to unicast packet. Hence the Root AP will receive the ACK for converted broadcast packet and retransmit in case of missing ACK.

The converted unicast packet's header will be changed from 3-address to 4-address format. WGB's MAC address will be used as receiver address (RA) instead of broadcast address and special multicast address with VLAN information will be used as destination address (DA). This BC2UC conversion for multiple VLAN's is possible for WGB and its wired clients. Since the converted packet is a unicast packet, Root AP will receive the ACK for each packet and retransmit based on the retry logic by the Root AP for every ACK which is not received for this broadcast to unicast conversion.

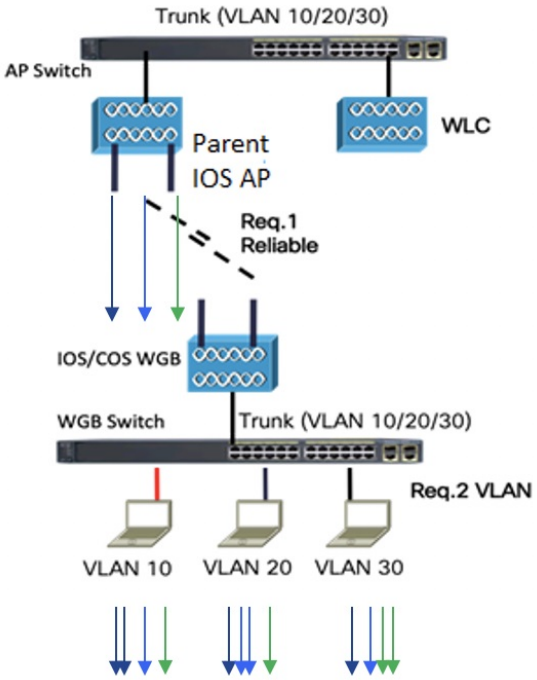
Note This enhancement is for WGB and its wired clients. It will not impact the non-WGB wireless clients.

- Supported AP platforms:
  - Cisco Industrial Wireless 3700 Series Access Points
  - Cisco Aironet 1570 Series Access Points
- Supported WGB platforms:
  - Cisco Industrial Wireless 3700 Series Access Points

- Supported AP modes:
  - Local
  - Bridge

As shown in the following figure, a WGB with wired clients of three different VLANs (VLAN 10, 20, and 30) joins the IOS AP wireless network. The broadcast traffic from AP to WGB will be transmitted to the clients with corresponding VLAN and retransmission will happen if traffic is lost on air.

Figure 9: WGB Bridged Network



The Receiver address (RA) of legacy broadcast packet is FF:FF:FF:FF:FF:FF and there will not be any retransmission if the packet is lost in the air. The reliable downstream broadcast feature replaces this RA with WGB address and Destination address (DA) with special multicast address 01:00:5e:80:xx:xx. This will make the packet as a unicast packet and enables ACK mechanism. The packet will be retransmitted when the ACK is not received.

The multicast address **01:00:5e:80:xx:xx** is introduced to transmit the VLAN information between AP and WGB. The VLAN value is embedded in 2 LSB of this multicast address. Both IOS and COS WGB support to decode this type of packet.

Root AP will make "N" copies for single broadcast packet for "N" WGBs associated to it on the specific VLAN. Also, non-converted packet will be sent for the benefit of non-WGB clients. Broadcast packets will not get converted if there is no WGBs associated on the specific VLAN.

QOS behavior:

- The new packet is a 802.11e Qos data.
- The 802.11e QoS priority of reliable broadcast packets will follow multicast default priority value from WLAN's QOS configuration.

The configuration similarities and changes between Release 8.10.130.0 and Release 8.3 are as following:

- **Similarities:**
  - Dynamic interface for all VLANs must be created on the controller. It is necessary for multi-vlan support in both Release 8.10.130.0 and Release 8.3.
  - Broadcast-tagging configurations are same on controller and WGB for both Release 8.10.130.0 and Release 8.3.
- **Changes:**
  - Interface-group must be configured in Release 8.3 to support downstream multiple VLANs. But in 8.10.130.0, it can be supported with or without interface-group configuration on the WLAN.
  - Broadcast packets are converted to multicast packets by Root AP in Release 8.3. While in Release 8.10.130.0, broadcast packets will be converted to unicast packets by Root AP.

The following figures illustrate an example of 802.11 packet forwarding from VLAN 106 (0x006a). The receiver address changes from FF:FF:FF:FF:FF:FF to the MAC address of WGB Radio (d4:c9:3c:e3:16:ec), and the destination address changes from FF:FF:FF:FF:FF:FF to 01:00:5E:80:**00**:**6a** (the last two bytes in MAC address represents corresponding VLAN in hexadecimal).

Figure 10: Normal Broadcast Packet

```
IEEE 802.11 Data, Flags: ......F.
    Type/Subtype: Data (0x0020)
  > Frame Control Field: 0x0802
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco_75:b2:2d (b0:8b:cf:75:b2:2d)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: RealtekS_36:1e:08 (00:e0:4c:36:1e:08)
    BSS Id: Cisco_75:b2:2d (b0:8b:cf:75:b2:2d)
    STA address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    1110 1001 0000 .... = Sequence number: 3728
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.100.106.35, Dst: 10.100.106.255
```

Figure 11: Reliable Broadcast Packet

```
IEEE 802.11 QoS Data, Flags: ......FT
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8803
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Cisco_e3:16:ec (d4:c9:3c:e3:16:ec)
    Transmitter address: Cisco_75:b2:2d (b0:8b:cf:75:b2:2d)
    Destination address: IPv4mcast_80:00:6a (01:00:5e:80:00:6a)
    Source address: RealtekS_36:1e:08 (00:e0:4c:36:1e:08)
    .... .... .... 0000 = Fragment number: 0
    0111 0010 1010 .... = Sequence number: 1834
  > Qos Control: 0x0004
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.100.106.35, Dst: 10.100.106.255
```

Controller Configuration

This section provides the basic configuration for AireOS controller.

- To enable or disable reliable broadcast traffic for IOS AP, configure broadcast-tagging on the WLAN from AireOS controller:

  ```
  (Cisco Controller)> config wlan wgb broadcast-tagging <enable|disable> <wlan-id>
  ```

- To support reliable broadcast feature, basic broadcasting forwarding and global multicast feature should be enabled on controller first. The following commands are for basic broadcast forwarding and global multicast configuration.
  - To enable global broadcast forwarding:

    ```
    (Cisco Controller)> config network broadcast enable
    ```

  - To configure AP multicast mode:

    ```
    (Cisco Controller)> config network multicast mode multicast multicast_Group_Address
    ```

WGB Configuration

To support multiple VLAN on IOS WGB, the following CLI should be configured on WGB:

```
WGB(config)#workgroup-bridge unified-vlan-client
```

To enable broadcast tagging on a VLAN:

```
WGB(config)#workgroup-bridge unified-vlan-client broadcast-tagging
```

To disable broadcast tagging on a VLAN:

```
WGB(config)#no workgroup-bridge unified-vlan-client broadcast-tagging
```

WGB will received both FF:FF:FF:FF:FF:FF and 01:00:5e:80:xx:xx packet on the native VLAN. By default, WGB will forward the normal broadcast (FF:FF:FF:FF:FF:FF) and discard the reliable broadcast (01:00:5e:80:xx:xx). If the CLI is enabled, WGB will forward the reliable broadcast (01:00:5e:80:xx:xx) to corresponding VLAN's wired client and discard the normal broadcast (FF:FF:FF:FF:FF:FF).

Troubleshooting Reliable Broadcast

This section describes the troubleshooting of reliable broadcast on controller, Root AP, and WGB.

- Troubleshooting on controller:
  - Use the **show wlan** <*wlanid*> command to check if broadcast tagging is enabled.

    ```
    (WLC) > show wlan 3
    Universal Ap Admin.............................. DisabledBroadcast
    Tagging.............................. Enabled
    ```

  - Use **debug capwap payload enable** to check the mgid information sent to AP.

    ```
    *spamApTask0: Feb 19 18:14:51.384: b0:8b:cf:75:b2:20 L2_MCAST_MGID_INFO : payload
    0 addOrDelete 1, mgidByte[0] 0, mgidByte[1] 10
    *spamApTask0: Feb 19 18:14:51.384: b0:8b:cf:75:b2:20 MCAST_MGID_INFO_PAYLOAD vapId
     3, isL3Mgid FALSE, numOfMgid 1, vlanInterfaceId 10
    ```

  - Use the **debug pem events** command to check the association of WGB and its wired clients.

    ```
    *iappSocketTask: Feb 19 14:05:38.379: 00:e0:4c:53:44:58 sending to spamAddMobile
    (wgb wired client) vlanId 106 mgid 11 numOfMgid 1
    ```

- Troubleshooting on Root AP:

- Use the **show capwap mcast mgid all** command to display L2 MGID information.

```
IOS-AP#show capwap mcast mgid all
L2 MGID Information:
 L2  MGID = 0       WLAN bit map (all slots) = 0x0001 VLAN ID = 103
  Slot map/tx-cnt: R0:0x0001/3446 R1:0x0001/3446 R2:0x0001/0
 L2  MGID = 1       WLAN bit map (all slots) = 0x0001 VLAN ID = 0
  Slot map/tx-cnt: R0:0x0001/7828 R1:0x0001/7828 R2:0x0000/0
 L2  MGID = 11      WLAN bit map (all slots) = 0x0001 VLAN ID = 106
  Slot map/tx-cnt: R0:0x0001/14 R1:0x0001/14 R2:0x0001/0
```

- Use the **show capwap mcast mgid id** <*mgid value*> command to display the details of a specific MGID.

```
IOS-AP#show capwap mcast mgid id 11
L2 MGID = 11     WLAN bit map (all slots) = 0x0001 VLAN ID = 106
  Slot map/tx-cnt: R0:0x0001/979 R1:0x0001/979 R2:0x0001/0

rx pkts = 979
tx packets:
wlan  :     0     1     2     3     4     5     6     7     8     9    10    11
 12    13    14    15
slots0 :     0     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
slots1 :   979     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
slots2 :     0     0     0     0     0     0     0     0     0     0     0     0
   0     0     0     0
 Reliable BCAST Clients: 1 Client: d4c9.3ce3.16ec    --- SlotId: 1   WlanId: 0
ConvertedBCASTtx: 263
```

- Use the **debug capwap mcast** command to get the information of WGB and its wired clients added to the BC2UC client list.

```
*Dec 19 21:09:29.795: CAPWAP MCAST: capwapAddEntryToL2MgidList:Added new client
d4c9.3ce3.16ec to mgid 11 list of vlan 105, Total clients in this list: 1.
*Dec 19 21:10:56.491: CAPWAP MCAST: capwapAddEntryToL2MgidList:Added new client
d4c9.3ce3.16ec to mgid 10 list of vlan 106 for wired client f076.1cdc.b22c, Total
clients in this list: 1.
```

- Use **debug dot11 dot11radio <0|1> trace print xmt** to check the transmission of original and converted broadcast packet.

```
Converted Packet(4-address format):
*May  6 14:04:40.859: 613B6145 t a8.1b2s0  - 8803 000 48B89C 75B22C m01005E 16F0
361E08 q4 l92
   IP 10.100.106.255 < 10.100.106.56 f1-0-0 id 0 ttl64 sum 50AA prot 1 len 84
  ICMP ping code 0 chk F4D7, id 20765 seq 330
  CF77 B25E 0000 0000 6F17 0100 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D

Original packet (3-address format):
*May  6 14:04:40.859: 613B6204 t 18     0  - 0802 000 mFFFFFF 75B22C 361E08 C020
l92
   IP 10.100.106.255 < 10.100.106.56 f1-0-0 id 0 ttl64 sum 50AA prot 1 len 84
  ICMP ping code 0 chk F4D7, id 20765 seq 330
```

- Troubleshooting on WGB:
  - Use the **show running-config** command to check the status of **workgroup unified-vlan-client** and **workgroup-bridge unified-vlan-client broadcast-tagging**.
  - Use the **debug dot11 forwarding** command to check whether the IOS WGB has recovered the VLAN information from converted broadcast packet.

```
*Sep 15 02:54:24.775: Unified WGB convert specific mcast+vlan pak to
ffff.ffff.ffff:0080.483f.d5f6 on Virtual-Dot11Radio0 received,
link 7, dest_vlan_id 0x402F  <- 2F (Vlan id)
```

- Use the **debug dot11 events** command to check whether the IOS WGB has received the original broadcast packet and dropped.

```
*Feb  4 17:41:19.081: Unified WGB drop original none-tagged bcast pak from source
00e0.4c36.1e08, ethertype: 0x0800, linktype: 7
```

- Use the **debug dot11 dot11radio <0|1> trace print rcv** command to check converted packets and original packets.

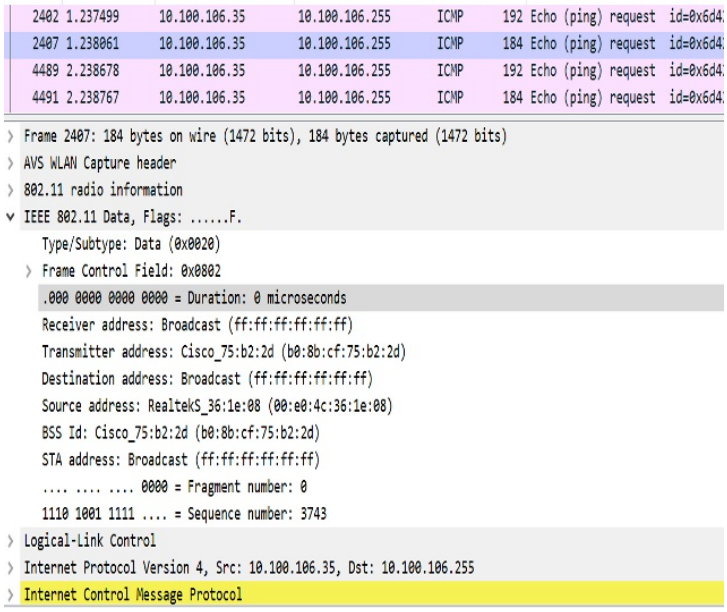
```
Converted Packet:
*Nov 27 15:27:23.727: CB8823A0 r  m6-2   24/128/128/128 71- 8803 02C 48B89C AD9A70
 m01005E 06A0 392AC9 q4 l92
 4500 0054 0000 4000 4001 56C9 0A64 6719 0A64 67FF 0800 2E6A 1556 03BF
 B74B DE5D 0000 0000 5604 0600 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D
 1E1F 2021 2223 2425 2627 2829 2A2B 2C2D 2E2F 3031 3233 3435 3637 4860 6C3D

Original Packet:
*Nov 27 15:27:23.727: CB88246F r 18      21/128/128/128 74- 0802 000 mFFFFFF AD9A70
 392AC9 4610 l92
 4500 0054 0000 4000 4001 56C9 0A64 6719 0A64 67FF 0800 2E6A 1556 03BF
 B74B DE5D 0000 0000 5604 0600 0000 0000 1011 1213 1415 1617 1819 1A1B 1C1D
 1E1F 2021 2223 2425 2627 2829 2A2B 2C2D 2E2F 3031 3233 3435 3637 0000 0000
```

Use Sniffer to capture packet over the air or on the wired side when the detailed packet information is needed.

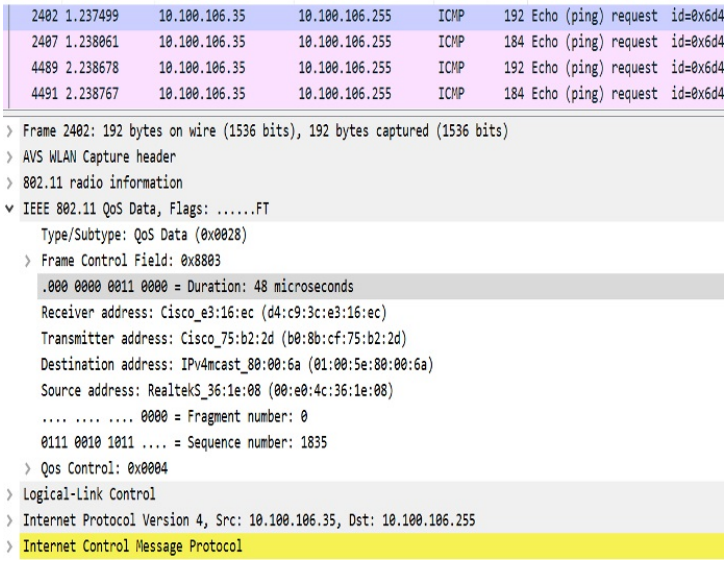
The following figure shows the original packet details.

Figure 12: Original Packet



The following figure shows the converted packet details.

Figure 13: Converted Packet



WGB M1 and M3 Timeout Enhancement

To fulfill the requirement for quick roaming to avoid longer outages, Release 8.10.130.0 provides an enhancement for faster detection of missing M1 or M3 message during 4-way handshake.

Before this enhancement, the minimum time to detect loss of M1 or M3 packet is 60 seconds by default (eap-timeout). But, this timeout will work for complete 4-way handshake process, which means it will not detect whether M1 or M3 is not received from authenticator. This timeout value can be reduced to 2 seconds by existing configuration, but it cannot be configured to less than 2 seconds. However, 2 seconds is too long for some mission critical applications where the requirement is to roam around 600 msec.

With this enhancement, M1 and M3 timeouts can be configured explicitly as part of existing eap-timeout CLI. The range of M1 timeout is 100 to 2000 milli seconds and the range of M3 timeout is 100 to 1000 milli seconds. If M1 or M3 is not received within configured timeout, reassociation will be triggered. M1 timer will be started at the same time of existing eap-timer start. M3 timer will be started once M1 is received by the WGB.

Note This enhancement will not have impact on non-WGB clients.

Note The new M1 and M3 timeout values are subset of the existing eap-timeout.

If M1 or M3 timeout is configured, the configured eap timer (eap-timeout) will be stopped, in case that M1 or M3 is not received within the configured timeout.

Supported platform:

- Controller: AireOS controller

- AP: All
- IOS WGB: Cisco Industrial Wireless 3700 Series Access Points

Configuration for IOS WGB

Use the following command to configure M1-timeout:

```
WGB(config)#workgroup-bridge timeouts eap-timeout <2-60> m1-timeout <100-2000>
```

Use the following command to configure M1-timeout and M3-timeout:

```
WGB(config)#workgroup-bridge timeouts eap-timeout <2-60> m1-timeout <100-2000>
 m3-timeout <100-1000>
```

The existing eap-timeout configuration can still be used without configuring M1 or M3 timeout.

```
WGB(config)#workgroup-bridge timeouts eap-timeout <2-60>
```

Note

- eap-timeout is configured in seconds and M1/M3 timeout is configured in milli seconds.
- eap-timeout value should be in nearest seconds that is at least 500ms higher than the sum of M1-timeout and M3-timeout.
- eap-timeout value should be at least one second higher than M1-timeout.

Troubleshooting

Use these debug commands to troubleshoot the configuration on WGB:

- Use the **debug dot11 dot11Radio [0|1] trace print uplink** command to check the WGB status like association and EAP authenticating, or to check if M1 or M3 timeout occurs.
  - If M1 timeout occurs, the following debug information displays

    ```
    *Nov  4 19:32:45.127: 165830EC-1 Uplink: Lost AP, EAP authentication M1 timeout
    ```

  - If M3 timeout occurs, the following debug information displays

    ```
    *Nov  4 19:39:23.645: 165830EC-1 Uplink: Lost AP, EAP authentication M3 timeout
    ```

- The **debug dot11 wpa-cckm-km-dot1x** command prints received M1 information, no matter whether it is received before or after setting the EAP state.

```
*Apr 29 09:30:30.911: [D]WPA/CCKM:SNonce is:29 E3 CF 7A AD E0 0C C5 DE 65 63 AC 86 80
DF DD 6D A4 05 5B C2 6F F9 BA C6 36 E0 DA 10 F7 A1 5F
*Apr 29 09:30:30.915: [D]WPA/CCKM:wpa_cckm_km_process_key: descriptor type = 2
*Apr 29 09:30:30.915: [D]WPA/CCKM:RSNA Descriptor 0x2
*Apr 29 09:30:30.915: [D]WPA/CCKM:wpa v2 handshake 1: passed the flags checking
*Apr 29 09:30:30.915: [D]WPA/CCKM:Replay counter for the first handshake is 0
*Apr 29 09:30:30.915: [D]WPA/CCKM:handshake2 key information is 010A, handshake1 is
008A
*Apr 29 09:30:30.923: [D]WPA/CCKM:wpa_cckm_km_process_key: descriptor type = 2
*Apr 29 09:30:30.923: [D]WPA/CCKM:RSNA Descriptor 0x2
*Apr 29 09:30:30.923: [D]WPA/CCKM:Handshake 3 - checking the key packet
*Apr 29 09:30:30.923: [D]WPA/CCKM:Start RSC from authenticator is 0
 wpav2 msg3 decrypted key data: 30 14 01 00 00 0F AC 04 01 00 00 0F AC 04 01 00 00 0F
AC 02 28 00 DD 16 00 0F AC 01 01 00 67 AA 52 2B 19 63 7F 8D 07 EF 30 48 3B 8E 2B 04 DD
```

```
 05 00 40 96 03 05 DD 05 00 40 96 14 01 DD 00 00 00
*Apr 29 09:30:30.923:
*Apr 29 09:30:30.923: [D]WPA/CCKM:wpav2 handshake 3 gtk len 16
*Apr 29 09:30:30.923: [D]WPA/CCKM:wpav2 handshake4 key information is 030A, handshake3
 is 13CA
*Apr 29 09:30:30.923: [D]WPA/CCKM:Index for the key is 0
```

- Use the **debug dot11 supp-sm-dot1x** command to check whether M1 packet is processed properly or not.

```
*Apr 29 09:39:46.291: Uplink address set to 00ee.ab25.6860
*Apr 29 09:39:46.291: Initialising common IOS structures for dot1x
*Apr 29 09:39:46.291: Done.
*Apr 29 09:39:46.291: DOT1X_SHIM: Start supplicant on Dot11Radio0 (credentials )
*Apr 29 09:39:46.291: DOT1X_SHIM: Skipping dot1x_mgr_auth start (open auth)
*Apr 29 09:39:46.291: DOT1X_SHIM: Initialising WPA [or WPA-PSK or CCKM or Dot11R] key
management module
*Apr 29 09:39:46.291: DOT1X_SHIM: Got Eapol key packet from dot1x manager
*Apr 29 09:39:46.291: DOT1X_SHIM: Passing key packet to KM module
*Apr 29 09:39:46.291: supp_km_processKey: descriptor type = 2
*Apr 29 09:39:46.291: supp_km_processKey: key length = 138
*Apr 29 09:39:46.299: DOT1X_SHIM: Got Eapol key packet from dot1x manager
*Apr 29 09:39:46.299: DOT1X_SHIM: Passing key packet to KM module
*Apr 29 09:39:46.299: supp_km_processKey: descriptor type = 2
*Apr 29 09:39:46.299: supp_km_processKey: key length = 5066
*Apr 29 09:39:46.299: dot1x_pakio_plumb_keys: trying to plumb PTK key
*Apr 29 09:39:46.299: dot1x_pakio_plumb_keys: trying to plumb vlan key - length: 16
```

- Use the **debug dot11 d[0|1] trace print xmt rcv mgmt uplink** command to print the EAPOL keys and management frames.

```
*Apr 29 09:56:41.731: 2182AC5E r  6      /18/128 78- 8802 03C E871B0 25686F 25686F 0040
 q7 l107 <-M1
  EAPOL2 EAPOL key desc 02  008A 0010 0000 0000 0000 0000 30C4 DE2A A5C9
  21D5 B8B0 0D26 FC11 39DF B75B ABE9 FE01 0E8B 8497 9FA5 55E5 928B 0000 0000
  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
*Apr 29 09:56:41.731: 2182AEC8 t  6     0  - 8801 000 25686F E871B0 25686F 0040 q7 l143
  <-M2
  EAPOL key desc 02  010A 0010 0000 0000 0000 0000 C80B A25F 2743 C855 FF72
  996B 9DAB D1AF 42D0 30D9 387D 5473 0637 CB20 13D7 11F2 0000 0000 0000 0000
  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 5876 3CDC C27D
*Apr 29 09:56:41.731: 2182B207 r  6      /18/128 78- 8802 03C E871B0 25686F 25686F 0050
 q7 l179 <-M3
  EAPOL2 EAPOL key desc 02  13CA 0010 0000 0000 0000 0001 30C4 DE2A A5C9
  21D5 B8B0 0D26 FC11 39DF B75B ABE9 FE01 0E8B 8497 9FA5 55E5 928B 0000 0000
  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 35F5
*Apr 29 09:56:41.735: 2182B436 t  6     0  - 8801 000 25686F E871B0 25686F 0050 q7 l107
 <-M4
  EAPOL key desc 02  030A 0010 0000 0000 0000 0001 0000 0000 0000 0000 0000
  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 A319 565A 7FD9
*Apr 29 09:56:42.439: 218D7757 t  6     0  - D040 8133 25686F E871B0 25686F 0000 action
 l 9
```

Parallel Redundancy Protocol Enhancement on AP and WGB

Cisco Wireless Release 8.4 provides the Parallel Redundancy Protocol (PRP) enhancement to improve wireless network availability for wired clients behind Workgroup Bridge (WGB), and improve the roaming performance by allowing wired clients to have dual wireless connections.

PRP allows a data communication network to prevent data transmission failures by providing two alternate paths for the traffic to reach its destination. Two Ethernet networks (LANs) with similar topologies are completely separated.

A device that requires protection for data across the network connects to the two independent networks (LAN-A and LAN-B) is called a Dual Attached Node implementing PRP (DANP). A DANP source sends two frames simultaneously on both LANs. A DANP destination receives both frames and discards the duplicating. If one LAN fails, a DANP destination can still receive a frame from the other LAN.

Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs). A Redundancy Box (RedBox) is used when a single interface node must be attached to both networks. Such a node can communicate with all other nodes. The switch implements RedBox functionality is a PRP switch.

To implement the PRP function for this release, you need to connect the AP and WGB to a PRP switch. The PRP switch is to offload PRP processing. AP or WGB is to keep dual wireless connections. You can have two WGBs interconnected through an external PRP switch and wirelessly connected to a single fixed AP or two fixed APs. Two WGBs can roaming between APs. Redundant packet transmissions can be supported over either single or both 2.4 GHz and 5 GHz. The infrastructure side also needs a PRP switch for AP side.

For the application where both WGBs may roam at the same time, the roaming coordination feature is introduced to avoid roaming gaps and guarantee staggered roaming. In this release, only dual radio links roaming coordination across two WGBs is supported for roaming coordination.

Supported platforms and AP mode:

- Controller and AP on the infrastructure side—FlexConnect AP mode (central authentication, local switching), the following IOS-based platforms are supported: IW3702, 2700, 3700, and 1570 series.
- WGB on the client side—Only supported for IW3700 Series
- Roaming coordination—Only supported for IW3700 Series

Sample Network Configuration

General guidelines for this configuration:

- Separation of expected redundancy in the network:
  - Traffic expecting redundancy mapped to two reserved SSID A and SSID B each with specified VLAN.
  - Each WGB is configured to connect either SSID A or SSID B.
  - Others traffic without expectation of redundancy is recommended to be mapped to other SSID.
- WGB supports unified VLAN function and it is recommended that wired clients not to use VLANs assigned to SSID A or SSID B.
- Wired clients connected to WGB are source and recipients of redundancy traffic.

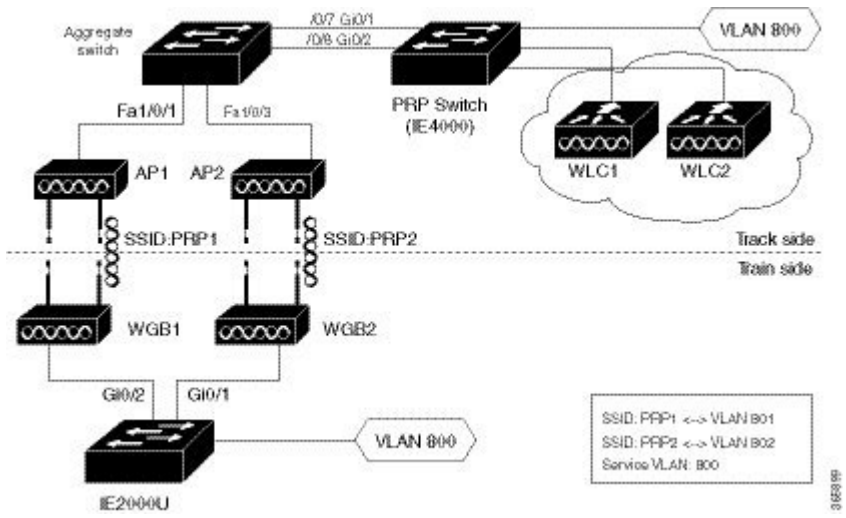
The following figure shows a topology of concurrent wireless transmission via two WGBs paired with one PRP switch, commonly used in train transportation.

On the train side, the PRP switch (in this example, Cisco IE2000U) duplicates upstream packets and sends both packets simultaneously via two different ports, Gi0/1 and Gi0/2. The dual packets will pass from different WGBs or APs, to ensure that at least one packet reaches the destination. On the track side, one more PRP

switch is added to each aggregating endpoint along the track. The PRP switch on the track side will remove the duplicating for upstream packets. The same redundancy for downstream packet is also available by the pair of PRP switches.

Note The throughput of this solution depends on the network elements depicted in the diagram. Each element along the wired and wireless transmission path should validate its throughput to avoid being the throughput bottleneck.

Figure 14: Concurrent Wireless Transmission via Two WGBs Paired With One PRP Switch



Controller Configuration (CLI Only)

To enable or disable PRP on a WLAN (new command):

```
(Cisco Controller)> config wlan wgb prp {enable|disable} <wlan id>
enable              Enable Parallel Redundancy Protocol (PRP) feature on a WLAN
disable             Disable Parallel Redundancy Protocol (PRP) feature on a WLAN
```

Note This feature is disabled by default.

This CLI will enable two WLANs to allow dual associations in flex-connect mode. It will also enable the AP to forward packets to or from WGB wired clients with double tags in flex-connect mode.

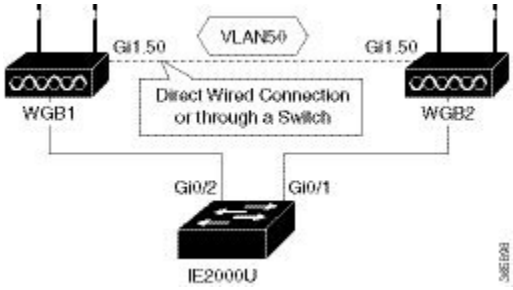
Note To enable unified VLANs in the WGB, the existing command config wgb vlan enable should also be executed. You should configure the inner VLAN (VLAN for wired client) on controller as well.

WGB Configuration for Roaming Coordination (CLI Only)

For Parallel Redundancy Protocol (PRP), wired client traffic will be duplicated to transmit in dual radio links in two WGBs. Dual radio links without any radio link coordination have the possibility to trigger roaming at the same time, so that the traffic will be broken in a short window time.

The following figure is a typical PRP scenario of train transportation. AP like IW3702 has two physical Ethernet ports. Gig0 will be exclusively used to bridge PRP traffic. Gig1 will be used for internal communication. Gig 1 will connect to a non-PRP port on the PRP switch or connect to a peer Gig1 port directly.

Figure 15: Peer Link Between Two WGBs



Configuration of Dual Radio Coordination on Two WGBs

Follow these steps to configure dual radio coordination on two WGBs:

1. Configure service VLAN.

   Use the following command to enable the service VLAN traffic that will be punted to local handling process for sub interface on Gig0 or Gig1.

   ```
   WGB(config)# workgroup-bridge service-vlan <vlan id>
   ```

2. Configure peer coordinator address.

   Use the following commands to set peer coordinator address and create the coordination communication process. For example, if you have configured the service VLAN to 50, you should configure the local/peer coordinator address under sub interface 50.

   ```
   WGB(config)# interface GigabitEthernet1.50
   WGB(config-subif)# encapsulation dot1q 50
   WGB(config-subif)# ip coordinator peer-addr <addr>
   ```

3. Configure dot11 radio coordinator on two WGBs.

   Use the following commands to create dot11 coordinator process, and enable dot11 roaming coordinator service on radio 0 or radio 1.

   ```
   WGB(config)# dot11 coordinator uplink single [radio 0|radio 1]
   ```

4. Configure dot11 coordination roaming waiting timer.

   Use the following command to set the dot11 coordination roaming waiting timer. The default is 100ms.

   ```
   WGB(config)# dot11 coordinator timeout roam-wait [value]
   ```

5. Configure Dot11 roaming coordination bypass.

   Use the following command to bypass roaming coordination decision on WGB. When configured, it is used to collect WGB's roaming conflict statistics, and will not affect the current roaming behavior.

   ```
   WGB(config)# dot11 coordinator bypass
   ```

6. Configure to avoid bridge loop.

Wired network on WGB side can introduce a bridge loop if you connect the Gig1 port of WGBs directly or via a switch. The following sample configurations can avoid the bridge loop.

Note The coordination traffic is forwarded on service VLAN and will not be blocked.

- To avoid bridge loop when connecting the Gig1 port of WGBs directly, configure the following on both WGBs:

```
WGB(config)# access-list 700 deny 0000.0000.0000 ffff.ffff.ffff
WGB(config)# interface gigabitEthernet 1
WGB(config-if)# l2-filter bridge-group-acl
WGB(config-if)# bridge-group 1
WGB(config-if)# bridge-group 1 output-address-list 700
```

- To avoid traffic loop when connecting two WGBs via a switch, configure the following on the switch port:

```
interface GigabitEthernet0/3
switchport trunk allowed vlan 50
switchport mode trunk

interface GigabitEthernet0/4
switchport trunk allowed vlan 50
switchport mode trunk
```

Controller Configuration

Note For more information about Controller configuration for FlexConnect, see the FlexConnect Chapter in the *Cisco Wireless Controller Configuration Guide*.

Follow these steps to configure the wireless controller for FlexConnect:

1. Create two WLANs with the SSID PRP1 and PRP2.
2. Enable local switching for each WLAN.

Note For any wired client within the service VLAN, you need to create a corresponding dynamic interface with the same service VLAN on controller.

Configuration of AP

1. Configure AP to FlexConnect mode and join controller.
2. Enable VLAN support on each AP, and make sure PRP SSID is included.

Configuration of WGBs

- WGB1 Configuration

```
hostname WGB1
dot11 ssid PRP1
   vlan 801
   authentication open
interface Dot11Radio1
 no ip address
 ssid PRP1
 antenna gain 0
 stbc
 beamform ofdm
 station-role workgroup-bridge
!
interface Dot11Radio1.800
 encapsulation dot1Q 800
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.801
 encapsulation dot1Q 801 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 2
!
interface GigabitEthernet0.801
 encapsulation dot1Q 801 native
 bridge-group 1
!
interface BVI1
 mac-address 4c00.821a.c0b0
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 route ip
!
workgroup-bridge unified-vlan-client
```

- WGB2 Configuration

```
hostname WGB2
dot11 ssid PRP2
   vlan 802
   authentication open
interface Dot11Radio1
 no ip address
 !
 ssid PRP2
 !
 antenna gain 0
 stbc
 beamform ofdm
 station-role workgroup-bridge
!
interface Dot11Radio1.800
```

```
 encapsulation dot1Q 800
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.802
 encapsulation dot1Q 802 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 2
!
interface GigabitEthernet0.802
 encapsulation dot1Q 802 native
 bridge-group 1
!
interface BVI1
 mac-address f872.eae4.a4d8
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
bridge 1 route ip
workgroup-bridge unified-vlan-client
```

Aggregated Switch Configuration

```
Agg-SW# show run int fa 1/0/1
description ***AP1***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end


Agg-SW#show run int fa 1/0/3
Building configuration...


Current configuration : 196 bytes
!
interface FastEthernet1/0/3
 description ***AP2***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end

Agg-SW# show run int fa 1/0/7
Building configuration...


Current configuration : 178 bytes
!
```

```
interface FastEthernet1/0/7
 description ***PRP-Track-SW***
 switchport access vlan 801
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
end


Agg-SW# show run int fa 1/0/8
Building configuration...


Current configuration : 178 bytes
!
interface FastEthernet1/0/8
 description ***PRP-Track-SW***
 switchport access vlan 802
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
```

PRP Switch Configuration

```
interface PRP-channel1
 switchport mode trunk
interface GigabitEthernet0/1
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
!
interface GigabitEthernet0/2
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
```

Note For the PRP configurations on the Cisco IE switches, refer to Parallel Redundancy Protocol Software Configuration Guide for Industrial Ethernet 2000U Series Switches.

Verifying the PRP Configurations

Follow these steps to verify the PRP configurations:

Before you begin

- Create an SVI interface on the train side PRP switch with service vlan: 800.
- Configure the SVI interface on the track side PRP switch with service vlan: 800, and create the DHCP pool.

Procedure

Step 1 On the train side PRP switch, use the following command to check whether an IP address has been assigned to Vlan 800 from the DHCP pool on the track side.

Example:

```
PRP-Train-SW# show ip int bri
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan800                10.10.80.67     YES DHCP   up                    up
```

Step 2 On the track side PRP switch, use the following command to display ingress packet statistics. In this example, LAN A and LAN B both have one packet.

Example:

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
   ingress pkt lan a: 1
   ingress pkt lan b: 1
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt_a: 0
   ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
   ingress pkt_lan a: 0
   ingress pkt_lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
```

Step 3 On the train side PRP switch, ping the track side with the following command, to send 5 packets from the train to the track side:

Example:

```
PRP-Train-SW# ping 10.10.80.1
<= issue ping from train to track side, 5 pkts
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.80.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```

Step 4 On the track side PRP switch, use the following command to display the number of packets that LAN A and LAN B have received, and the number of duplicated packets that have been discarded. In this example, after receiving 5 packets, both LAN A and LAN B have 6 packets in total.

Example:

```
PRP-Track-SW# show prp statistics ingressPacketStatistics
GE ports PRP INGRESS STATS:
   ingress pkt lan a: 6   <= LAN A receives 5pkts
   ingress pkt lan b: 6   <= LAN B receives 5pkts
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 5
   ingress danp pkt dscrd: 5  <= discard 5 duplicate pkts
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt_a: 0
   ingress pri over pkt_b: 0
FE ports PRP INGRESS STATS:
   ingress pkt_lan a: 0
   ingress pkt_lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
```

Dual Radio Parallel Redundancy Protocol Enhancement on WGB

Release 8.5 provides the Dual Radio Parallel Redundancy Protocol (PRP) enhancement as the second phase of the PRP feature.

This feature enables dual radio (2.4G and 5G) workgroup bridge mode on a WGB simultaneously. The WGB is wirelessly connected to the access points, with redundant packet transmissions over 2.4 GHz and 5 GHz subsystem.

Supported platforms and access point mode:

- Controller and AP on the infrastructure side—FlexConnect AP mode (central authentication, local switching), the following IOS-based platforms are supported: IW3702, 2700, 3700, and 1570 series.
- WGB on the client side—Only supported for IW3700 Series
- Roaming coordination—Only supported for IW3700 Series

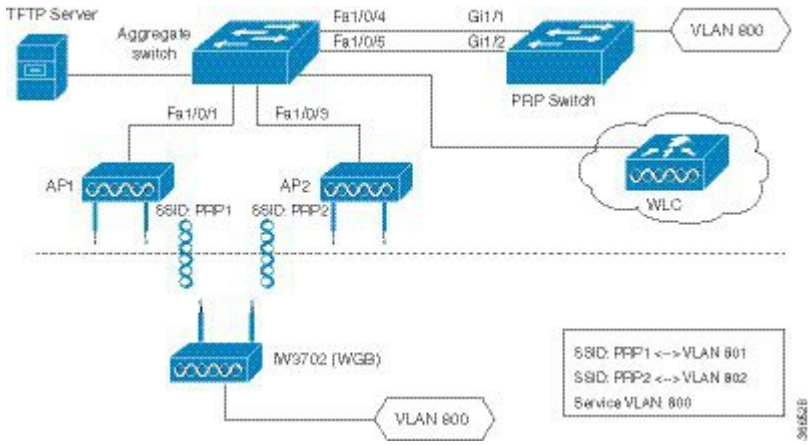
Sample Network Configuration

Figure 16: Concurrent Wireless Transmission Via One WGB With Dual Radio and Paired With One PRP Switch, on page 38 shows a topology of concurrent wireless transmission via one WGB with dual radio and paired with one PRP switch.

The WGB (Cisco IW3702 Access Point) duplicates upstream packets and sends both packets simultaneously via 2.4 GHz and 5 GHz. The duplicated packets will pass to the access points, to ensure that at least one packet reaches the destination. On the infrastructure side, a PRP switch (for example, Cisco IE4000) is added to each aggregating endpoint. The PRP switch on the infrastructure side will remove the duplicating for upstream packets. The same redundancy for downstream packet is also implemented by the pair of PRP switch and WGB.

Note The throughput of this solution depends on the network elements depicted in the diagram. Each element along the wired and wireless transmission path should validate its throughput to avoid being the throughput bottleneck.

Figure 16: Concurrent Wireless Transmission Via One WGB With Dual Radio and Paired With One PRP Switch



Configuration of Roaming Coordination on a Single WGB

As the client traffic will be duplicated to transmit in dual radio links of one WGB, radio link coordination is necessary to avoid the possibility to trigger roaming at the same time, which will cause the traffic to be broken in a short window time.

- Configure dot11 dual radio coordinator on one WGB.

```
WGB(config)# dot11 coordinator uplink both
```

- Configure dot11 coordination roaming waiting timer. The value of the timer is from 50–150 ms. The default is 100 ms.

```
WGB(config)# dot11 coordinator timeout roam-wait [value]
```

Controller Configurations

This section contains the configurations on controller to enable PRP under WLAN and multiple VLAN support.

Note When you create WLAN, the BSSID of WLAN (mapping to 2.4G radio) and the BSSID of WLAN (mapping to 5G radio) must be different.

Note From release 8.5, you can configure the PRP settings via both CLI and GUI.

Enabling PRP Under WLAN (CLI)

- Use the following command to enable PRP under WLAN. The value of WLAN ID is between 1 and 512.

```
(WLC)> config wlan wgb prp enable <WLAN id>
```

- Use the following command to check the PRP status:

```
(WLC)> show wlan <WLAN id>
```

The output of this show command displays the PRP status as below:

```
Universal Ap Admin.............................. Disabled
Broadcast Tagging............................... Disabled
PRP............................................. Enabled
```

Enabling PRP Under WLAN (GUI)

To enable PRP under WLAN in GUI, choose **WLAN** -> **Advanced**. In the **WGB PRP** field, select the check box in front of **Enable**.

Enabling Multiple VLAN Support (CLI)

Use the following command to enable or disable the multiple VLAN support:

```
(WLC-PRP)> config wgb vlan {enable|disable}
enable Enable WGB Vlan Client Support
disable Disable WGB Vlan Client Support
```

Enabling Multiple VLAN Support (GUI)

To enable multiple VLAN support in GUI, choose **Controller** -> **General**. In the **WGB Vlan Client** field, choose **Enable** from the drop-down list.

WGB Configurations

This section contains the commands on WGB to configure the PRP settings.

Enabling PRP Mode on WGB

The following commands enable the PRP submode on WGB.

```
iw3702(config)# dot11 wgb prp
iw3702(config-prp)# no shutdown
```

Note PRP is disabled by default after the **dot11 wgb prp** command is executed. To enable the PRP feature, execute the **no shutdown** command.

Submode PRP Configuration Commands

- **bvi-vlanid**—Configure vlan id of the BVI interface.
- **dummy-ip**—Configure dummy ip for the radio interface.
- **shutdown**—Disable the PRP feature.
- **exit**—Exit from prp sub-mode.
- **no**—Negate a command or set its defaults.

Configuring Dummy IP Address for Radio Interface

Use the following command to configure the dummy ip address for the radio interface to associate to the access point. By default the IP address will be assigned as 1.1.X.Y and 1.1.X.(Y+1) to 2.4G and 5G, where X and Y are the last 2 bytes of the WGB's Ethernet MAC address.

```
iw3702(config-prp)# dummy-ip <IP_addr>
```

Configuring Vlan for BVI Under PRP Mode

Use the following command to configure Vlan for BVI under PRP mode. If not configured, the BVI interface cannot get IP address via DHCP under PRP mode.

```
iw3702(config-prp)# bvi-vlanid <Vlan_Id>
```

Note The vlan configured by the **bvi-vlanid** command is reserved for BVI only. Do not use it for any wired clients.

Configuration Example of WGB

This section provides an example of the WGB configuration. .

```
hostname Vehicle
!
dot11 wgb prp
  no shutdown
  bvi-vlanid 900
```

```
!
dot11 ssid PRP1
   vlan 801
   authentication open
   no ids mfp client
!
dot11 ssid PRP2
   vlan 802
   authentication open
   no ids mfp client
!
interface Dot11Radio0
 no ip address
 load-interval 30
 !
 ssid PRP1
 !
 antenna gain 0
 antenna a-antenna
 packet retries 32 drop-packet
 station-role workgroup-bridge
 rts retries 32
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface Dot11Radio0.801
 encapsulation dot1Q 801
 bridge-group 100
 bridge-group 100 spanning-disabled
!
interface Dot11Radio1
 no ip address
 load-interval 30
 !
 ssid PRP2
 !
 antenna gain 0
 antenna a-antenna
 peakdetect
 packet retries 32 drop-packet
 station-role workgroup-bridge
 rts retries 32
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface Dot11Radio1.802
 encapsulation dot1Q 802
 bridge-group 200
 bridge-group 200 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 load-interval 30
 duplex auto
```

```
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.800
 encapsulation dot1Q 800
 bridge-group 50
 bridge-group 50 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 mac-address 0081.c408.c594
 ip address dhcp
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 route ip
!
workgroup-bridge unified-vlan-client
end
```

Aggregated Switch Configuration

```
interface FastEthernet1/0/1
 description ***AP1***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end

interface FastEthernet1/0/3
 description ***AP2***
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 201
 switchport trunk allowed vlan 201,801,802
 switchport mode trunk
end
interface FastEthernet1/0/4
 description ***PRP-Track-SW***
 switchport access vlan 801
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
end

interface FastEthernet1/0/5
 description ***PRP-Track-SW***
 switchport access vlan 802
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 no cdp enable
```

PRP Switch Configuration

```
interface PRP-channel1
 switchport mode trunk
interface GigabitEthernet1/1
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
interface GigabitEthernet1/2
 switchport mode trunk
 no ptp enable
 no cdp enable
 prp-channel-group 1
```

Verifying the Configuration

- Verify the packet replication and discarding details.

```
Vehicle# show dot11 wgb prp
available uplink count: 0
Index: 0 Status: DOWN Name: Dot11Radio0 Virtual-Dot11Radio0 AP: cc46.d616.ad84
Index: 1 Status: DOWN Name: Dot11Radio1 Virtual-Dot11Radio1 AP: cc46.d616.ad8a
======== Statistic counters ==========================
cnt_total_sent_A_: 5481     <= RADIO 0 REPLICATION
cnt_total_sent_B_: 940       <= RADIO 1 REPLICATION
cnt_tx_difference: 4541
cnt_total_received_A_: 337   <= RADIO 0 DISCARDING
cnt_total_received_B_: 56     <= RADIO 1 DISCARDING
cnt_rx_difference: 281
cnt_total_errors_A_: 0
cnt_total_errors_B_: 0
cnt_total_discard: 1              <= DISCARDED PACKET COUNT
cnt_discard_table_used_items: 0
max_duplicate_delay_: 0
```

- Display the roaming coordination status.

```
WGB# show coordinator status
current coordinator role is: Master
```

- Display the roaming coordination statistics.

```
WGB# show dot11 coordinator statistics
Vehicle#show dot11 coordinator statistics
Dot11 Roaming Coordination CURRENT Statistics:
                        Total Roaming Count: 1034
-------------------------------------------------------------------------------
      Scheduled Roaming: 1034                  Forced Roaming: 0
--------------------------------------    --------------------------------------
RATESHIFT          RSSI                   MAXRETRY           BEACON_LOST
0                  1034                   0                  0
--------------------------------------
Backoff     Timeout       Immediate
3           1             1030
-------------------------
```

```
Master Conflict: 4          Slave Conflict: 0
-------------------------------------------------
            Total Conflict Count: 4
Dot11 Roaming Coordination FULL Statistics:
                        Total Roaming Count: 1034
-------------------------------------------------------------------------------
      Scheduled Roaming: 1034                 Forced Roaming: 0
--------------------------------------    --------------------------------------
RATESHIFT          RSSI                   MAXRETRY           BEACON_LOST
0                  1034                   0                  0
--------------------------------------
Backoff     Timeout       Immediate
3           1             1030
------------------------
Conflict: 4
Roaming Coordination Settings
-------------------------------------------------------------------------------
Current Roaming Wait Timeout: 100 ms
```

Debug Commands

- Clear roaming coordination statistics.

  clear dot11 coordinator {**all**|**current**} **statistics**

- Clear PRP statistics.

  clear dot11 wgb prp statistics

- Debug roaming coordination.
  - Use the following command to view the primary-subordinate role and communication related debug information:

    debug coordinator {**detail**|**error**|**event**|**packet**|**timers**

  - Use the following command to view dot11 radio roaming coordination related debug information:

    debug dot11 coordinator {**detail**|**error**|**event**|**timers**

- Disable PRP debug messages on CLI.

  no debug dot11 prp {**bvi**|**config**|**uplink**|**forward**|**event**|**trailer**|**bypass**

- Debug PRP configuration.

  debug dot11 prp {**bvi**|**config**|**uplink**|**forward**|**event**|**trailer**|**bypass**

DLEP Client Support on WGB

Radio Aware Routing (RAR) is a mechanism where radios can interact with routing protocols (such as OSPFv3 or EIGRP, but only EIGRP is supported in this feature) to signal the appearance, disappearance, and link conditions of one-hop routing neighbors. The Dynamic Link Exchange Protocol (DLEP) is a radio aware routing (RAR) protocol, which addresses the challenges faced when merging IP routing and radio frequency (RF) communications.

The DLEP client support feature allows the workgroup bridge (WGB) to report radio link metrics to a router, for example, the Cisco Embedded Services Router (ESR). The WGB acts as the DLEP client, and the ESR acts as the DLEP server. The uplink selection is based on radio link quality metrics. For example, when two WGBs are deployed in a truck, there are redundancy radio links. The link with better radio quality while the truck is moving can be selected before the radio link completely goes down.

There are two methods of DLEP peer discovery, auto discovery and manual configuration. In this release, only the manual configuration method is supported.



Note This feature applies to the IW3700 Series. Only DLEP version 7 is supported.

Configuring the Physical Interface

The DLEP session is established between ESR and WGB through wired Ethernet interface. Static IP address needs to be configured under BVI interface. Subinterface of Gigabit Ethernet is also supported. But the subinterface should be configured with the same VLAN as the wireless interface. Here is an example:

```
interface GigabitEthernet0.811
encapsulation dot1Q 811
ip address 8.1.1.50 255.255.255.0
ip dlep local-port 38682 server-addr 8.1.1.211 server-port 55556
```

Configuring DLEP Local TCP Port and Server Address

Use the following command to enable the WGB to work as a DLEP client and configure the DLEP local port and server address.

```
wgb(config-if)# ip dlep local-port x server-addr x.x.x.x server-port x
```

Once configured, the WGB will listen on the configured local port for incoming DLEP connections.

Configuring Optional DLEP Timers

Configuring Heartbeat Timer

Use the following command to set the interval for the DLEP client to wait before declaring a DLEP server peer failed.

```
wgb(config-if)# ip dlep set heartbeat-timer x
```

The value range of the heartbeat timer is from 1 to 60 seconds. The default value is 5 seconds. The new heartheat timer value will take effect in the next new dlep session.

Configuring Neighbor Update Interval

Use the following command to set the interval for DLEP client to send neighbor update event in millisecond.

```
wgb(config-if)# ip dlep set neighbor-update-interval x
```

The value range of the neighbor update interval is from 100 to 5000 milliseconds. If not specified, the default value is 4000 milliseconds. The new neighbor update timer will take effect in the next new DLEP session. The WGB will send neighbor update message which contains radio metrics to the DLEP server every x milliseconds. Neighbor update interval will impact ESR response speed when link state changes. It is recommended to set a shorter neighbor-update-interval for high speed roaming. For example, you may set neighbor-update-interval to 500ms when WGB's moving speed is up to 80km/h.

Configuring DLEP Neighbors

The WGB uses the radio interface to detect neighbor and neighbor's metrics. Configure DLEP neighbor information under the radio interface.

Configuring Neighbor MAC Address

Use the following command to configure routing neighbor MAC address:

```
wgb(config-if)# dlep neighbor <mac address>
```

(Optional) Configuring RSSI Threshold and CDR Threshold

Use the following command to configure RSSI and CDR threshold:

```
wgb(config-if)# dlep neighbor <mac address> rssi-threshold x cdr-threshold x
```

Use the following command to configure RSSI threshold:

```
wgb(config-if)# dlep neighbor <mac address> rssi-threshold x
```

The value range of RSSI threshold is 1–100 dbm. The default value is 80 dbm. Once the RSSI value is above the configured RSSI threshold, the WGB will send neighbor update message including all the radio metrics to the DLEP server immediately.

Use the following command to configure CDR threshold:

```
wgb(config-if)# dlep neighbor <mac address> cdr-threshold x
```

The value range of CDR threshold is 7-6000 mbps. If not configured, no event will be triggered no matter what the current data rate is. Once configured, the neighbor update will be sent to the DLEP server when the current data rate is lower than the configured CDR threshold.

Note For roaming scenarios, the neighbor update will be sent out immediately after the roaming is completed.

Note There are two ways to trigger the metric update. One is the event trigger which is controlled by rssi-threshold or cdr-threshold. The other is the timer trigger which is controlled by the neighbor update interval.

Verifying DLEP Configuration

Displaying DLEP Configuration

The following command shows information about DLEP configurations, such as the server's IP address, port, heartbeat threshold, and peer-terminate-ack-timeout value.

```
WGB# show dlep config
 local tcp port=38682
 local ipv4=8.1.1.50
 router tcp port=55556
 router ipv4=8.1.1.211
 Type Description: no type description
 local ID=0
 peer offer tiemout=5 seconds
 peer heartbeat interval=5 seconds
 peer heartbeat missed threshold=3
 peer termination ack timeout=1000 milliseconds
 peer termination missed ack threshold=3
 neighbor up ack timeout=1000 milliseconds
 neighbor up missed ack threshold=3
 neighbor update interval timeout=4000 milliseconds
 neighbor activity timer=10 seconds
 neighbor down ack timeout=1000 milliseconds
 neighbor down missed ack threshold=3
```

Displaying DLEP Peer Information

The following command provides DLEP peer (DLEP server for WGB) information.

```
WGB# show dlep peers
DLEP Local Client 3
 Client ID=0
 Router ID=0
 Peer Description=
 Peer TCP port=55556
 Peer IPv4=8.1.1.211
 router offer timeout count=0
 peer heartbeat missed count=1
 peer term ack missed count=0
 peer term ack missed threshold=3
 neighbor up ack timeout=1000 milliseconds
 neighbor up missed ack threshold=3
 neighbor update interval timeout=4000 milliseconds
 neighbor activity timer=10 seconds
 neighbor down ack timeout=1000 milliseconds
 neighbor down missed ack threshold=3
```

```
 Metrics:
 RLQ TX=100 <0-100> RLQ RX=100 <0-100>
 Resources TX=100 <0-100> Resources RX=100 <0-100>
 Latency=0 milliseconds
 CDR TX=100000000 bps  CDR RX=100000000 bps
 MDR TX=100000000 bps  MDR RX=100000000 bps
```

Displaying DLEP Neighbors

The following command shows information of DLEP neighbors.

```
WGB# show dlep neighbors
DLEP Local Client 3
 Client ID=0
 Router ID=0
 Peer Description=
 Peer TCP port=55556
 Peer IPv4=8.1.1.211 Neighbor Local ID=5004
 Neighbor MAC= 00:50:56:8F:5F:FE
 activity timer=5 milliseconds
 Metrics:
 RLQ TX=100 <0-100> RLQ RX=100 <0-100>
 Resources TX=100 <0-100> Resources RX=100 <0-100>
 Latency=0 milliseconds
 CDR TX=144000000 bps  CDR RX=144000000 bps
 MDR TX=217000000 bps  MDR RX=217000000 bps
 Credits:
 MRW CREDITS=0 credits
 RRW CREDITS=0 credits
```

Displaying DLEP Client Counters

The following command shows packets counters of DLEP client.

```
WGB# show dlep counters
DLEP Client Counters
Last Clear Time = 13:13:51 UTC Mon Sep 15 2014
DLEP Server IP=8.1.1.111:55556
Peer Counters:
 RX Peer Discovery       0      TX Peer Offer             0
 RX Peer Offer           0      TX Peer Discovery         0
 RX Peer Init            0      TX Peer Init Ack          0
 RX Peer Init Ack        0      TX Peer Init              0
 RX Heartbeat            7449   TX Heartbeat              7278
 RX Peer Terminate       0      TX Peer Terminate Ack     0
 RX Peer Terminate Ack   0      TX Peer Terminate         0
 RX Peer Update Request  0      TX Peer Update Response   0
Neighbor Counters:
 RX Neighbor Up                0      TX Neighbor Up Ack                0
 RX Neighbor Up Ack            0      TX Neighbor Up                    0
 RX Neighbor Metric            0      TX Neighbor Metric                0
 RX Neighbor Down              0      TX Neighbor Down Ack              0
 RX Neighbor Down Ack          0      TX Neighbor Down                  0
 RX Neighbor Link Char Request  0      TX Neighbor Link Char Response    0
 RX Neighbor Link Char Response 0      TX Neighbor Link Char Request     0

Exception Counters:
 RX Invalid Message    0      RX Unknown Message        0
 Neighbor Not Found    0
Timer Counters:
```

```
Peer Heartbeat Timer               7278
Peer Terminate Ack Timer           0
Neighbor Init Ack Timer            0
Neighbor Update Ack Timer          0
Neighbor Metrics Interval Timer    0
Neighbor Terminate Ack Timer       0
```

Debug Commands



Note Contact your Cisco Support engineer for any troubleshooting support you may need.

The following command triggers the WGB to send peer terminate to the DLEP server to remove the specified peer:

```
wgb# clear dlep peer
```

The following command clears the DLEP client counters:

```
wgb# clear dlep counters
```

The following command displays the DLEP client process event information:

```
WGB# debug dlep client [detail]
```

The following command displays the DLEP neighbor transaction information:

```
WGB# debug dlep neighbor {<mac-address>|all|detail|error|metric|state}
  H.H.H    DLEP client neighbor MAC addr
  all      debugging information for all DLEP neighbors
  detail   DLEP neighbor detail information
  error    DLEP neighbor error information
  metrics  DLEP neighbor metrics information
  state    DLEP neighbor state machine information
```

The following commands display the DLEP peer transaction information:

```
WGB# debug dlep peer {detail|error|state|packet {detail|dump|incoming|outgoing}}
  detail  DLEP peer detail information
  error   DLEP peer error information
  packet  display DLEP peer packet information
  state   DLEP peer state machine information

WGB# debug dlep peer packet {detail|dump|incoming|outgoing}
  detail    display DLEP client packet details
  dump      display DLEP peer packet as a hex dump
  incoming  filter DLEP client incoming packets
  outgoing  filter DLEP client outgoing packets
```

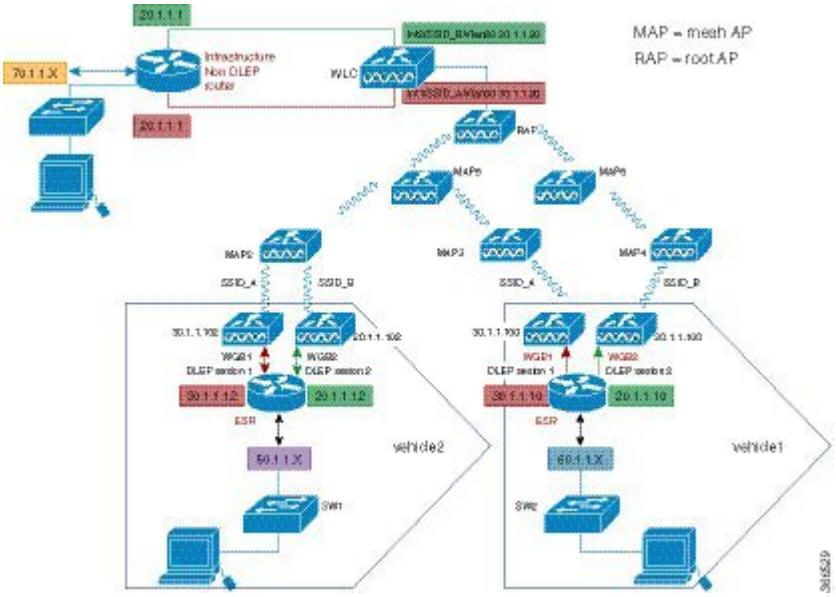
The following commands display the DLEP timer detail information:

```
WGB# debug dlep timer [detail
```

Configuration Example

This section contains a DLEP configuration example, including the configurations of WGB, controller, and ESR.

In this example, the DLEP server is implemented by ESR. Two WGBs act as DLEP clients. deployed in the same vehicle to provide redundant radio links. Each mesh AP (MAP) is configured with two SSIDs. Each WGB associates to a different SSID and establish a DLEP session with the ESR respectively. WGBs report radio link metrics to ESR through the DLEP sessions. Based on these radio link metrics, routing protocol of the ESR makes routing selection. The L2TPv3 tunnel is required to bridge the network behind ESR to be layer 2 adjacency across the IP networks.



Controller Configuration

Follow these steps to configure controller:

Procedure

Step 1 Configure AP to FlexConnect mode.

Step 2 Create two WLAN SSID for the redundant radio links.

Step 3 Configure CCKM.

WGB Configuration

For WGB fast secure roaming use case, it is recommended to configure CCKM and you need to configure CCKM on controller first. You are suggested to enable roaming coordinator when using DLEP.

Follow these steps to configure WGB:

Procedure

Step 1 Configure DLEP neighbor under radio interface.

Example:

```
dlep neighbor 000c.29da.a804 rssi-threshold 72 cdr-threshold 120
```

where the MAC address is the interface MAC of ISR-G2.

Step 2 Configure DLEP local port and server address under BVI1 or GigabitEthernet0 subinterface.

Example:

```
ip dlep local-port 38682 server-addr 100.100.1.2 server-port 55556
```

where the server address is the interface IP address of the ESR.

Step 3 Configure CCKM.

Example:

```
dot11 ssid k901
   vlan 901
   authentication open eap EAP-FAST
   authentication network-eap EAP-FAST
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
eap profile FAST
 method fast
dot1x credentials FAST
 username cisco
 password 0 cisco
interface Dot11Radio1
 no ip address
 encryption mode ciphers aes-ccm
 encryption vlan 901 mode ciphers aes-ccm
```

Step 4 Enable coordinator.

Example:

```
dot11 coordinator uplink single Dot11Radio1
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.0
 ip coordinator peer-addr 192.168.0.2
!
workgroup-bridge service-vlan 10
```

What to do next

The following examples show the configurations of WGB1 and WGB2:

WGB1 Configuration Example

```
dot11 ssid k901
   vlan 901
   authentication open eap EAP-FAST
   authentication network-eap EAP-FAST
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
dot11 coordinator uplink single Dot11Radio1
eap profile FAST
 method fast
dot1x credentials FAST
 username cisco
 password 0 cisco
interface Dot11Radio0
 no ip address
 shutdown
 !
 encryption vlan 901 mode ciphers aes-ccm
 !
 ssid k901
 !
packet retries 32 drop-packet
 station-role root
 rts retries 32
 infrastructure-client
!
interface Dot11Radio1
 no ip address
 !
 encryption mode ciphers aes-ccm
 !
 encryption vlan 901 mode ciphers aes-ccm
 !
 ssid k901
 !
peakdetect
station-role workgroup-bridge
 dlep neighbor 286f.7f75.0810 rssi-threshold 72 cdr-threshold 120
 mobile station scan 5220 5280
 mobile station period 1 threshold 76
 infrastructure-client
!
interface Dot11Radio1.901
 encapsulation dot1Q 901 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.901
 encapsulation dot1Q 901 native
 ip address 100.100.1.12 255.255.255.0
 ip dlep set neighbor-update-interval 500
 ip dlep local-port 38682 server-addr 100.100.1.2 server-port 55556
 bridge-group 1
```

```
 no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 duplex auto
 speed auto
 l2-filter bridge-group-acl
 bridge-group 1
no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.0
 ip coordinator peer-addr 192.168.0.2
!
interface BVI1
 mac-address 0081.c475.b73c
 ip address 100.100.1.11 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
workgroup-bridge unified-vlan-client
workgroup-bridge service-vlan 10
workgroup-bridge timeouts auth-response 300
workgroup-bridge timeouts assoc-response 300
```

WGB2 Configuration Example

```
dot11 ssid k902
   vlan 902
   authentication open eap EAP-Methods
   authentication network-eap EAP-Methods
   authentication key-management wpa version 2 cckm
   dot1x credentials FAST
   dot1x eap profile FAST
!
dot11 coordinator uplink single Dot11Radio1
!
power out-never
eap profile FAST
 method fast
!
no ipv6 cef
!
dot1x credentials FAST
 username cisco
 password 0 cisco
!
interface Dot11Radio0
 no ip address
 shutdown
 !
 encryption vlan 902 mode ciphers aes-ccm
 !
 ssid k902
 !
station-role root
 rts retries 32
 infrastructure-client
!
interface Dot11Radio1
 no ip address
```

```
 !
 encryption vlan 902 mode ciphers aes-ccm
 !
 ssid k902
 !
 antenna gain 0
 antenna a-antenna
 peakdetect
 ampdu transmit priority 6
 amsdu transmit priority 6
 packet retries 32 drop-packet
 station-role workgroup-bridge
 dlep neighbor 286f.7f75.0810 rssi-threshold 72 cdr-threshold 120
 mobile station scan 5220 5280
 mobile station period 1 threshold 76
 infrastructure-client
!
interface Dot11Radio1.902
 encapsulation dot1Q 902 native
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.902
 encapsulation dot1Q 902 native
 ip address 100.100.2.12 255.255.255.0
 ip dlep set neighbor-update-interval 500
 ip dlep local-port 38682 server-addr 100.100.2.2 server-port 55555
 bridge-group 1
 no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1
 no ip address
 duplex auto
 speed auto
 l2-filter bridge-group-acl
 bridge-group 1
no bridge-group 1 spanning-disabled
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 ip address 192.168.0.2 255.255.255.0
 ip coordinator peer-addr 192.168.0.1
!
interface BVI1
 mac-address 002a.1001.3eb0
 ip address 100.100.2.11 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
!
workgroup-bridge unified-vlan-client
workgroup-bridge service-vlan 10
workgroup-bridge timeouts auth-response 300
workgroup-bridge timeouts assoc-response 300
```

ESR Configuration

Follow these steps to configure ESR.



Note For more information of configuring DLEP on ESR, See the following chapter of the *Software Configuration Guide for the Cisco 5900 Embedded Services Routers* : https://www.cisco.com/c/en/us/td/docs/solutions/GGSG-Engineering/15-4-3M/config-guide/Configuration-Guide/DLEP.html

Procedure

Step 1 Configure DLEP under Ethernet interfaces.

Example:

```
interface Ethernet0/1
 description DLEP radio connection
 ip address 100.100.1.2 255.255.255.0
 ip dlep vtemplate 1 version v1.7 client ip 100.100.1.12 port 38682
 duplex auto
 speed auto
interface Ethernet0/2
 description DLEP radio connection
 ip address 100.100.2.2 255.255.255.0
 ip dlep vtemplate 2 version v1.7 client ip 100.100.2.12 port 38682
 duplex auto
 speed auto
```

Step 2 Configure the virtual template.

Example:

```
interface Virtual-Template 1
 ip unnumbered Ethernet0/1
 ipv6 enable
interface Virtual-Template 2
 ip unnumbered Ethernet0/2
```

Step 3 Configure the VMI interface.

Example:

```
interface vmi1
 ip unnumbered Ethernet0/1
 physical-interface Ethernet0/1
interface vmi2
 ip unnumbered Ethernet0/2
 physical-interface Ethernet0/2
```

Step 4 Configure EIGRP with static neighbor.

The link metrics of VMI interface map to the basic EIGRP interface parameters according to the following mapping table:

VMI	EIGRP
Current data rate	Bandwidth

VMI	EIGRP
Relative link quality resources	Reliability
Latency	Delay
Load	Load

For more information about this mapping, see Enhanced Interior Gateway Routing Protocol (EIGRP) Wide Metrics White Paper.

For the implementation of this feature, relative link quality (RLQ) is the main factor to be considered for link quality. So the default EIGRP metric weights should be updated using the **metric weights** command.

Note
When DLEP works between WGB and ESR, WGB reports CDR and RLQ. Default K values of EIGRP are: K1=K3=1, K2=K4=K5=0. Thus, by default, only CDR will impact ESR route selection. When calculating CDR, WGB will take negotiated data rate, RF status, retry counters, roaming event, and so on into consideration. For WGB low speed moving scenarios, CDR can guarantee the better link to be selected. But for WGB high speed moving scenario, or other cases where RF signal changes rapidly, the delay introduced by CDR calculation may cause large data interruption. To make ESR respond more quickly to link state change, you may change the K values of EIGRP case by case, for example, setting K5=<1-255>, to make RLQ impact more on route selection.

Example:

```
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 2.2.2.2 0.0.0.0
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
 neighbor 100.100.1.1 vmi1
 neighbor 100.100.2.1 vmi2
 eigrp router-id 2.2.2.2
```

Step 5 (Optional) Configure L2TPv3 tunnel, which is required by this example, but optional for basic DLEP configurations.

Example:

```
pseudowire-class R1R2
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
```

What to do next

ESR Configuration Example

```
hostname ESR-Vehicle
!
boot-start-marker
```

```
boot-end-marker
!
!
enable secret 5 $1$DecM$eQ2Pbh2rdVafrS9UngqnA0
enable password cisco123!
!
no aaa new-model
clock timezone CST 8 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip multicast-routing
!
no ip domain lookup
ip host ESR-Infra 209.165.200.10
ip cef
no ipv6 cef
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie size 8
!
multilink bundle-name authenticated
!
no virtual-template subinterface
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
```

```
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
license udi pid CISCO5921-K9 sn 9W30339RC8G
license platform throughput level c5921-x86-level5
!
redundancy
!
pseudowire-class R1R2
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 bfd interval 50 min_rx 50 multiplier 3
!
interface Ethernet0/1
 description DLEP radio connection
 ip address 100.100.1.2 255.255.255.0
 ip dlep vtemplate 1 version v1.7 client ip 100.100.1.12 port 38682
 duplex auto
 speed auto
!
interface Ethernet0/2
 description DLEP radio connection
 ip address 100.100.2.2 255.255.255.0
 ip dlep vtemplate 2 version v1.7 client ip 100.100.2.12 port 38682
 duplex auto
 speed auto
!
interface Ethernet0/3
 ip address 100.100.3.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no keepalive
!
interface Ethernet1/0
 no ip address
 duplex auto
 speed auto
 xconnect 209.165.200.10 123 encapsulation l2tpv3 pw-class R1R2
!
interface Ethernet1/1
 ip address 10.124.22.237 255.255.255.0
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Virtual-Template1
```

```
 ip unnumbered Ethernet0/1
 ipv6 enable
!
interface Virtual-Template2
 ip unnumbered Ethernet0/2
!
interface vmi1
 ip unnumbered Ethernet0/1
 ip dampening-change eigrp 100 5
 ipv6 address FE80::901 link-local
 physical-interface Ethernet0/1
!
interface vmi2
 ip unnumbered Ethernet0/2
 ip dampening-change eigrp 100 5
 ip hello-interval eigrp 100 60
 ip hold-time eigrp 100 180
 physical-interface Ethernet0/2
!
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 2.2.2.2 0.0.0.0
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
 neighbor 100.100.1.1 vmi1
 neighbor 100.100.2.1 vmi2
 eigrp router-id 2.2.2.2
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 10.0.0.0 255.0.0.0 Ethernet1/1
!
dialer-list 1 protocol ip permit
ipv6 ioam timestamp
!
access-list 1 permit 2.2.2.2
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
 no domain-lookup
line aux 0
line vty 0 4
 password cisco
 login
 transport input all
!
ntp mindistance 0
!
end
```

ISR-G2 Configuration

The ISR-G2 in this example can be replaced by an ESR with no need to configure DLEP.

Use these commands to configure L2TPv3 on ISR-G2. It is required by this example, but optional for basic DLEP configuration.

```
pseudowire-class R2R1
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
```

ISR-G2 Configuration Example

```
hostname ISR-G2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
!
ip dhcp excluded-address 100.100.0.1 100.100.0.10
ip dhcp excluded-address 100.100.1.1 100.100.1.10
ip dhcp excluded-address 100.100.2.1 100.100.2.10
!
ip dhcp pool vlan900
 network 100.100.0.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.0.1
 lease 0 0 30
!
ip dhcp pool vlan901
 network 100.100.1.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.1.1
 lease 0 0 30
!
ip dhcp pool vlan902
 network 100.100.2.0 255.255.255.0
 domain-name cisco.com
 default-router 100.100.2.1
 lease 0 0 30
!
no ip domain lookup
ip cef
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie size 8
!
ipv6 source-route
ipv6 dhcp pool vlan900-v6
 address prefix 2016:1:0:900::/112 lifetime 120 90
 dns-server 2016:1:0:900::3
 domain-name cisco.com
!
ipv6 multicast-routing
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
!
voice-card 0
!
license udi pid CISCO2911/K9 sn FGL205010MR
license accept end user agreement
```

```
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
!
username cisco privilege 15 secret 5 $1$MxQb$wNWP92nY5L3eFxnGHKs.60
!
redundancy
!
pseudowire-class R2R1
 encapsulation l2tpv3
 protocol l2tpv3 l2tp-defaults
 ip local interface Loopback1
!
interface Loopback1
 ip address 10.10.10.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.900
 encapsulation dot1Q 900
 ip address 100.100.0.1 255.255.255.0
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 1
 ipv6 address 2016:1:0:900::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd ra interval 30
 ipv6 dhcp server vlan900-v6
!
interface GigabitEthernet0/0.901
 encapsulation dot1Q 901
 ip address 100.100.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/0.902
 encapsulation dot1Q 902
 ip address 100.100.2.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 xconnect 2.2.2.2 123 encapsulation l2tpv3 pw-class R2R1
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 metric weights 0 1 0 1 0 1
 traffic-share min across-interfaces
 network 10.10.10.1 0.0.0.0
 network 100.100.0.0 0.0.0.255
 network 100.100.1.0 0.0.0.255
 network 100.100.2.0 0.0.0.255
```

```
 neighbor 100.100.2.2 GigabitEthernet0/0.902
 neighbor 100.100.1.2 GigabitEthernet0/0.901
 eigrp router-id 10.10.10.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 1 permit 10.10.10.1
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Viewing the Status of Workgroup Bridges (GUI)

Procedure

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB” if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

Step 3 See the details of any wired clients that are connected to a particular WGB as follows:

a) Click **Back** on the Clients > Detail page to return to the Clients page.

b) Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

Note
If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

c) Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows "WGB Client," and the rest of the text boxes on this page provide additional information for this client.

Viewing the Status of Workgroup Bridges (CLI)

Procedure

Step 1 See any WGBs on your network by entering this command:

show wgb summary

Step 2 See the details of any wired clients that are connected to a particular WGB by entering this command:

show wgb detail *wgb_mac_address*

Debugging WGB Issues (CLI)

Before you begin

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
  - **debug iapp all enable**—Enables debugging for IAPP messages.
  - **debug iapp error enable**—Enables debugging for IAPP error events.
  - **debug iapp packet enable**—Enables debugging for IAPP packets.
- Debug an roaming issue by entering this command:

  debug mobility handoff enable
- Debug an IP assignment issue when DHCP is used by entering these commands:
  - **debug dhcp message enable**
  - **debug dhcp packet enable**
- Debug an IP assignment issue when static IP is used by entering these commands:

- **debug dot11 mobile enable**
- **debug dot11 state enable**

Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller drops the following types of messages:

- ARP REQ from the distribution system for the WGB client
- ARP RPLY from the WGB client
- DHCP REQ from the WGB client
- DHCP RPLY for the WGB client

The following are some guidelines for non-Cisco workgroup bridges:

- The controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the work group bridge to the access point.



Note For FlexConnect APs in local switching, non-Cisco workgroup-bridge clients in bridged mode are supported using the **config flexconnect group** *group-name* **dhcp overridden-interface enable** command.

- When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.
- If you have clients that use PC virtualization software such as VMware, you must enable this feature.



Note We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

- You must enable the passive client functionality for all non-Cisco workgroup bridges.
- You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the **config dhcp proxy disable** command.
  - Enable DHCP boot broadcast by using the **config dhcp proxy disable bootp-broadcast enable** command.

This section contains the following subsection:

Restrictions for Non-Cisco Workgroup Bridges

- Only Layer 2 roaming is supported for WGB devices.
- Layer 3 security (web authentication) is not support for WGB clients.
- Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
- ARP poisoning detection does not work on a WLAN when the flag is enabled.
- VLAN select is not supported for WGB clients.
- Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the **config dhcp proxy disable** and **config dhcp proxy disable bootp-broadcast disable** commands.

  The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.

Cisco Wave 2 Access Points as Workgroup Bridges

Starting Release 8.8.120.0, Cisco Wave 2 Access Points can operate as Workgroup Bridges.

Universal WGB (UWGB) is a complementary mode of WGB feature that associates with any Root AP (Cisco or Non-Cisco RAP). When the WGB device is in UWGB mode this limits the association to one wired client.

Note Before changing the WGB to UWGB mode, ensure that the WGB has had a graceful exit from the Cisco controller.

This section contains the following subsections:

Guidelines and Restrictions on Cisco Wave 2 Access Points as Workgroup Bridges

- A maximum of 20 clients are supported behind a Cisco WGB device.
- The Workgroup Bridges mode is supported only on Cisco 2800, 3800, 4800, and 1560 Series Access Points.
- This feature functions only when you connect a power supply unit capable of providing minimum of 26W power to the Cisco Wave 2 AP.
- We recommend you to shut down the primary Ethernet port of the WGB before executing **clear wgb client all** command. If there is any traffic flowing in the WGB, then the above command might not clear all the WGB client entries.

Caution Before shutting down the primary Ethernet port of the WGB please make sure that the WGB is powered by an external power source and NOT Powered-Over-Ethernet.

- Access points in WGB mode do not support LAG.
- Access points in WGB mode do not support the Aux port.
- Before you change from WGB mode to UWGB mode, we recommend that you remove the client entry from the controller. This prevents association of the actual client instead of the client identity and getting added to the exclusion list.
- When associated with an SSID, the WGB MAC address is unique for each radio slot (0/1).
- IPv6 protocol is not supported.
- VLANs are not supported. For more information, see CSCvk32521.

Configuring Cisco Wave 2 Access Points Image (CLI)

Procedure

Step 1 Configure the boot path by entering this command:

(cisco-wave2-ap)#configure boot path {**1** | **2**}

Default value is *2*.

Step 2 Load the AP image from archives by entering one of the following commands:

To load the AP image, choose from one of the following CLIs:

- Reload after loading the image—**(cisco-wave2-ap)#archive download-sw /reload** *tftp://tftp-server-ip-address/tar-filename-along-with-path*
- No reload after loading the image—**(cisco-wave2-ap)#archive download-sw /no-reload** *tftp://tftp-server-ip-address/tar-filename-along-with-path*

Step 3 Configure the NTP server on the AP by entering this command:

(cisco-wave2-ap)#configure ntp server *ntp-server-ipv4-addr*

Step 4 View the current booth path by entering this command:

(cisco-wave2-ap)#show boot

Step 5 View the current NTP server settings by entering this command:

(cisco-wave2-ap)#show ntp

Configuring Cisco Wave 2 Access Points as Workgroup Bridge (CLI)

Before you begin

To prevent the connected wired client and switch behind the WGB using the same IP address which is observed in controller, we recommend you to disable the IGMP snooping using the command **no ip igmp snooping** on the WGB switch.

Procedure

Step 1 Enter the privileged mode in the AP by entering this command:

(cisco-wave2-ap)#enable

Step 2 Switch the AP to Workgroup Bridge mode by entering this command:

(cisco-wave2-ap)#ap-type workgroup-bridge

Step 3 Configure the IP address of the AP by entering this command:

- IPv4:
  - DHCP IP address—**(cisco-wave2-ap)#configure ap address ipv4 dhcp**
  - Static IP address—**(cisco-wave2-ap)#configure ap address ipv4 static** *ip-addr netmask gateway-ipaddr*

Step 4 Add a username for the AP management by entering this command:

(cisco-wave2-ap)#configure ap management add username *username* **password** *pwd* **secret** *secret-hint*

Step 5 Configure the AP hostname by entering this command:

(cisco-wave2-ap)#configure ap hostname *ap-name*

Configuring a Dot1X Credential (CLI)

Procedure

- Configure a dot1x credential by entering this command:

  (cisco-wave2-ap)#configure dot1x credential *profile-name* **username** *name* **password** *pwd*

- [Optional] Delete a dot1x profile by entering this command:

  (cisco-wave2-ap)#configure dot1x credential *profile-name* **delete**

- Deauthenticate WGB client by entering this command:

  (cisco-wave2-ap)#clear wgb client {**all** | **single** *mac-addr*}

Configuring an EAP Profile (CLI)

Procedure

Step 1 Configure the EAP profile method type by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **method** {**fast** | **leap** | **peap** | **tls**}

Step 2 Configure an EAP profile with a Trustpoint by entering this command:

An EAP profile can be associated with a Trustpoint with two types of certificates.

- Configuring EAP profile to Trustpoint with MIC certificate

  (cisco-wave2-ap)#configure eap-profile *profile-name* **trustpoint default**

- Configuring EAP profile to Trustpoint with CA certificate

  (cisco-wave2-ap)#configure eap-profile *profile-name* **trustpoint name** *trustpoint-name*

Step 3 Attaching the CA Trustpoint by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*}

Note
With the default profile, WGB uses the internal MIC certificate for authentication.

Step 4 Configure the 802.1X credentials profile by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **dot1x-credential** *profile-name*

Step 5 [Optional] Delete an EAP profile by entering this command:

(cisco-wave2-ap)#configure eap-profile *profile-name* **delete**

Step 6 View the WGB EAP dot1x profile summary by entering this command:

(cisco-wave2-ap)#show wgb eap dot1x credential profile

Step 7 View summary of the EAP profiles by entering this command:

(cisco-wave2-ap)#show wgb eap profile

Step 8 View summary of EAP and dot1x profiles by entering this command:

(cisco-wave2-ap)#show wgb eap profile all

Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

Step 1 Create a Trustpoint in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enrollment terminal**

Step 2 Authenticate a Trustpoint manually by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **authenticate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 3 Configure a private key size by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Generate a private key and Certificate Signing Request (CSR) by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enroll**

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

Step 6 Import the signed certificate in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **import certificate**

Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.

Step 7 [Optional] Delete a Trustpoint by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *trustpoint-name* **delete**

Step 8 View the Trustpoint summary by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint

Step 9 View the content of the certificates that are created for a Trustpoint by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint *trustpoint-name* **certificate**

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

Step 1 Enroll a Trustpoint in WGB using the server URL by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enrollment url** *ca-server-url*

Step 2 Authenticate a Trustpoint by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **authenticate**

This command will fetch the CA certificate from CA server automatically.

Step 3 Configure a private key size by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Enroll the Trust point by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enroll**

Request the digitally signed certificate from the CA server.

Step 6 Enable auto-enroll by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **auto-enroll enable** *renew-percentage*

You can disable auto-enrolling by using the disable syntax in the command.

Step 7 [Optional] Delete a Trustpoint by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *trustpoint-name* **delete**

Step 8 View the Trustpoint summary by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint

Step 9 View the content of the certificates that are created for a Trustpoint by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint *trustpoint-name* **certificate**

Step 10 View the PKI timer information by entering this command:

(cisco-wave2-ap)#show crypto pki timers

Configuring Manual Certificate Enrollment Using TFTP Server (CLI)

Procedure

Step 1 Specify the enrollment method to retrieve the CA certificate and client certificate for a Trustpoint in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enrollment tftp** *tftp-addr/file-name*

Step 2 Authenticate a Trustpoint manually by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **authenticate**

Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension ".ca" to the specified filename.

Step 3 Configure a private key size by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **key-size** *key-length*

Step 4 Configure the subject-name by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email*

Step 5 Generate a private key and Certificate Signing Request (CSR) by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **enroll**

Generates certificate request and writes the request out to the TFTP server. The filename to be written is appended with the extension ".req".

Step 6 Import the signed certificate in WGB by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **import certificate**

Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The WGB will attempt to retrieve the granted certificate via TFTP using the same filename and the file name append with ".crt" extension.

Step 7 View the Trustpoint summary by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint

Step 8 View the content of the certificates that are created for a Trustpoint by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint *trustpoint-name* **certificate**

Importing the PKCS12 format certificates from the TFTP server (CLI)

Procedure

Step 1 Import PKCS12 format certificate from the TFTP server by entering this command:

(cisco-wave2-ap)#configure crypto pki trustpoint *ca-server-name* **import pkcs12 tftp** *tftp-addr/file-name* **password** *pwd*

Step 2 View the Trustpoint summary by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint

Step 3 View the content of the certificates that are created for a Trustpoint by entering this command:

(cisco-wave2-ap)#show crypto pki trustpoint *trustpoint-name* **certificate**

Configuring an SSID Profile (CLI)

Procedure

- Choose one of the following authentication protocols for the SSID profile.

- Configure an SSID profile with Open Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication open**
- Configure an SSID profile with PSK Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication psk** *preshared-key* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**} }
- Configure an SSID profile with EAP Authentication—**(cisco-wave2-ap)#configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**} }

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

  (cisco-wave2-ap)#configure dot11radio *radio-nterface* **mode wgb ssid-profile** *profle-name*

- [Optional] Delete an SSID profile by entering this command:

  (cisco-wave2-ap)#configure ssid-profile *ssid-profile-name* **delete**

- View the summary of configured and connected SSIDs by entering this command:

  (cisco-wave2-ap)#show wgb ssid

- View the management, control, and data packet statistics by entering this command:

  (cisco-wave2-ap)#show wgb packet statistics

Configuring Radio Interface for Workgroup Bridges (CLI)

Procedure

- From the available two radio interfaces, before configuring WGB or UWGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode root-ap**

Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

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

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode wgb ssid-profile** *ssid-profile-name*

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

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **mode uwgb** *mac-addr* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* {**enable** | **disable** }

Note After configuring the uplink to the SSID profile, we recommend you to disable and enable the radio for the changes to be active.

- Configure the radio antenna by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **antenna** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}

- Enable encryption on a radio interface by entering this command:

  (cisco-wave2-ap)#configure dot11Radio *radio-int* **encryption mode ciphers aes-ccm**

- Configure the device channel rate by entering this command:

  (cisco-wave2-ap)#configure wgb mobile rate { **basic 6 9 18 24 36 48 54** | **mcs** *mcs-rate*}

- Configure the threshold duration and signal strength to trigger scanning by entering this command:

  (cisco-wave2-ap)#configure wgb mobile period *seconds thres-signal*

- Configure the static roaming channel by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan** *channel-number* **add**

- [Optional] Delete the mobile channel by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan** *channel-number* **delete**

- [Optional] Disable the mobile channel scanning by entering this command:

  (cisco-wave2-ap)#configure wgb mobile station interface dot11Radio *radio-int* **scan disable**

- Configure the beacon miss-count by entering this command:

  (cisco-wave2-ap)#configure wgb beacon miss-count *value*

  Default setting is set to disabled.

Note When you set the beacon miss-count value to 10 or lower, then the beacon miss-count gets disabled. Set the value to 11 or higher to enable this function.

- View the Wi-Fi station statistics by entering this command:

  (cisco-wave2-ap)#show wgb wifi *wifi-interface* **stats**

- View the radio antenna settings by entering this command:

  (cisco-wave2-ap)#show controllers dot11Radio *radio-interface* **antenna**

- View the mobile station channels scan configuration by entering this command:

  (cisco-wave2-ap)#show wgb mobile scan channel

- View the configuration that is stored in the NV memory by entering this command:

(cisco-wave2-ap)#show configuration

- View the running configuration in the device by entering this command:

  (cisco-wave2-ap)#show running-config



Note The output displays the configured parameters only.

- View the WGB forwarding details by entering this command:

  (cisco-wave2-ap)#show wgb forwarding all

Configuring Workgroup Bridge Timeouts (CLI)

Procedure

- Configure the WGB association response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb association response timeout *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.
- Configure the WGB authentication response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb authentication response timeout *response-millisecs*

  The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.
- Configure the Universal WGB client response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb uclient timeout *timeout-secs*

  The default timeout value is 60 seconds. The valid range is between 1 and 65535 seconds.
- Configure the WGB EAP timeout by entering this command:

  (cisco-wave2-ap)#configure wgb eap timeout *timeout-secs*

  The default value is 3 seconds. The valid range is between 2 and 60 seconds.
- Configure the WGB channel scan timeout by entering this command:

  (cisco-wave2-ap)#configure wgb channel scan timeout {**fast** | **medium** | **slow** }
- Configure the WGB DHCP response timeout by entering this command:

  (cisco-wave2-ap)#configure wgb dhcp response timeout *timeout-millisecs*

  The default value is 60 seconds. The valid range is between 1000 and 60000 milliseconds.
- View the WGB association summary by entering this command:

  (cisco-wave2-ap)#show wgb dot11 association

Configuring Bridge Forwarding for Workgroup Bridge (CLI)

The Cisco Wave 2 AP as Workgroup Bridge recognizes the Ethernet clients only when the traffic has the bridging tag.

We recommend setting the WGB bridge client timeout value to default value of 300 seconds, or less in environment where change is expected, such as:

- Ethernet cable is unplugged and plugged back.
- Endpoint is changed.
- Endpoint IP is changed (static to DHCP and vice versa).

If you require to retain the client entry in the WGB table for a longer duration, we recommend you to increase the client WGB bridge timeout duration.

Procedure

Step 1 Add a WGB client using the MAC address by entering this command:

(cisco-wave2-ap)#configure wgb bridge client add *mac-addr*

Step 2 Configure the WGB bridge client timeout by entering this command:

(cisco-wave2-ap)#configure wgb bridge client timeout *timeout-secs*

Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.

Step 3 View the WGB wired clients over the bridge by entering this command:

(cisco-wave2-ap)#show wgb bridge

Step 4 View the WGB Gigabit wired clients over the bridge by entering this command:

(cisco-wave2-ap)#show wgb bridge wired gigabitEthernet *giga-wire-interface*

Step 5 View the WGB bridge radio interface summary by entering this command:

(cisco-wave2-ap)#show wgb bridge dot11Radio *interface-number*