Configure Work Group Bridge (WGB) Multiple VLAN Support

Contents

Introduction

This document explanis how to configure a WGB to support multiple Virtual Local Area Networks (VLANs) under different scenarios.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge in AireOS Wireless LAN Controller (WLC) and Access Point (AP) in autonomous mode configuration.

Components Used

- WLC v8.2
- Autonomous AP v15.3(3)JD4
- Control And Provisioning of Wireless Access Points (CAPWAP) AP
- Switch 802.1q capable

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

WGB with Multiple VLANs Associated to a CAPWAP AP

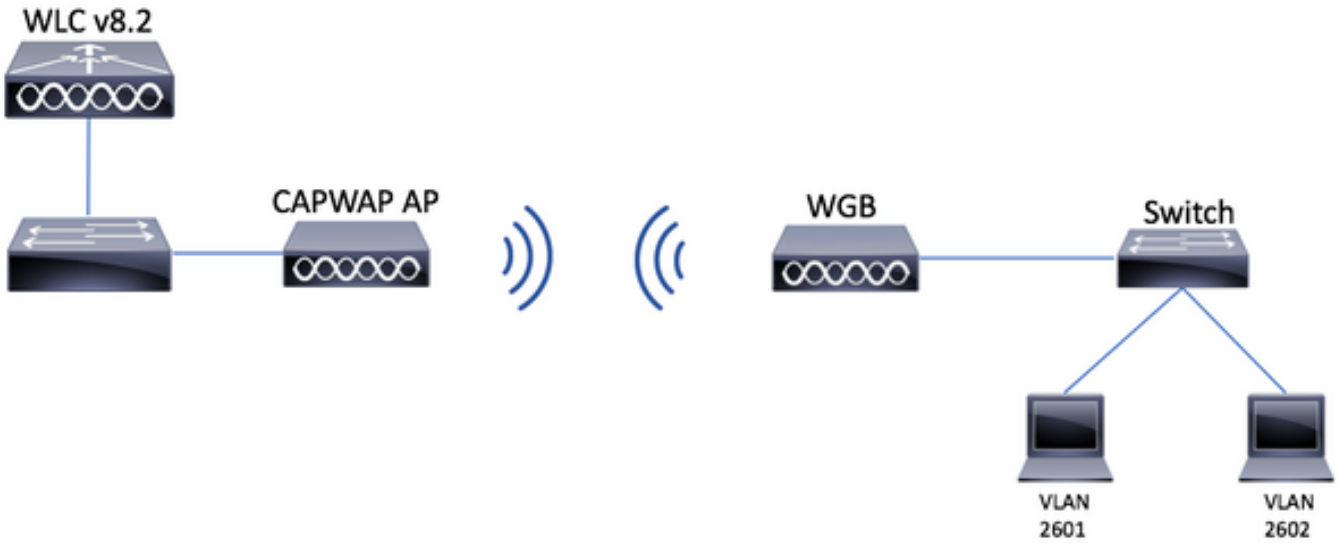
This example explains how to configure a WGB supporting multiple VLANs, associated to a CAPWAP AP. The Access Point can be in Local mode or Bridge Mode (Mesh). This scenario requires that the WGB is connected to a switch that support 802.1q, otherwise WGB cannot support multiple VLANs. In this example the WGB is connected to a Cisco Switch 3560.

If the switch does not support 802.1q, all the clients will be assigned to the native VLAN.

In this example WGB is assigned to VLAN 210 and the clients connected to the switch behind the WGB are assigned to VLAN 2601 and 2602.

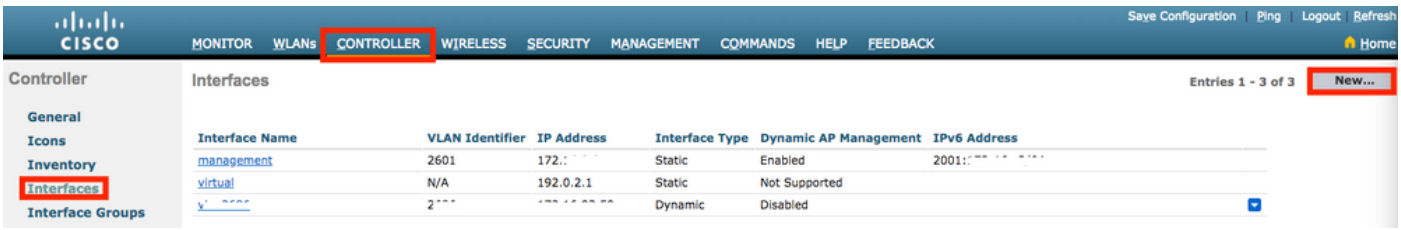
The WLC must also have configured dynamic interfaces that belongs to client's vlan. In this example the WLC must have dynanic interfaces on VLAN 2601, 2602 and 210.

Network Diagram

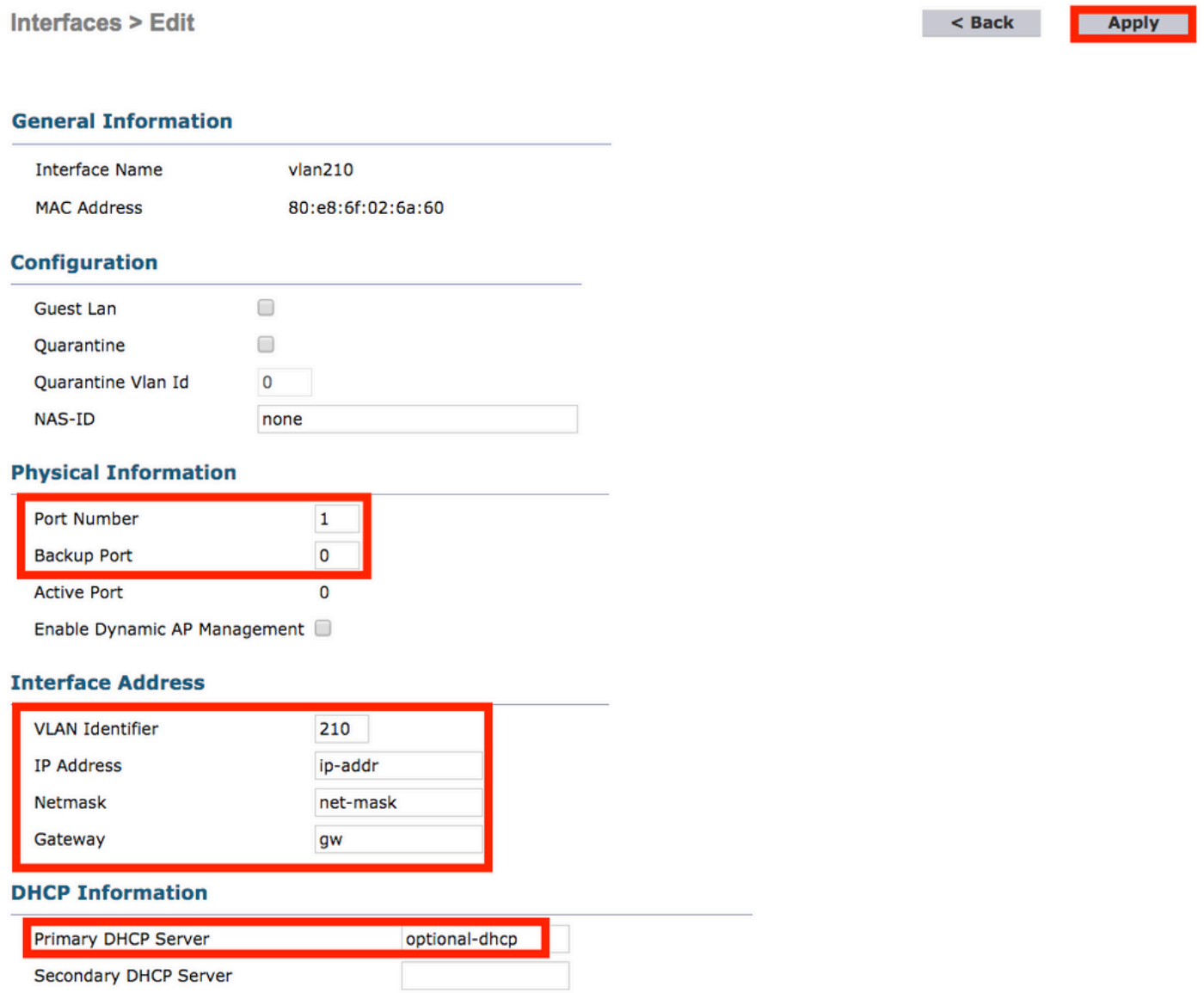


WLC Configuration

Step 1. Open the WLC's Graphical User Interface (GUI) and navigate to **CONTROLLER > Interfaces** to verify the current dynamic interfaces configured on the WLC.If the needed vlans are not already configured, click **New** and add the needed ones.

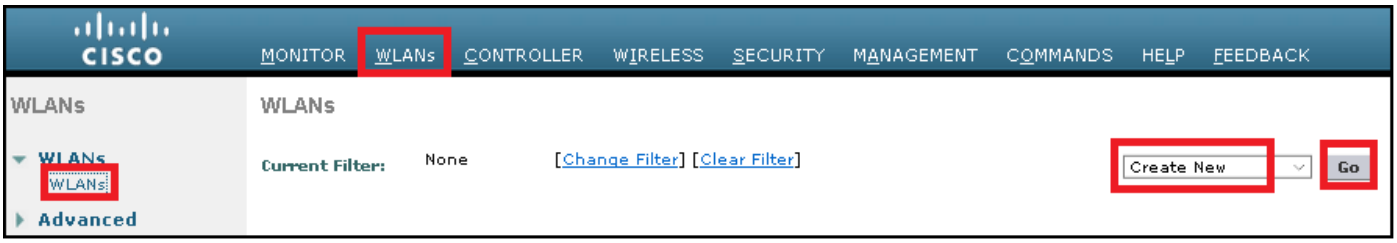


Enter the interface's information

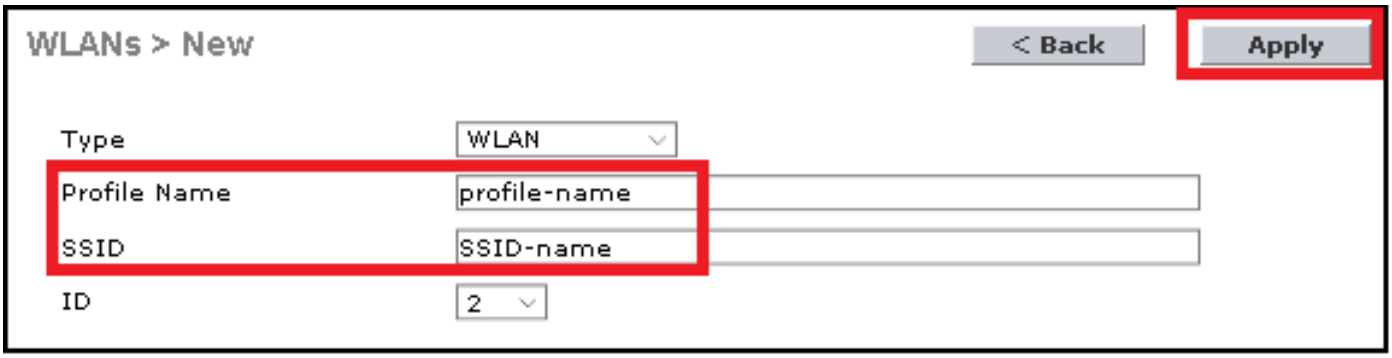


Note: If your WLC has Link Aggregation (LAG) enabled, you are not able to select a port number.

Step 2. Navigate to **WLANs > Create New > Go.**



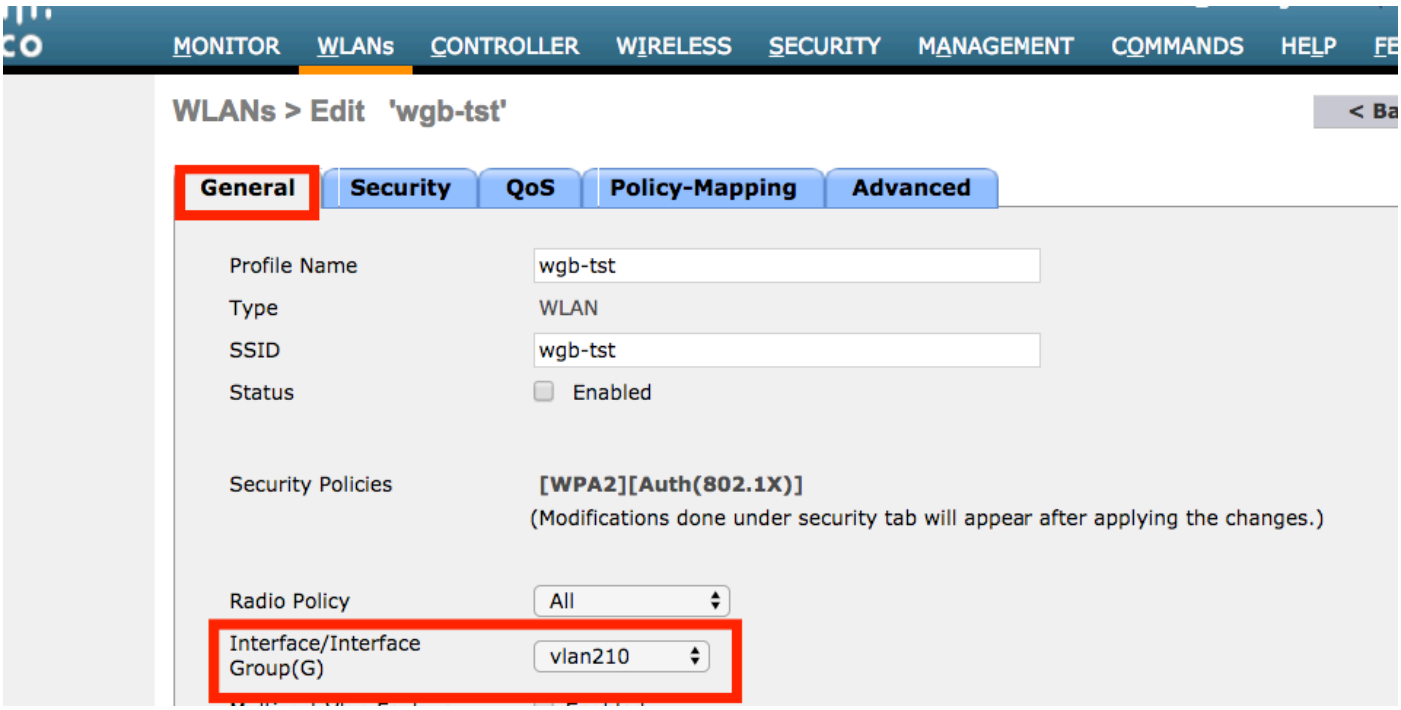
Step 3. Choose a name for the SSID and profile, then click **Apply.**



CLI:

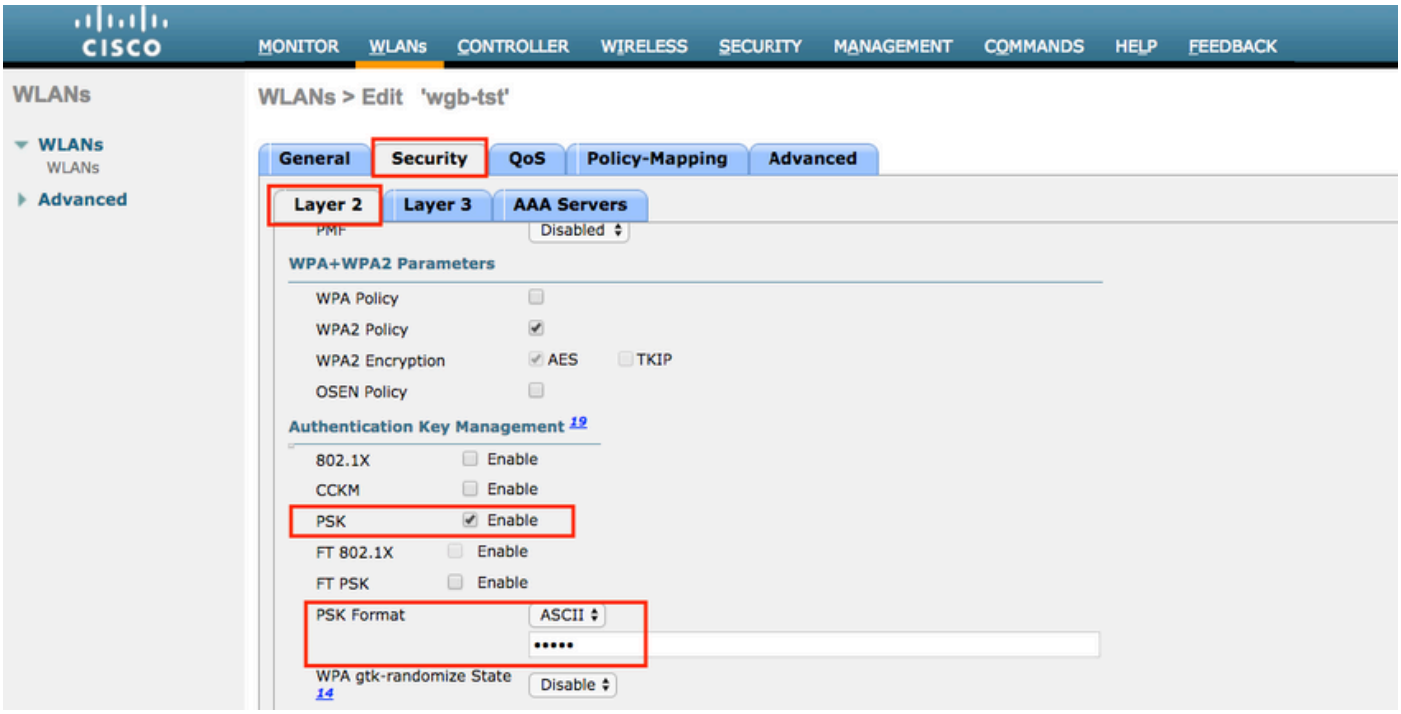
```
> config wlan create <id> <profile-name> <ssid-name>
```

Step 4. Assign the WGB's native VLAN to the WLAN

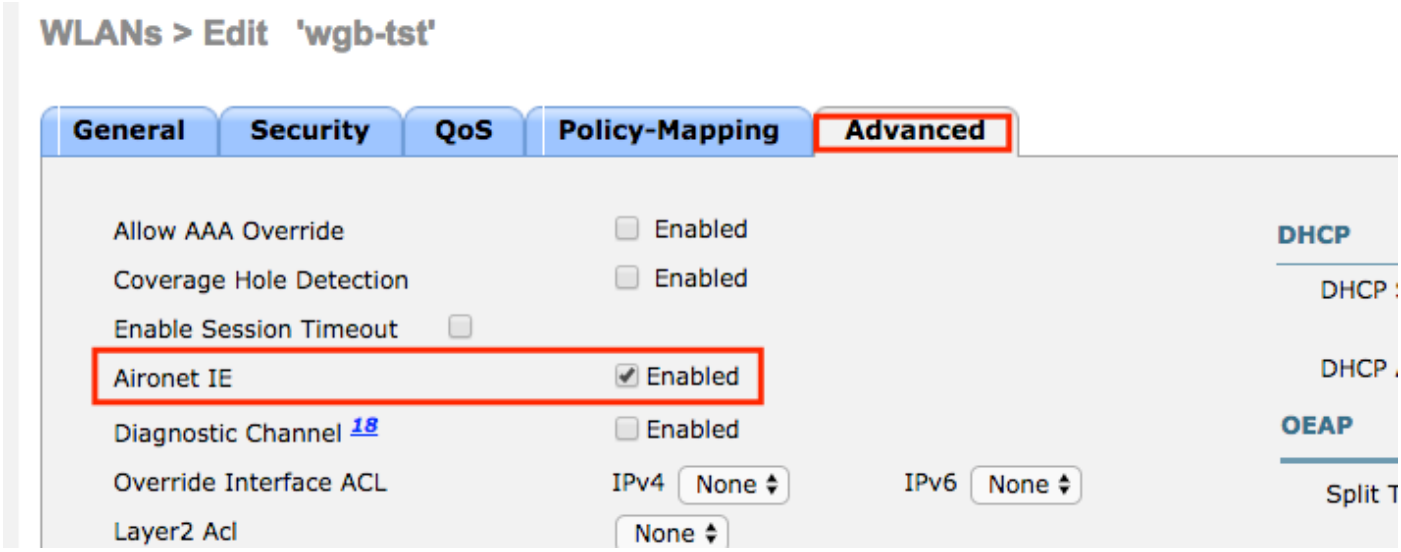


Step 5. Assign the Pre Shared Key that WGB uses to associate to the SSID.

Navigate to **Security > Layer 2 > Authentication Key Management.** Select **PSK** and fill the password.



Step 6. Ensure that the WLAN has **Aironet IE** enable, otherwise WGB wont be able to associate.



Note: In this example the SSID is using WPA2/PSK security, if you need to configure the WLAN with a stronger security method like WPA2/802.1x you can consult the this link: [802.1x authentication with PEAP, ISE 2.1 and WLC 8.3]

Step 7. Enable the WLC to support multiple VLANs from a WGB

```
>config wgb vlan enable
```

WGB Configuration

Step 1. Add the subinterfaces needed per VLAN. In this example VLANs 210 (Native), 2601 and 2602 are

added to the WGB configuration.

```
WGB# config t
WGB# interface dot11radio 0.210
WGB# encapsulation dot1q 210 native

WGB# interface dot11radio 0.2601
WGB# encapsulation dot1q 2601
WGB# bridge-group 21

WGB# interface dot11radio 0.2602
WGB# encapsulation dot1q 2602
WGB# bridge-group 22

WGB# interface dot11radio 1.210
WGB# encapsulation dot1q 210 native

WGB# interface dot11radio 1.2601
WGB# encapsulation dot1q 2601
WGB# bridge-group 21

WGB# interface dot11radio 1.2602
WGB# encapsulation dot1q 2602
WGB# bridge-group 22

WGB# interface gigabit 0.210
WGB# encapsulation dot1q 210 native

WGB# interface gigabit 0.2601
WGB# encapsulation dot1q 2601
WGB# bridge-group 21

WGB# interface gigabit 0.2602
WGB# encapsulation dot1q 2602
WGB# bridge-group 22
```

Note: Bridge group of subinterfaces 2601 and 2602 are 21 and 22 because the valid range for bridge groups is from 1 to 255.

Note: Bridge group for subinterface 210 is not specified because when the native VLAN is assigned to a subinterface, it automatically assigns bridge group 1.

Step 2. Create the Service Set Identifier (SSID).

In this example the SSID is using WPA2/PSK, if you need the WGB to associate to an SSID with a stronger security method like WPA2/802.1x you can consult this link:

Workgroup Bridges with PEAP Authentication Configuration Example

```
WGB# config t
```

```
WGB# dot11 ssid wgb-tst
WGB# vlan 210
WGB# authentication open
WGB# authentication key-management wpa version 2
WGB# infrastructure-ssid
WGB# wpa-psk ascii 0 cisco123
```

Step 3. Add the SSID into the interface used to associate to the CAPWAP AP.

This step also set the AP as work group bridge with the command **station-role workgroup-bridge**.

Note: In this example the WGB uses its 2.4GHz Interface to associate to the CAPWAP AP, if you need the WGB to associate with its 5GHz interface add this configuration to the interface Dot11Radio1.

```
WGB# config t
WGB# interface Dot11Radio0
WGB# encryption vlan 210 mode ciphers aes-ccmp
WGB# ssid WGB-tst
WGB# station-role workgroup-bridge
```

Step 4. Enable the WGB Unified VLAN feature.

This command will allow the WGB to inform the WLC in which VLAN the clients should be assigned.

```
WGB# config t
WGB# workgroup-bridge unified-vlan-client
```

Switch configuration

Step 1. Create the VLANs.

```
SW# config t
SW# vlan 210, 2601, 2602
```

Step 2. Configure the port where the WGB is pluged in.

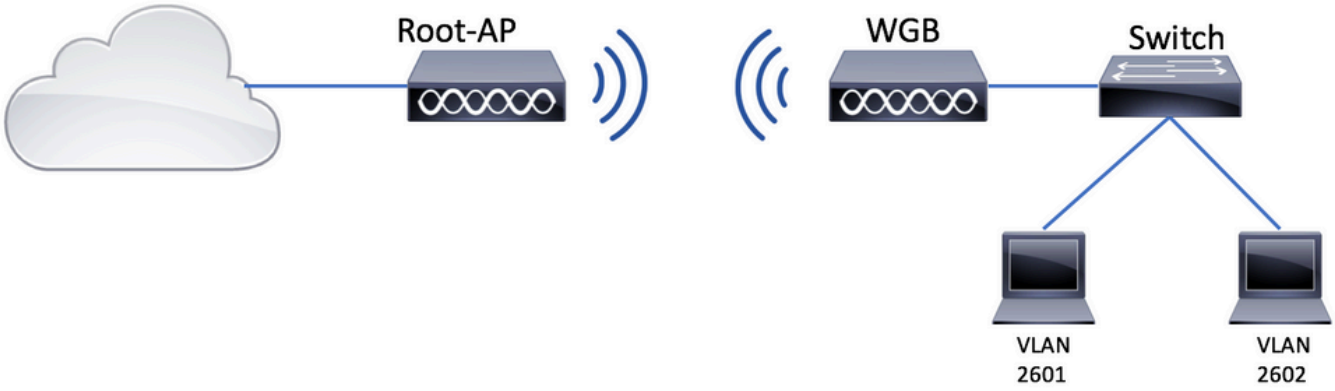
```
SW# config t
SW# interface <interface-id>
SW# switchport mode trunk
SW# switchport trunk native vlan 210
SW# switchport trunk allowed vlan 210, 2601, 2602
```

Step 3. Assign the interfaces where the clients are pluged in to the needed VLAN.

```
SW# config t
SW# interface <interface-id>
SW# switchport mode access
SW# switchport access vlan <vlan-id>
```

WGB with 802.1q Switch behind and Multiple VLANs Associated to an Autonomous AP in Root Mode.

Network Diagram



Root AP Configuration

Step 1. Add the subinterfaces needed per VLAN.

In this example VLANs 210 (Native), 2601 and 2602 are added to the Root AP configuration as instructed in Step 1 of WGB with Multiple VLANs Associated to a CAPWAP AP - WGB Configuration.

Step 2. Create the Service Set Identifier (SSID).

In this example the SSID is using WPA2/PSK, if you need to configure the Root AP with a SSID with a stronger security method like WPA2/802.1x you can consult the this link:

Configure SSIDs and VLANs on Autonomous APs

```
Root-AP# config t
Root-AP# dot11 ssid WGB-tst
Root-AP# vlan 210
Root-AP# authentication open
Root-AP# authentication key-management wpa version 2
Root-AP# infrastructure-ssid
Root-AP# wpa-psk ascii 0 cisco123
```

Step 3. Add the SSID to the interface that Root AP will use to broadcast the SSID.

Note: In this example the Root-AP uses its 2.4GHz Interface to broadcast the SSID, if you need the Root-AP to broadcast it with its 5GHz interface add this configuration to the interface Dot11Radio1.

```
Root-AP# config t
Root-AP# interface Dot11Radio0
Root-AP# encryption vlan 210 mode ciphers aes-ccmp
Root-AP# ssid WGB-tst
Root-AP# infrastructure-client
Root-AP# no shut
```

The command **infrastructure-client** allows the Root AP to respect the VLAN assignment that WGB have for its wired clients. Without this command, the Root AP will assign all the clients to the native VLAN.

WGB configuration

Step 1. Add the subinterfaces needed per VLAN.

In this example VLANs 210 (Native), 2601 and 2602 are added to the Root AP configuration as instructed in Step 1 of WGB with Multiple VLANs Associated to a CAPWAP AP - WGB Configuration.

Step 2. Create the Service Set Identifier (SSID).

In this example the SSID is using WPA2/PSK, if you need the WGB to associate to an SSID with a stronger security method like WPA2/802.1x you can consult the this link:

Workgroup Bridges with PEAP Authentication Configuration Example

```
WGB# config t
WGB# dot11 ssid WGB-tst
WGB# vlan 210
WGB# authentication open
WGB# authentication key-management wpa version 2
WGB# infrastructure-ssid
WGB# wpa-psk ascii 0 cisco123
```

Step 3. Add the SSID into the interface used to associate to the CAPWAP AP.

This step also set the AP as work group bridge with the command **station-role workgroup-bridge.**

Note: In this example the WGB uses its 2.4GHz Interface to associate to the CAPWAP AP, if you need the WGB to associate with its 5GHz interface add this configuration to the interface Dot11Radio1.

```
WGB# config t
WGB# interface Dot11Radio0
WGB# encryption vlan 210 mode ciphers aes-ccmp
WGB# ssid WGB-tst
WGB# station-role workgroup-bridge
WGB# no shut
```

Switch configuration

You can follow same configuration for switch on WGB with Multiple VLANs Associated to a CAPWAP AP.

WGB with no Switch Behind and Multiple VLANs Associated to an Autonomous AP in Root Mode.

This example allows WGB to use 2 different VLANs (native and another one), if you need to have more than two VLANs then you will need to add a 802.1q switch capable behind the WGB and connect the clients on it. Then follow the instructions on WGB with 802.1q Switch behind and Multiple VLANs Associated to an Autonomous AP in Root Mode.

Network Diagram

Root AP Configuration

Step 1. Add the subinterfaces needed per VLAN.

Subinterfaces configuration is the same as seen on Step 1 of WGB with Multiple VLANs Associated to a CAPWAP AP - WGB Configuration, but in this case you only need to configure VLAN 210 (Native) and VLAN 2602 (client VLAN).

Step 2. Create the Service Set Identifier (SSID).

In this example the SSID is using WPA2/PSK, if you need to configure the Root AP with a SSID with a stronger security method like WPA2/802.1x you can consult the this link:

Configure SSIDs and VLANs on Autonomous APs

```
Root-AP# config t
Root-AP# dot11 ssid WGB-tst
Root-AP# vlan 210
Root-AP# authentication open
Root-AP# authentication key-management wpa version 2
```

```
Root-AP# infrastructure-ssid
Root-AP# wpa-psk ascii 0 cisco123
```

Step 3. Add the SSID to the interface that Root AP will use to broadcast the SSID.

Note: In this example the Root-AP uses its 2.4GHz Interface to broadcast the SSID, if you need the Root-AP to broadcast it with its 5GHz interface add this configuration to the interface Dot11Radio1.

```
Root-AP# config t
Root-AP# interface Dot11Radio0
Root-AP# encryption vlan 210 mode ciphers aes-ccmp
Root-AP# ssid WGB-tst
Root-AP# infrastructure-client
Root-AP# no shut
```

The command **infrastructure-client** allows the Root AP to respect the VLAN assignment that WGB have for its wired clients. Without this command, the Root AP assigns all the clients to the native VLAN.

WGB configuration

Step 1. Add the subinterfaces needed per VLAN. In this example VLANs 210 (Native) and 2601 are added to the WGB configuration.

Subinterfaces configuration is the same as seen on Step 1 of WGB with Multiple VLANs Associated to a CAPWAP AP - WGB Configuration, but in this case you will only need to configure VLAN 210 (Native) and VLAN 2602 (client VLAN).

Step 2. Create the Service Set Identifier (SSID).

In this example the SSID is using WPA2/PSK, if you need the WGB to associate to an SSID with a stronger security method like WPA2/802.1x you can consult the this link:

Workgroup Bridges with PEAP Authentication Configuration Example

```
WGB# config t
WGB# dot11 ssid WGB-tst
WGB# vlan 210
WGB# authentication open
WGB# authentication key-management wpa version 2
WGB# infrastructure-ssid
WGB# wpa-psk ascii 0 cisco123
```

Step 3. Add the SSID into the interface used to associate to the CAPWAP AP.

This step also set the AP as work group bridge with the command **station-role workgroup-bridge.**

Note: In this example the WGB uses its 2.4GHz Interface to associate to the CAPWAP AP, if you need the WGB to associate with its 5GHz interface add this configuration to the interface Dot11Radio1.

```
WGB# config t
WGB# interface Dot11Radio0
WGB# encryption vlan 210 mode ciphers aes-ccmp
WGB# ssid WGB-tst
WGB# station-role workgroup-bridge
WGB# no shut
```

Step 4. Specify the client VLAN.

```
WGB# config t
WGB# workgroup-bridge client-vlan 2601
```

Verify

Run this command to verify WGB is associated to Root AP, and that Root AP can see the wired clients connected behind the WGB:

<#root>

```
WGB# show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [WGB-tst] :

MAC Address    IP address      IPV6 address                            Device        Name            Par
00eb.d5ee.da70 200.200.200.4   ::                                      ap1600-Parent Root-AP         -

Root-AP# show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [WGB-tst] :

MAC Address    IP address      IPV6 address                            Device        Name            Par
0035.1ac1.78c7 206.206.206.2   ::                                      WGB-client    -               00f
00f6.6316.4258 200.200.200.3   ::                                      WGB           WGB             sel
```