Workgroup Bridges

- Cisco WGBs, on page 1
- Third-Party WGBs and Client VMs, on page 42

Cisco WGBs

Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point. The lightweight access point treats the WGB as a wireless client.

A Cisco IOS AP as a WGB using the Cisco IOS 15.2 or later releases support Protected Extensible Authentication Protocol (PEAP) with the controller.

*Figure 1: WGB Example*
If the lightweight access point fails, the WGB attempts to associate to another access point.

The following are some guidelines for Cisco Workgroup Bridges:

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

Enable the workgroup bridge mode on the WGB as follows:

- On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.
- On the WGB access point CLI, enter the `station-role workgroup-bridge` command.

See the sample WGB access point configuration in the WGB Configuration Example section.

- The following features are supported for use with a WGB:
  - Guest N+1 redundancy
  - Local EAP
  - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, 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.
Workgroup Bridge (WGB) Downstream Broadcast On Multiple VLANs

Cisco Wireless LAN Controller (WLC) 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
  - 1552H/SA/SD/WU Series

Supported AP mode:
- Local mode
- Bridge mode

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 WLC. 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 WLC.

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 WLC, 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.
When you have multiple VLAN configurations on WGB, you need to configure the encryption cipher mode and keys as the following examples show:

```
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.

---

**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 topology 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:
- WLC 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.
**WLC Configuration (CLI Only)**

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

```bash
(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 WLC 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. Gig1 will connect to a non-PRP port on the PRP switch or connect to a peer Gig1 port directly.
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 10, you should configure the local/peer coordinator address under sub interface 10.
   
   ```
   WGB(config)# interface GigabitEthernet1.10
   WGB(config-subif)# encapsulation dot1q 10
   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. The following sample configuration can avoid the bridge loop.

---

**Note**

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

WLC Configuration

Note
For more information about WLC 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 WLC.

Configuration of AP

1. Configure AP to FlexConnect mode and join WLC.
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 BVII
  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 BVII
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 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
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
```
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
```

```
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

The Cisco Wireless LAN Controller (WLC) 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:

- WLC 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 5: Concurrent Wireless Transmission Via One WGB With Dual Radio and Paired With One PRP Switch, on page 15 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.
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]
```

WLC Configurations

This section contains the configurations on WLC 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 by 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 by GUI

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

Enabling Multiple Vlan Support by 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 by 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
tipv6 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

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 Master-Slave 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.
### 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 heartbeat 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 timeout=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:
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

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]
```

- `<mac-address>`: 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, WLC, 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 establishes 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.
WLC Configuration

Follow these steps to configure WLC:

**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 security reason, it is recommended to configure CCKM for fast roaming and you need to configure CCKM on WLC 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 wpaa 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 wpaa 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
tcp

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
  amdu 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
  12-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


Procedure

Step 1

Configure DLEP under Ethernet interfaces.

Example:

interface Ethernet0/1
description DLEP radio connection
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:

<table>
<thead>
<tr>
<th>VMI</th>
<th>EIGRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current data rate</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>Relative link quality resources</td>
<td>Reliability</td>
</tr>
<tr>
<td>Latency</td>
<td>Delay</td>
</tr>
<tr>
<td>Load</td>
<td>Load</td>
</tr>
</tbody>
</table>

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.
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
capsulation 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$eQ2Pbh2rdVafYs9Ungqna0
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 1.1.1.1
  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 1E003353 04031317 43697363
  6F204C69 36356573 69666720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E003353 04031317 43697363 6F204C69 36356573 69666720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 01F0030
  82010A02 82010100 A68CB96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655DBD7 9471380D 8711441E 1A8F071A 9CAE6388 8A3EE520
  1C394D78 462EF339 C659F715 B98C0A59 58B83CBE 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E8D0 DBF6FD1C 60B1FD18 FFC69C9C 6FA69857 A217DE7 104FDC5E EA2956AC
  7930A8EB 285436A0 C847A2C5 DAB553EB 69A9A5A3 58E9F3E3 C0B23C5F 58BD7188
  68E69E91 20F320E7 948E71D7 AE38CC84 F10684C7 4EB8E00F 539BA428 42C68BB7
  C7479096 B4CB2B62 EA2F502D C7BD82A4 681D95B 8EB250FC 50D5DFB8 8F2D7191
  C55F0D76 61F9A4CD 3D9D2327 A88B03BD 4E6D7069 7CBADFP8 DF5F4368 95135E44
  DFC76C6F 04DD7DF1 02030100 01A34230 43000E06 03551D0F 010FF04 04032021
  063000F6 0551D013 0101FF04 05300301 01FF301D 0603551D 0EE14604 1449DC85
  4B3D31E5 1B3E6A17 60A8F333 3D384C75 E8300D06 092A8648 86F70D01 01080500
  03820101 00507F24 D932A66 86025D9F E83A8B5C 604DF6B0 49631C78 240DA905
  604EDCDE FF4FEDEB 776CC5FD CD6D57F2 D046BE1E 3A5673AB 9093D3B1 6C9E39DB
  D989B7B E40C0DBE 1AECAC92 2189BB5C 86858668 CD9B8464 5755B146 8DFD66A8
  467A3F4D 4D565700 64ADF0F0D CF830515 3C04F7FC 21E878AC 11BA9CD2 55A9232C
  7CA7B7E7 C1AF74FE 152E99B7 B1FC9B9B E973DE7F 58DDEEE6 C71E3B49 1765309B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BEE 1A4A8229 C371C3E9 39F08678
  80DDC1D6 D6BACECA EEBCC7FC9 8428787B 35202CDD 60E4616A B623CDBD 230E3AF8
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862F0AE 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 1.1.1.1 123 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

close-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

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 an 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 1.1.1.1 255.255.255.255
  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 1.1.1.1 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 1.1.1.1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 1 permit 1.1.1.1
!
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
Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with lightweight access points.

- Only WGBs in client mode (which is the default value) are supported. Those WGBs in infrastructure mode are not supported. Perform one of the following to enable client mode on the WGB:
  
  - On the WGB access point GUI, choose Disabled for the Reliable Multicast to WGB parameter.
  
  - On the WGB access point CLI, enter the no infrastructure client command.

  ![Note] VLANs are not supported for use with WGBs.

- The following features are not supported for use with a WGB:
  
  - Idle timeout
  
  - Web authentication

  ![Note] If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted.

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.

- The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied.
• 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 delete a WGB record from the controller, all of the WGB wired clients’ records 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.

• Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the `config wgb vlan enable` command.

• The `dot11 arp-cache` global configuration command that you can enter on the access point that is in WGB mode is not supported.

• WGB clients do not show enc-cipher and AKM because they are wired clients. WGB APs, however, show correct values of enc-cipher and AKM.

### WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

```
ap# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# dot11 ssid WGB_with_static_WEP
ap(config-ssid)# authentication open
ap(config-ssid)# guest-mode
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
```
Verify that the WGB is associated to an access point by entering this command on the WGB:

```
show dot11 association
```

Information similar to the following appears:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address IP address Device Name Parent State
000b.8581.6aee 10.11.12.1 WGB-client map1 - Assoc
ap#
```

### 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`

Third-Party WGBs and Client VMs

Information About 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.

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.