

Configurez le support du multiple VLAN de la passerelle de groupe de travail (WGB)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[WGB avec le multiple VLAN associé à un CAPWAP AP](#)

[Diagramme du réseau](#)

[Configuration WLC](#)

[Configuration WGB](#)

[Commutez la configuration](#)

[WGB avec le commutateur de 802.1Q derrière et le multiple VLAN associé à AP autonome dans le mode racine.](#)

[Diagramme du réseau](#)

[Configuration d'AP racine](#)

[Configuration WGB](#)

[Commutez la configuration](#)

[WGB sans le commutateur derrière et le multiple VLAN associé à AP autonome dans le mode racine.](#)

[Diagramme du réseau](#)

[Configuration d'AP racine](#)

[Configuration WGB](#)

[Vérifier](#)

Introduction

Explanis de ce document comment configurer un WGB pour prendre en charge les plusieurs réseaux locaux virtuels (VLAN) sous différents scénarios.

Conditions préalables

Exigences

Cisco recommande que vous ayez la connaissance de base au contrôleur LAN Sans fil d'AireOS (WLC) et au Point d'accès (AP) en configuration de mode autonome.

[Composants utilisés](#)

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

- Contrôle et ravitaillement des points d'accès sans fil (CAPWAP) AP
- Commutez le 802.1Q capable

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurer

WGB avec le multiple VLAN associé à un CAPWAP AP

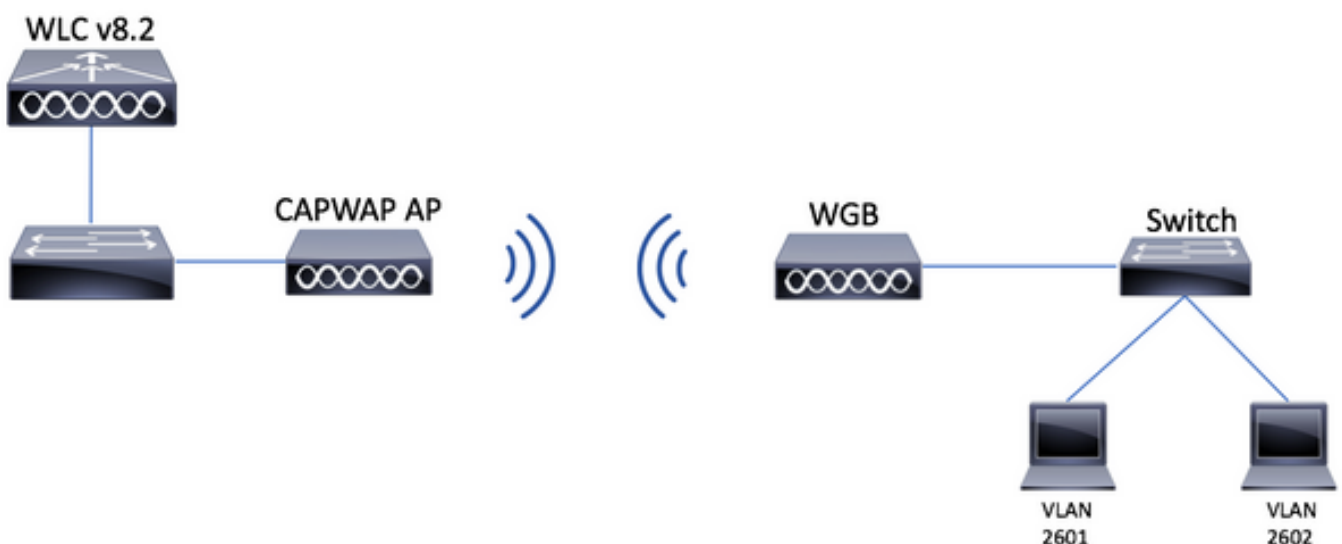
Cet exemple explique comment configurer un WGB prenant en charge des VLAN multiples, associés à un CAPWAP AP. Le Point d'accès peut être en mode local ou mode de passerelle (maille). Ce scénario exige que le WGB est connecté à un commutateur qui prennent en charge le 802.1Q, autrement WGB ne peut pas prendre en charge des VLAN multiples. Dans cet exemple le WGB est connecté à un commutateur 3560 de Cisco.

Si le commutateur ne prend en charge pas le 802.1Q, tous les clients seront assignés au VLAN indigène.

Dans cet exemple WGB est assigné à VLAN 210 et les clients connectés au commutateur derrière le WGB sont assignés à VLAN 2601 et 2602.

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

Diagramme du réseau



Configuration WLC

Étape 1. Ouvrez l'interface utilisateur graphique du WLC (GUI) et naviguez vers le **Controller > Interfaces** pour vérifier les interfaces dynamiques en cours configurées sur le WLC. If que les VLAN nécessaires ne sont pas déjà configurés, cliquez sur **New** et **ajoutez les nécessaires**.

CISCO MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration | Ping | Logout | Refresh Home

Controller Interfaces Entries 1 - 3 of 3 **New...**

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		Dynamic	Disabled	

CISCO MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration | Ping | Logout | Refresh Home

Controller Interfaces > New < Back **Apply**

Interface Name

VLAN Id

Écrivez les informations de l'interface

Interfaces > Edit < Back **Apply**

General Information

Interface Name

MAC Address

Configuration

Guest Lan

Quarantine

Quarantine Vlan Id

NAS-ID

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

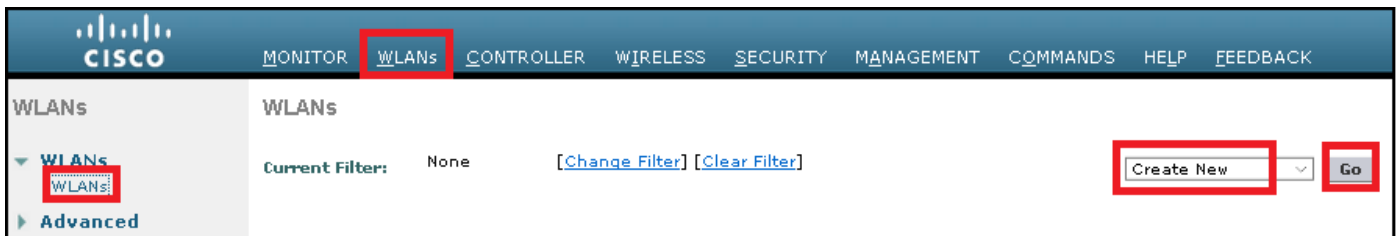
DHCP Information

Primary DHCP Server

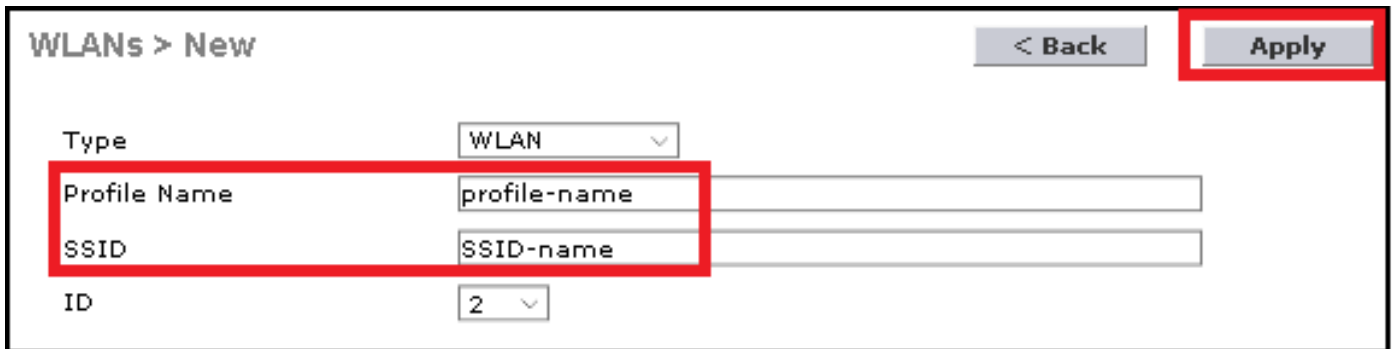
Secondary DHCP Server

Note: Si votre WLC a l'agrégation de liaisons (LAG) activée, vous ne pouvez pas sélectionner un numéro de port.

Étape 2. Naviguez vers des WLAN > créent nouveau > vont.



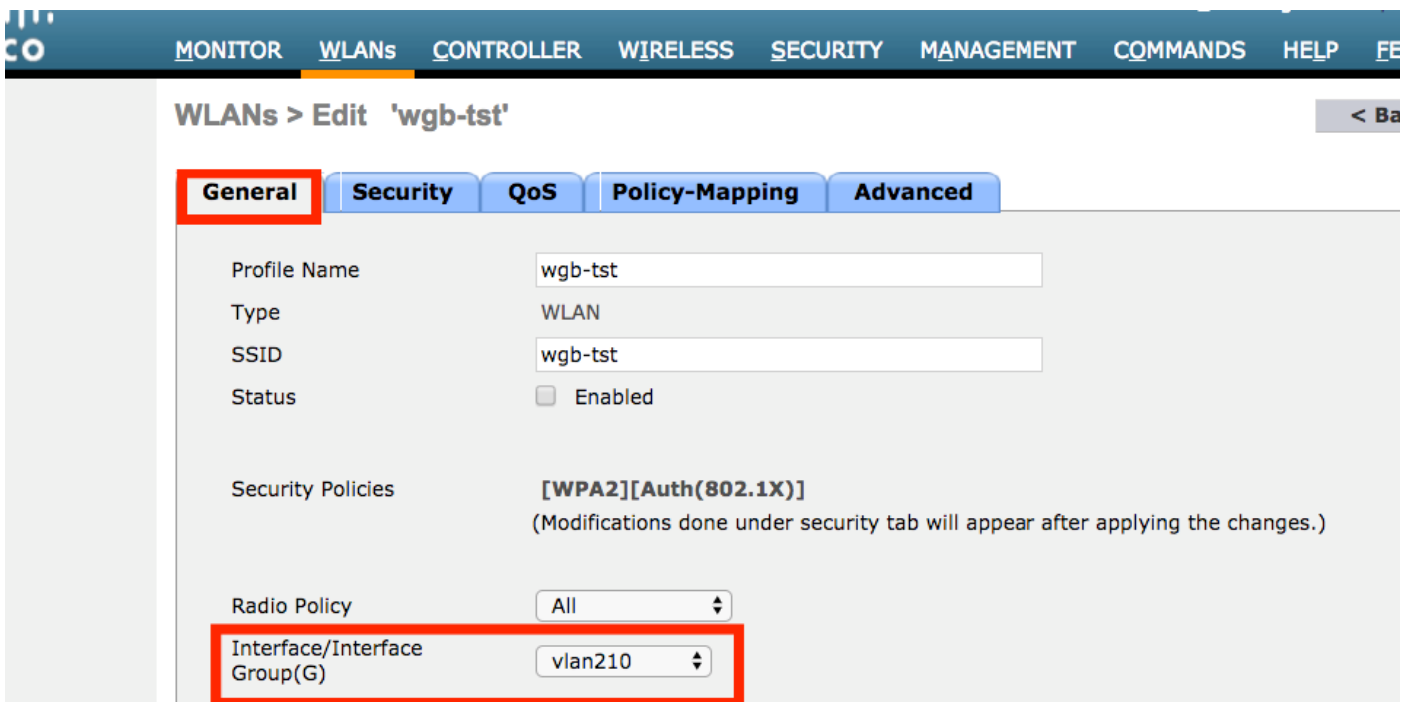
Étape 3. Choisissez un nom pour le SSID et le profil, puis cliquez sur Apply.



CLI :

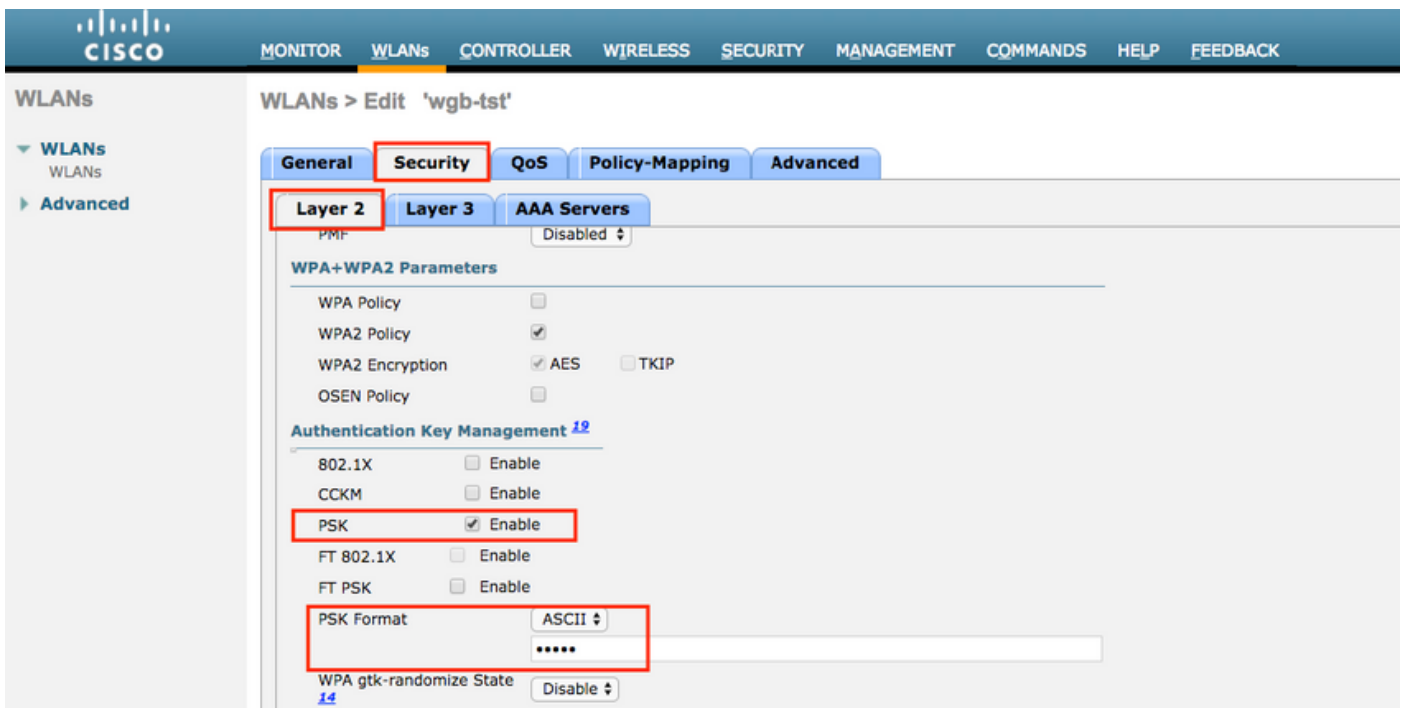
```
> config wlan create <id> <profile-name> <ssid-name>
```

Étape 4. Assignez le VLAN indigène du WGB au WLAN

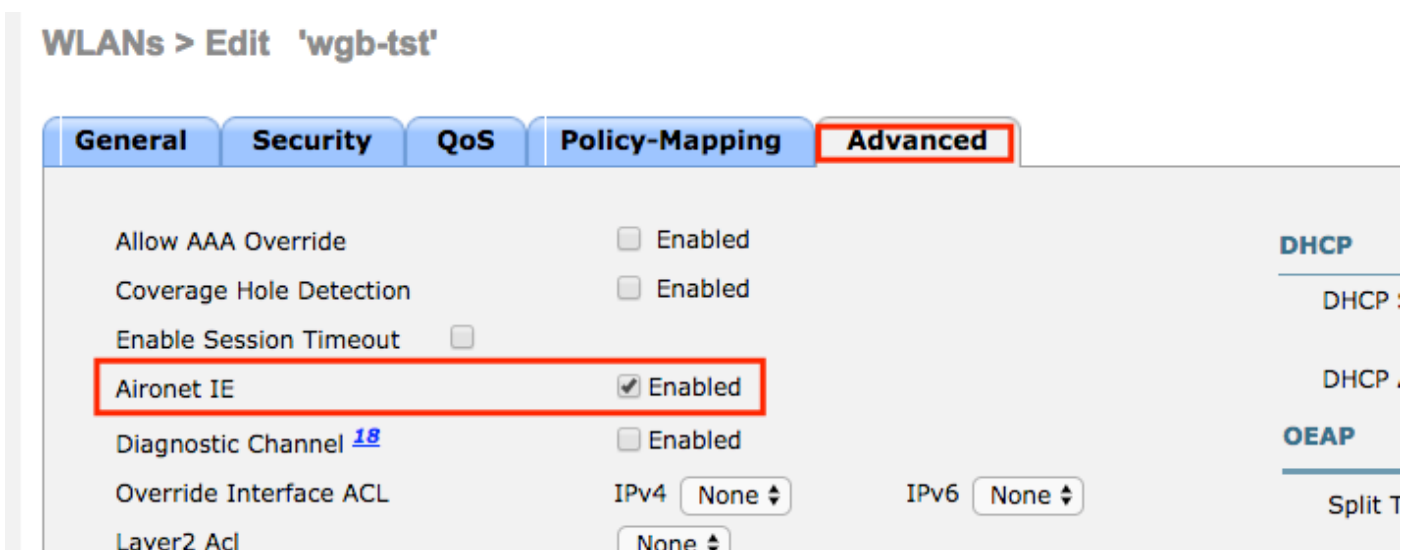


Étape 5. Assignez la clé pré partagée que WGB l'utilise pour associer au SSID.

Naviguez vers la **Sécurité** > la couche 2 > gestion des clés d'authentification. PSK choisit et remplissent mot de passe.



Étape 6. Assurez-vous que le WLAN a l'enable IE d'Aironet, autrement WGB ne pourra pas s'associer.



Note: Dans cet exemple le SSID utilise la Sécurité WPA2/PSK, si vous devez configurer le WLAN avec une méthode de sécurité accrue comme WPA2/802.1x que vous pouvez consulter le ce lien : [authentification de 802.1x avec le PEAP, l'ISE 2.1 et le WLC 8.3](#)

Étape 7. Permettez au WLC de prendre en charge des VLAN multiples d'un WGB

```
>config wgb vlan enable
```

Configuration WGB

Étape 1. Ajoutez les sous-interfaces requises par VLAN. Dans cet exemple VLAN 210 (indigène), 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
```

Note: Le groupe de passerelle de sous-interfaces 2601 et 2602 sont 21 et 22 parce que la plage valide pour des groupes de passerelle est de 1 à 255.

Note: Le groupe de passerelle pour la sous-interface 210 n'est pas spécifié parce que quand le VLAN indigène est assigné à une sous-interface, elle assigne automatiquement le groupe 1. de passerelle.

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

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

[Ponts de groupe de travail avec l'exemple de configuration d'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 dans l'interface utilisée pour s'associer au CAPWAP AP.

Cette étape a également placé AP en tant que passerelle de groupe de travail avec la **station-
role de pont de groupe de travail de** commande.

Note: Dans cet exemple le WGB emploie son interface 2.4GHz pour s'associer au CAPWAP AP, si vous avez besoin du WGB pour s'associer avec son interface 5GHz 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 caractéristique VLAN unifiée par WGB.

Cette commande permettra au WGB pour informer le WLC dans quel VLAN les clients devraient être assigné.

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

Commutez la configuration

Étape 1. Créez les VLAN.

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

Étape 2. Configurez le port où le WGB plugged dedans.

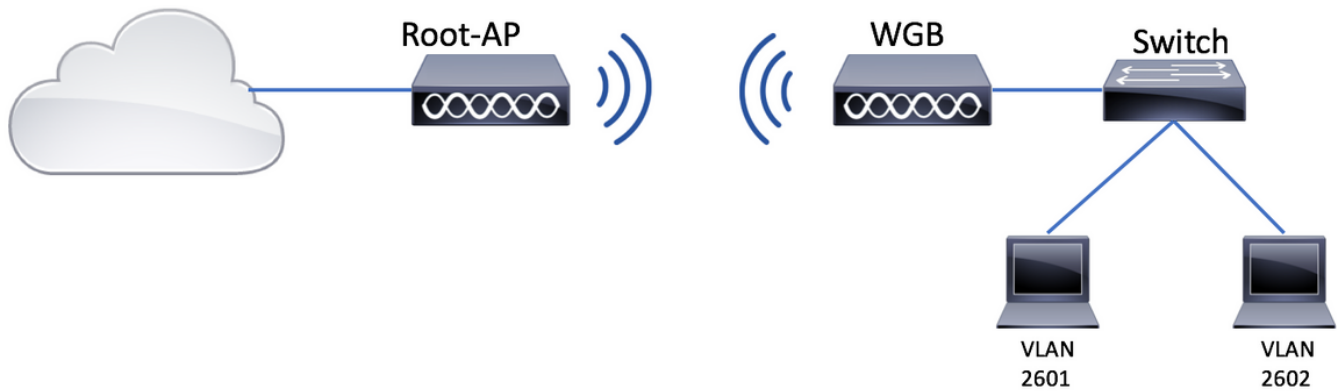
```
SW# config t
SW# interface <interface-id>
SW# switchport mode trunk
SW# switchport trunk native vlan 210
SW# switchport trunk allowed vlan 210, 2601, 2602
```

Étape 3. Assignez les interfaces où les clients plugged dedans au VLAN nécessaire.

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

WGB avec le commutateur de 802.1Q derrière et le multiple VLAN associé à AP autonome dans le mode racine.

[Diagramme du réseau](#)



Configuration d'AP racine

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

Dans cet exemple VLAN 210 (indigène), 2601 et 2602 sont ajoutés à la configuration d'AP racine comme indiqué dans l'étape 1 de [WGB avec le multiple VLAN associé à un CAPWAP AP - configuration WGB](#).

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

Dans cet exemple le SSID utilise WPA2/PSK, si vous devez configurer l'AP racine avec un SSID avec une méthode de sécurité accrue comme WPA2/802.1x que vous pouvez consulter le ce lien :

[Configurez le SSID et les VLAN sur des aps 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 l'AP racine l'utilisera pour annoncer le SSID.

Note: Dans cet exemple l'AP racine emploie son interface 2.4GHz pour annoncer le SSID, si vous avez besoin de l'AP racine pour l'annoncer avec son interface 5GHz 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
```


L'infrastructure-client de commande permet à l'AP racine pour respecter l'affectation VLAN que WGB ont pour ses clients câblés. Sans cette commande, l'AP racine affectera tous les clients au VLAN indigène.

Configuration WGB

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

Dans cet exemple VLAN 210 (indigène), 2601 et 2602 sont ajoutés à la configuration d'AP racine comme indiqué dans l'étape 1 de [WGB avec le multiple VLAN associé à un CAPWAP AP - configuration WGB](#).

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

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

[Ponts de groupe de travail avec l'exemple de configuration d'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 dans l'interface utilisée pour s'associer au CAPWAP AP.

Cette étape a également placé AP en tant que passerelle de groupe de travail avec la **station-role de pont de groupe de travail de** commande.

Note: Dans cet exemple le WGB emploie son interface 2.4GHz pour s'associer au CAPWAP AP, si vous avez besoin du WGB pour s'associer avec son interface 5GHz 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
```

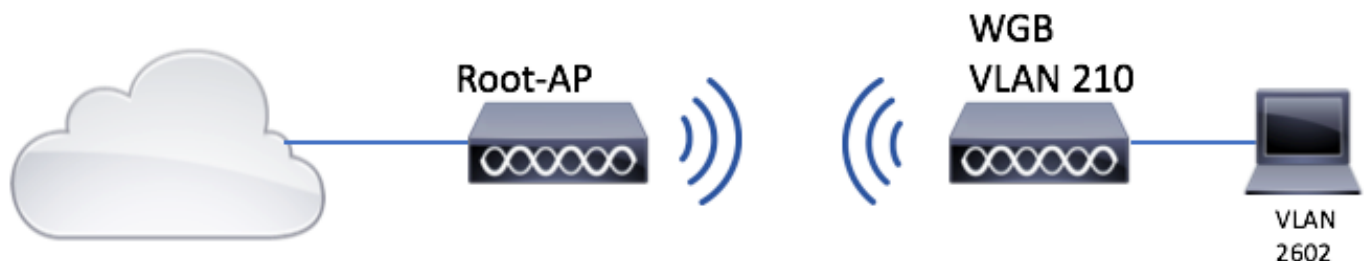
Commutez la configuration

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

WGB sans le commutateur derrière et le multiple VLAN associé à AP autonome dans le mode racine.

Cet exemple permet à WGB pour utiliser 2 VLAN différents (indigènes et un autre), si vous devez avoir plus de deux VLAN alors vous devrez ajouter un commutateur de 802.1Q capable derrière le WGB et connecter les clients là-dessus. Suivez alors les instructions sur [WGB avec le commutateur de 802.1Q derrière et le multiple VLAN associé à AP autonome dans le mode racine](#).

Diagramme du réseau



Configuration d'AP racine

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

La configuration de sous-interfaces est identique que vue sur l'étape 1 de [WGB avec le multiple VLAN associé à un CAPWAP AP - configuration WGB](#), mais dans ce cas vous devez seulement configurer VLAN 210 (indigène) et VLAN 2602 (client VLAN).

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

Dans cet exemple le SSID utilise WPA2/PSK, si vous devez configurer l'AP racine avec un SSID avec une méthode de sécurité accrue comme WPA2/802.1x que vous pouvez consulter le ce lien :

Configurez le SSID et les VLAN sur des aps 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 l'AP racine l'utilisera pour annoncer le SSID.

Note: Dans cet exemple l'AP racine emploie son interface 2.4GHz pour annoncer le SSID, si vous avez besoin de l'AP racine pour l'annoncer avec son interface 5GHz 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
```

L'infrastructure-client de commande permet à l'AP racine pour respecter l'affectation VLAN que WGB ont pour ses clients câblés. Sans cette commande, l'AP racine affecte tous les clients au VLAN indigène.

Configuration WGB

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

La configuration de sous-interfaces est identique que vue sur l'étape 1 de [WGB avec le multiple VLAN associé à un CAPWAP AP - configuration WGB](#), mais dans ce cas vous devrez seulement configurer VLAN 210 (indigène) et VLAN 2602 (client VLAN).

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

Dans cet exemple le SSID utilise WPA2/PSK, si vous avez besoin du WGB pour s'associer à un SSID avec une méthode de sécurité accrue comme WPA2/802.1x que vous pouvez consulter le [ce lien](#) :

[Ponts de groupe de travail avec l'exemple de configuration d'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 dans l'interface utilisée pour s'associer au CAPWAP AP.

Cette étape a également placé AP en tant que passerelle de groupe de travail avec la **station-role de pont de groupe de travail de commande**.

Note: Dans cet exemple le WGB emploie son interface 2.4GHz pour s'associer au CAPWAP AP, si vous avez besoin du WGB pour s'associer avec son interface 5GHz 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 client VLAN.

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

Vérifiez

Exécutez cette commande de vérifier WGB est associé à l'AP racine, et cela AP racine peut voir les clients câblés connectés derrière le WGB :

```
WGB# show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [WGB-tst] :
```

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

```
Root-AP# show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [WGB-tst] :
```

MAC Address	IP address	IPV6 address	Device	Name
Parent	State			
0035.1ac1.78c7	206.206.206.2	::	WGB-client	-
00f6.6316.4258	Assoc			
00f6.6316.4258	200.200.200.3	::	WGB	WGB
self	Assoc			