

# Configuration de la prise en charge de plusieurs VLAN WGB (Work Group Bridge)

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[WGB avec plusieurs VLAN associés à un AP CAPWAP](#)

[Diagramme du réseau](#)

[Configuration WLC](#)

[Configuration WGB](#)

[Configuration du commutateur](#)

[WGB avec commutateur 802.1q derrière et plusieurs VLAN associés à un point d'accès autonome en mode racine.](#)

[Diagramme du réseau](#)

[Configuration du point d'accès racine](#)

[configuration WGB](#)

[Configuration du commutateur](#)

[WGB sans commutateur derrière et plusieurs VLAN associés à un point d'accès autonome en mode racine.](#)

[Diagramme du réseau](#)

[Configuration du point d'accès racine](#)

[configuration WGB](#)

[Vérifier](#)

---

## Introduction

Ce document explique comment configurer un WGB pour prendre en charge plusieurs réseaux locaux virtuels (VLAN) dans différents scénarios.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir des connaissances de base sur le contrôleur LAN sans fil (WLC) et le point d'accès (AP) AireOS en configuration de mode autonome.

### Composants utilisés

- WLC v8.2
- AP autonome v15.3(3)JD4

- Point d'accès de contrôle et de mise en service des points d'accès sans fil (CAPWAP)
- Commutateur compatible 802.1q

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.

## Configurer

### WGB avec plusieurs VLAN associés à un AP CAPWAP

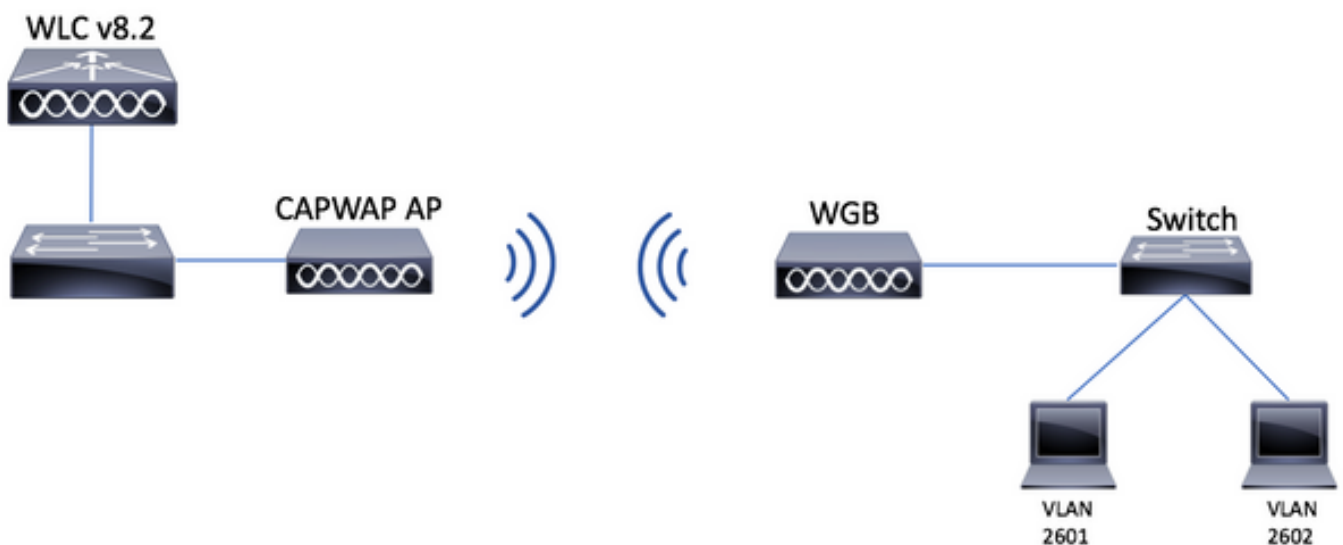
Cet exemple explique comment configurer un WGB prenant en charge plusieurs VLAN, associés à un point d'accès CAPWAP. Le point d'accès peut être en mode Local ou Bridge (Mesh). Ce scénario nécessite que le WGB soit connecté à un commutateur qui prend en charge 802.1q, sinon le WGB ne peut pas prendre en charge plusieurs VLAN. Dans cet exemple, le WGB est connecté à un commutateur Cisco 3560.

Si le commutateur ne prend pas en charge la norme 802.1q, tous les clients sont affectés au VLAN natif.

Dans cet exemple, WGB est attribué au VLAN 210 et les clients connectés au commutateur derrière le WGB sont attribués aux VLAN 2601 et 2602.

Le WLC doit également avoir configuré des interfaces dynamiques qui appartiennent au VLAN du client. Dans cet exemple, le WLC doit avoir des interfaces dynamiques sur VLAN 2601, 2602 et 210.

Diagramme du réseau



### Configuration WLC

Étape 1. Ouvrez l'interface graphique utilisateur du WLC et accédez à CONTROLLER > Interfaces

pour vérifier les interfaces dynamiques actuelles configurées sur le WLC. Si les VLAN nécessaires ne sont pas déjà configurés, cliquez sur New et ajoutez les VLAN nécessaires.

The screenshot shows the Cisco WLC Controller interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected. On the left, a sidebar menu has 'Interfaces' highlighted. The main content area is titled 'Interfaces' and shows a table with 3 entries. A 'New...' button is visible in the top right corner of the table area.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	2601	172.17.0.1	Static	Enabled	2001::1
virtual	N/A	192.0.2.1	Static	Not Supported	
vlan210	210	192.168.210.1	Dynamic	Disabled	

The screenshot shows the 'Interfaces > New' configuration page. The 'CONTROLLER' tab is selected. The left sidebar has 'Interfaces' highlighted. The main form has two input fields: 'Interface Name' with the value 'vlan210' and 'VLAN Id' with the value '210'. 'Back' and 'Apply' buttons are visible at the top right.

Interface Name	vlan210
VLAN Id	210

Saisissez les informations de l'interface

Interfaces > Edit

< Back

Apply

### General Information

Interface Name	vlan210
MAC Address	80:e8:6f:02:6a:60

### Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

### Physical Information


Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Management	<input type="checkbox"/>

### Interface Address

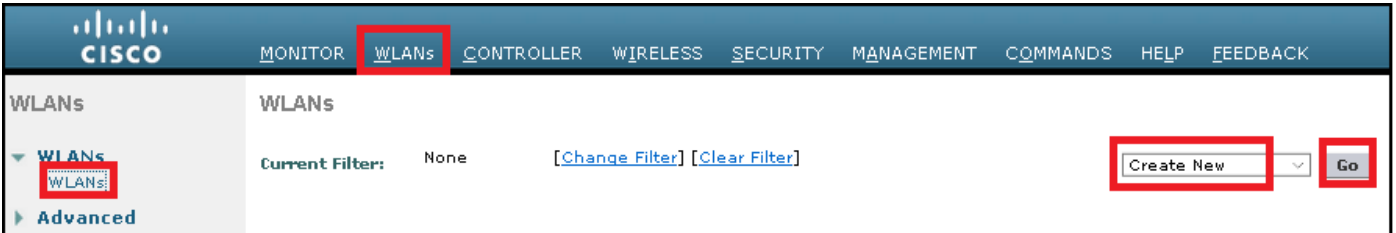
VLAN Identifier	210
IP Address	ip-addr
Netmask	net-mask
Gateway	gw

### DHCP Information

Primary DHCP Server	optional-dhcp
Secondary DHCP Server	

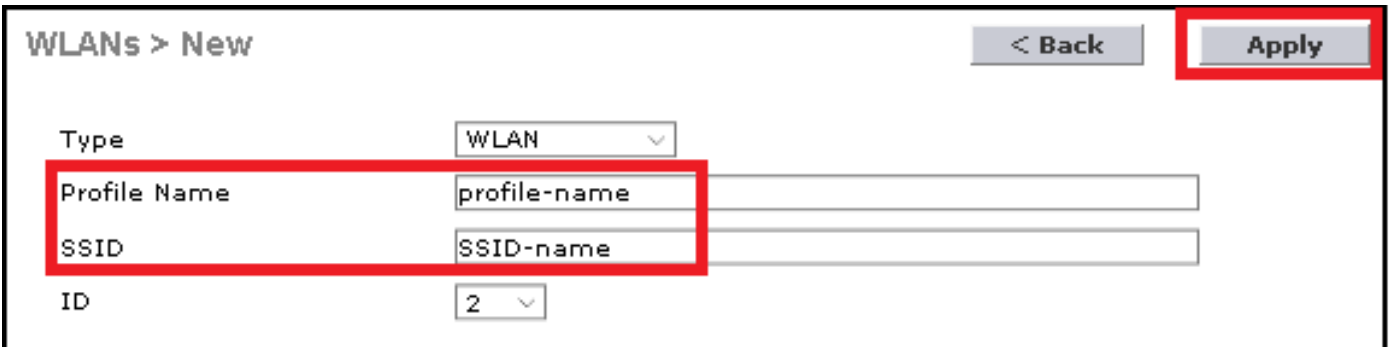
 Remarque : si l'agrégation de liens (LAG) est activée sur votre WLC, vous ne pouvez pas sélectionner un numéro de port.

Étape 2. Accédez à WLANs > Create New > Go.



The screenshot shows the Cisco WLC GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu is expanded, showing 'WLANs' and 'Advanced'. The 'WLANs' page displays 'Current Filter: None' and links for '[Change Filter]' and '[Clear Filter]'. A 'Create New' button with a dropdown arrow and a 'Go' button are visible in the top right corner.

Étape 3. Choisissez un nom pour le SSID et le profil, puis cliquez sur Apply.

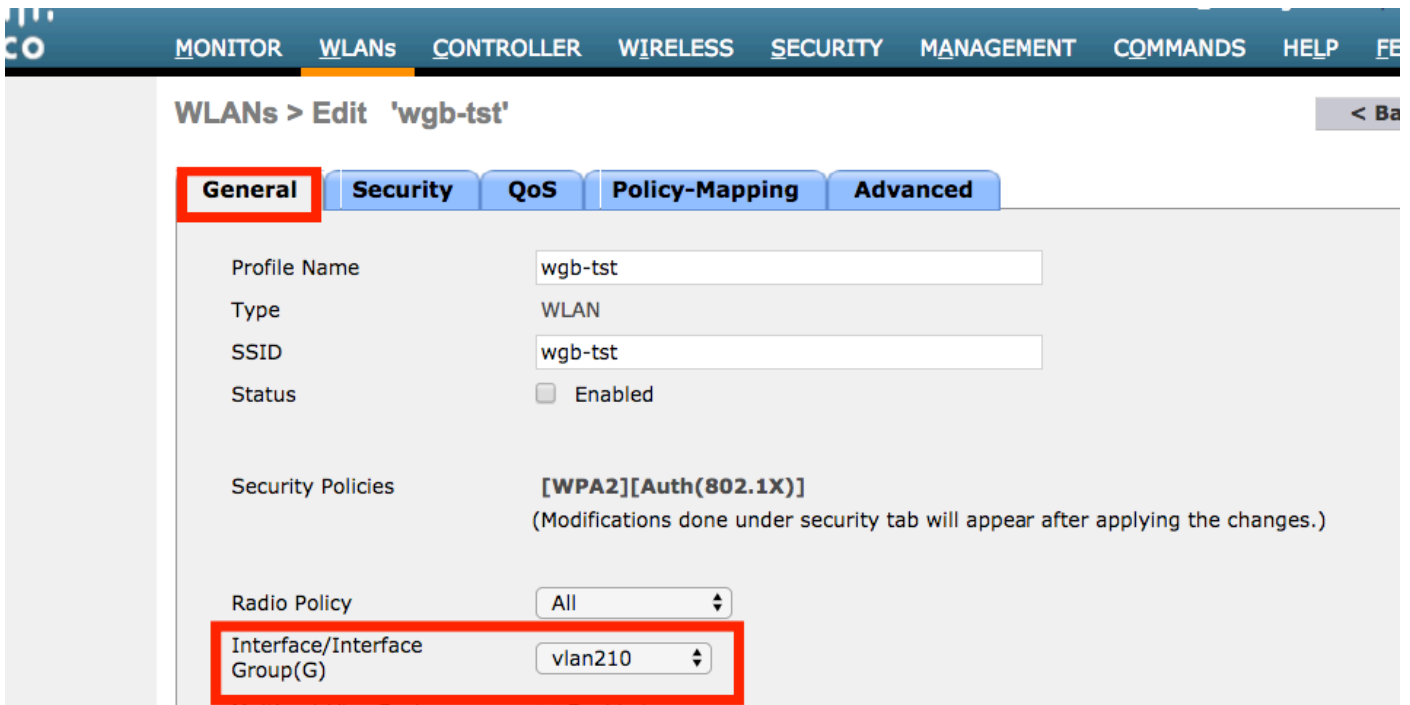


The screenshot shows the 'WLANs > New' form. It includes a '< Back' button and an 'Apply' button. The form fields are: 'Type' (WLAN), 'Profile Name' (profile-name), 'SSID' (SSID-name), and 'ID' (2). The 'Profile Name' and 'SSID' fields are highlighted with a red box.

CLI :

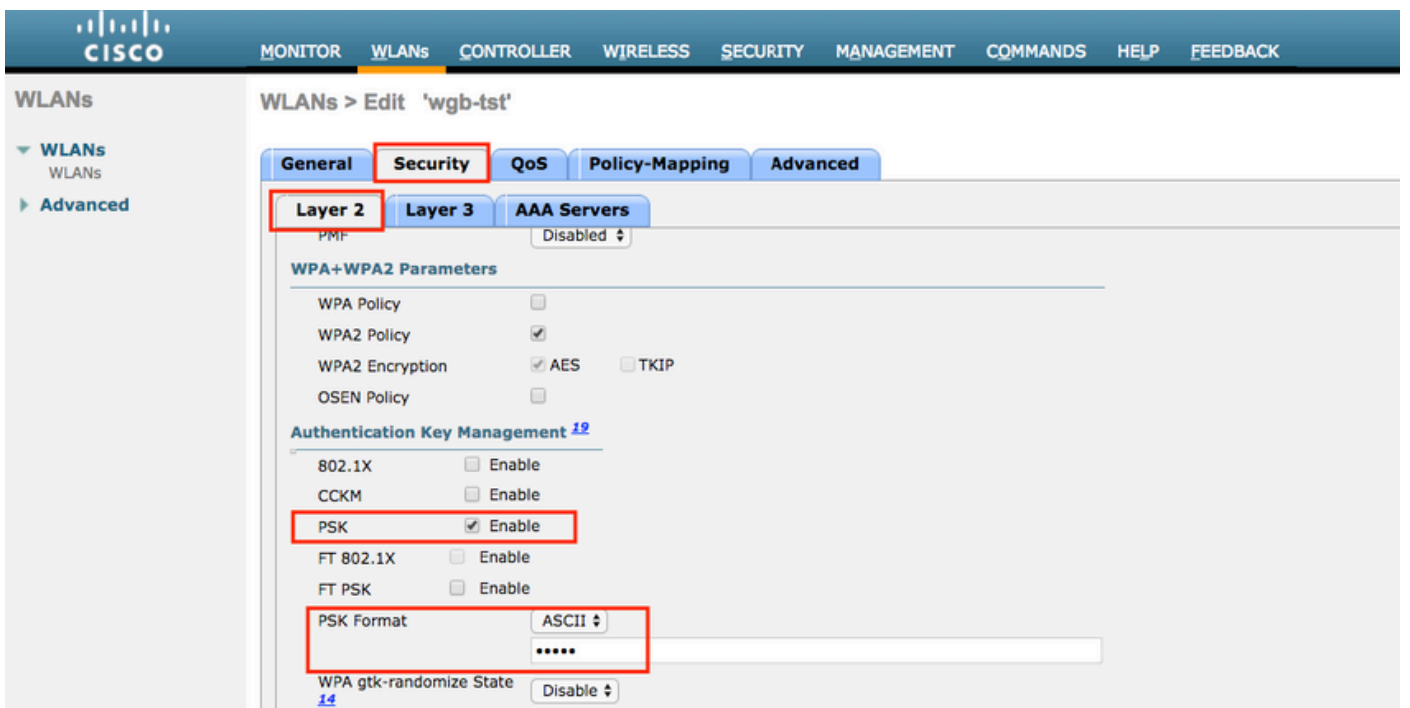
```
> config wlan create <id> <profile-name> <ssid-name>
```

Étape 4. Attribuer le VLAN natif du WGB au WLAN



Étape 5. Attribuez la clé pré-partagée que WGB utilise pour associer au SSID.


Accédez à Security > Layer 2 > Authentication Key Management. Sélectionnez PSK et saisissez le mot de passe.



Étape 6. Assurez-vous que le WLAN a Aironet IE activé, sinon WGB ne sera pas en mesure de s'associer.

## WLANs > Edit 'wgb-tst'

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input type="checkbox"/>	Enabled		<b>DHCP</b>
Coverage Hole Detection	<input type="checkbox"/>	Enabled		DHCP :
Enable Session Timeout	<input type="checkbox"/>			DHCP :
Aironet IE	<input checked="" type="checkbox"/>	Enabled		<b>OEAP</b>
Diagnostic Channel <a href="#">18</a>	<input type="checkbox"/>	Enabled		Split T
Override Interface ACL	IPv4	None	IPv6	None
Layer2 Acl		None		

 Remarque : Dans cet exemple, le SSID utilise la sécurité WPA2/PSK, si vous devez configurer le WLAN avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter le lien suivant : [authentification 802.1x avec PEAP, ISE 2.1 et WLC 8.3](#)

Étape 7. Activer le WLC pour prendre en charge plusieurs VLAN à partir d'un WGB

```
>config wgb vlan enable
```

### Configuration WGB

Étape 1. Ajoutez les sous-interfaces nécessaires par VLAN. Dans cet exemple, les VLAN 210 (natifs), 2601 et 2602 sont ajoutés à la configuration WGB.

```
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
```

---

 Remarque : les groupes de ponts des sous-interfaces 2601 et 2602 sont 21 et 22, car la plage valide pour les groupes de ponts est comprise entre 1 et 255.

---

 Remarque : le groupe de ponts pour la sous-interface 210 n'est pas spécifié car lorsque le VLAN natif est attribué à une sous-interface, il attribue automatiquement le groupe de ponts 1.

---

Étape 2. Créez l'identifiant SSID (Service Set Identifier).

Dans cet exemple, le SSID utilise WPA2/PSK, si vous avez besoin que le WGB s'associe à un SSID avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter ce lien :


[Exemple de configuration de ponts de groupe de travail avec authentification PEAP](#)

```
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
```

Étape 3. Ajoutez le SSID à l'interface utilisée pour l'association au point d'accès CAPWAP.

Cette étape définit également le point d'accès comme pont de groupe de travail avec la commande `station-role workgroup-bridge`.

---

 Remarque : dans cet exemple, le WGB utilise son interface 2,4 GHz pour s'associer au point d'accès CAPWAP, si vous avez besoin que le WGB s'associe à son interface 5 GHz, ajoutez cette configuration à l'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
```

Étape 4. Activez la fonctionnalité WGB Unified VLAN.

Cette commande permettra au WGB d'informer le WLC dans quel VLAN les clients doivent être assignés.

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

Configuration du commutateur

Étape 1. Créez les VLAN.

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

Étape 2. Configurez le port sur lequel le WGB est connecté.

```
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
```

Étape 3. Attribuez les interfaces sur lesquelles les clients sont connectés au VLAN requis.

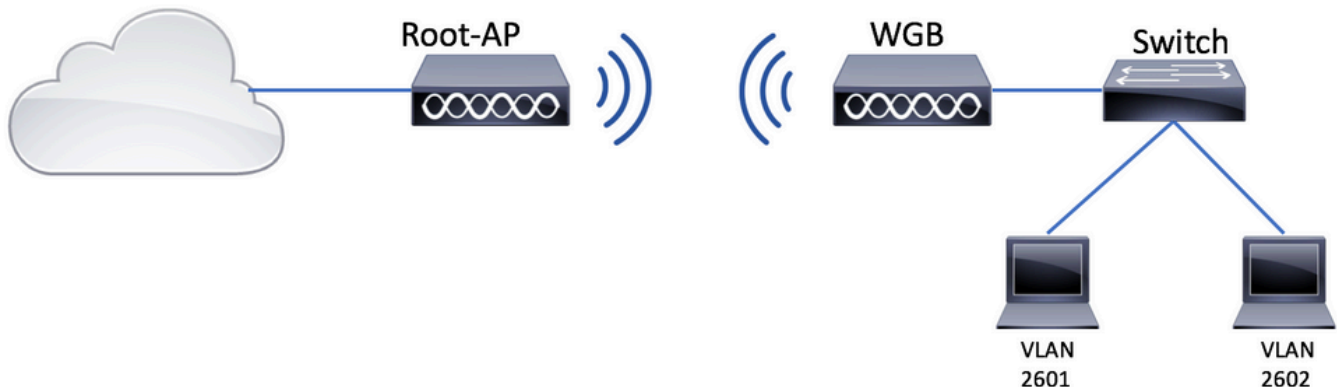
```
SW# config t
SW# interface <interface-id>
SW# switchport mode access
SW# switchport access vlan <vlan-id>
```

WGB avec commutateur 802.1q derrière et plusieurs VLAN associés à un AP



autonome en mode racine.

Diagramme du réseau



Configuration du point d'accès racine

Étape 1. Ajoutez les sous-interfaces nécessaires par VLAN.

Dans cet exemple, les VLAN 210 (natifs), 2601 et 2602 sont ajoutés à la configuration du point d'accès racine comme indiqué à l'étape 1 de [WGB with Multiple VLANs Associated to a CAPWAP AP AP - WGB Configuration](#).

Étape 2. Créez l'identifiant SSID (Service Set Identifier).


Dans cet exemple, le SSID utilise WPA2/PSK, si vous devez configurer le point d'accès racine avec un SSID avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter le lien suivant :

[Configurer les SSID et les VLAN sur les points d'accès autonomes](#)

```
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
```

Étape 3. Ajoutez le SSID à l'interface que le point d'accès racine utilisera pour diffuser le SSID.

---

 Remarque : dans cet exemple, le point d'accès racine utilise son interface 2,4 GHz pour

---



diffuser le SSID, si vous avez besoin du point d'accès racine pour le diffuser avec son interface 5 GHz, ajoutez cette configuration à l'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
```

La commande infrastructure-client permet au point d'accès racine de respecter l'affectation de VLAN que WGB a pour ses clients filaires. Sans cette commande, l'AP racine affectera tous les clients au VLAN natif.

## configuration WGB

Étape 1. Ajoutez les sous-interfaces nécessaires par VLAN.

Dans cet exemple, les VLAN 210 (natifs), 2601 et 2602 sont ajoutés à la configuration du point d'accès racine comme indiqué à l'étape 1 de [WGB with Multiple VLANs Associated to a CAPWAP AP AP - WGB Configuration](#).

Étape 2. Créez l'identifiant SSID (Service Set Identifier).


Dans cet exemple, le SSID utilise WPA2/PSK, si vous avez besoin que le WGB s'associe à un SSID avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter le lien suivant :

[Exemple de configuration de ponts de groupe de travail avec authentification PEAP](#)

```
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
```

Étape 3. Ajoutez le SSID à l'interface utilisée pour l'association au point d'accès CAPWAP.

Cette étape définit également le point d'accès comme pont de groupe de travail avec la commande station-role workgroup-bridge.

 Remarque : dans cet exemple, le WGB utilise son interface 2,4 GHz pour s'associer au point d'accès CAPWAP, si vous avez besoin que le WGB s'associe à son interface 5 GHz, ajoutez cette configuration à l'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
```

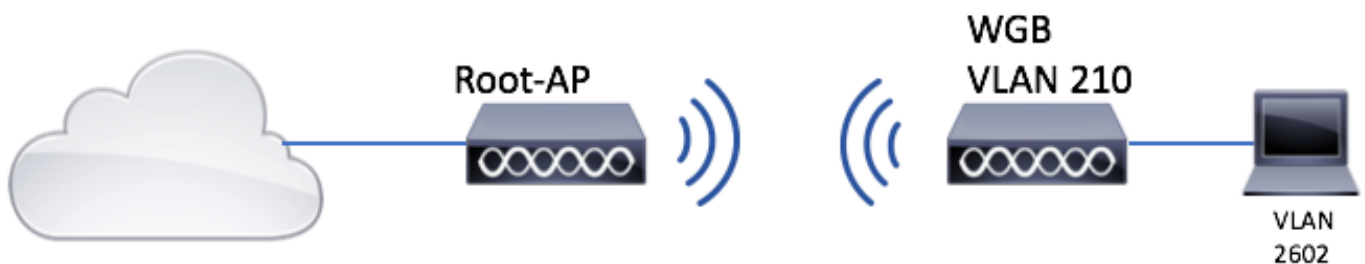
### Configuration du commutateur

Vous pouvez suivre la même configuration pour le commutateur sur [WGB avec plusieurs VLAN associés à un AP CAPWAP](#).

WGB sans commutateur derrière et plusieurs VLAN associés à un AP autonome en mode racine.

Cet exemple permet à WGB d'utiliser 2 VLAN différents (natif et un autre), si vous devez avoir plus de deux VLAN, alors vous devrez ajouter un commutateur 802.1q capable derrière le WGB et connecter les clients dessus. Suivez ensuite les instructions sur [WGB with 802.1q Switch behind and Multiple VLANs Associated to an Autonomous AP in Root Mode](#).

### Diagramme du réseau



### Configuration du point d'accès racine

Étape 1. Ajoutez les sous-interfaces nécessaires par VLAN.

La configuration des sous-interfaces est la même que celle de l'étape 1 de [WGB avec plusieurs VLAN associés à un AP CAPWAP - Configuration WGB](#), mais dans ce cas, vous devez seulement configurer VLAN 210 (natif) et VLAN 2602 (VLAN client).

Étape 2. Créez l'identifiant SSID (Service Set Identifier).


Dans cet exemple, le SSID utilise WPA2/PSK, si vous devez configurer le point d'accès racine avec un SSID avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter le lien suivant :

[Configurer les SSID et les VLAN sur les points d'accès autonomes](#)

```
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
```

Étape 3. Ajoutez le SSID à l'interface que le point d'accès racine utilisera pour diffuser le SSID.

---

 Remarque : dans cet exemple, le point d'accès racine utilise son interface 2,4 GHz pour diffuser le SSID, si vous avez besoin du point d'accès racine pour le diffuser avec son interface 5 GHz, ajoutez cette configuration à l'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
```

La commande infrastructure-client permet au point d'accès racine de respecter l'attribution de VLAN que WGB a pour ses clients filaires. Sans cette commande, l'AP racine attribue tous les clients au VLAN natif.

configuration WGB

Étape 1. Ajoutez les sous-interfaces nécessaires par VLAN. Dans cet exemple, les VLAN 210 (natifs) et 2601 sont ajoutés à la configuration WGB.

La configuration des sous-interfaces est identique à celle de l'étape 1 de [WGB avec plusieurs VLAN associés à un point d'accès CAPWAP - Configuration WGB](#), mais dans ce cas, il vous suffit de configurer le VLAN 210 (natif) et le VLAN 2602 (VLAN client).

Étape 2. Créez l'identifiant SSID (Service Set Identifier).

Dans cet exemple, le SSID utilise WPA2/PSK, si vous avez besoin que le WGB s'associe à un SSID avec une méthode de sécurité plus forte comme WPA2/802.1x, vous pouvez consulter le

lien suivant :


[Exemple de configuration de ponts de groupe de travail avec authentification PEAP](#)

```
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
```

Étape 3. Ajoutez le SSID à l'interface utilisée pour l'association au point d'accès CAPWAP.

Cette étape définit également le point d'accès comme pont de groupe de travail avec la commande `station-role workgroup-bridge`.

---

 Remarque : dans cet exemple, le WGB utilise son interface 2,4 GHz pour s'associer au point d'accès CAPWAP, si vous avez besoin que le WGB s'associe à son interface 5 GHz, ajoutez cette configuration à l'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
```

Étape 4. Spécifiez le VLAN client.

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

## Vérifier

Exécutez cette commande pour vérifier que WGB est associé au point d'accès racine et que ce dernier peut voir les clients filaires connectés derrière le 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	se1

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.