

Ondersteuning van meerdere VLAN's configureren voor werkgroepbridge (WGB)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[WGB met meerdere VLAN's die aan een CAPWAP zijn gekoppeld](#)

[Netwerkdigram](#)

[WLC-configuratie](#)

[WGB-configuratie](#)

[Switchconfiguratie](#)

[WGB met 802.1q Switch erachter en meerdere VLAN's gekoppeld aan een Autonomous AP in Root Mode.](#)

[Netwerkdigram](#)

[Configuratie van basismap](#)

[WGB-configuratie](#)

[Switchconfiguratie](#)

[WGB zonder Switch erachter en meervoudige VLAN's die zijn gekoppeld aan een autonoom AP in Root Mode.](#)

[Netwerkdigram](#)

[Configuratie van basismap](#)

[WGB-configuratie](#)

[Verifiëren](#)

Inleiding

Dit document legt uit hoe u een WGB kunt configureren om meerdere Virtual Local Area Networks (VLAN's) onder verschillende scenario's te ondersteunen.

Voorwaarden

Vereisten

Cisco raadt u aan om over basiskennis te beschikken op het gebied van AireOS Wireless LAN Controller (WLC) en access point (AP) in autonome modemconfiguratie.

Gebruikte componenten

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

- Beheer en provisioning van Wireless Access points (CAPWAP) access point
- Geschikt voor switch 802.1q

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

WGB met meerdere VLAN's die aan een CAPWAP zijn gekoppeld

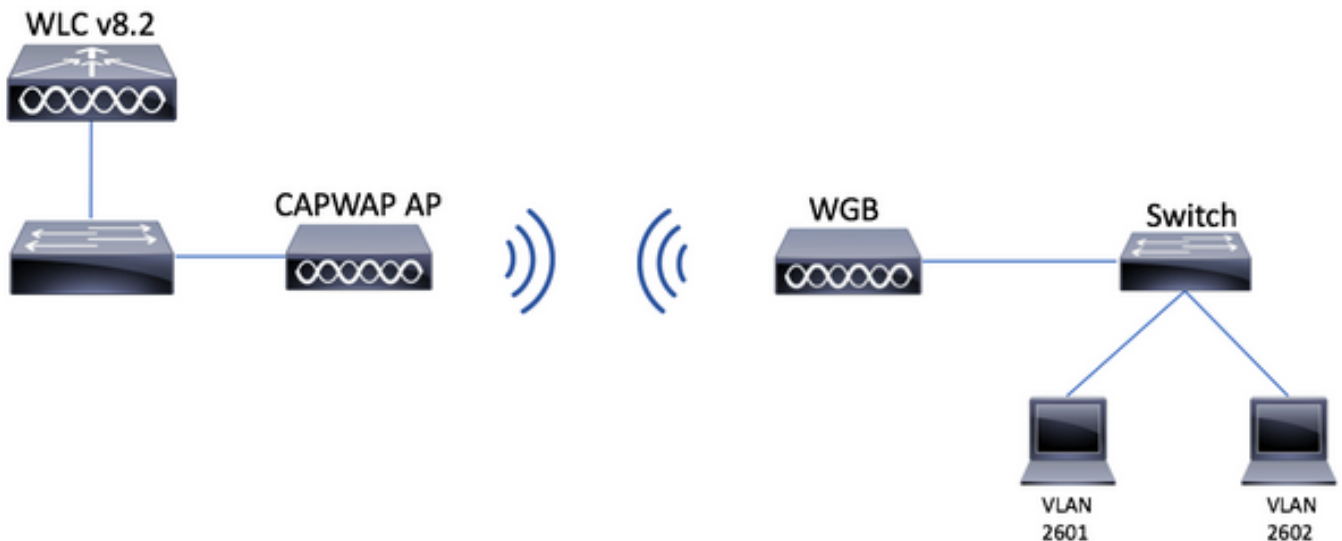
Dit voorbeeld legt uit hoe u een WGB kunt configureren die meerdere VLAN's ondersteunt, gekoppeld aan een CAPWAP. Het access point kan in de Local Mode of Bridge Mode (Mesh) worden weergegeven. Voor dit scenario moet de WGB zijn verbonden met een switch die 802.1q ondersteunt, anders kan WGB geen meerdere VLAN's ondersteunen. In dit voorbeeld is de WGB aangesloten op een Cisco-Switch 3560.

Als de switch 802.1q niet ondersteunt, worden alle clients toegewezen aan het native VLAN.

In dit voorbeeld wordt WGB toegewezen aan VLAN 210 en de clients die zijn aangesloten op de switch achter de WGB worden toegewezen aan VLAN 2601 en 2602.

De WLC moet ook dynamische interfaces geconfigureerd hebben die tot het VLAN van de client behoren. In dit voorbeeld moet WLC dynamische interfaces hebben op VLAN 2601, 2602 en 210.

Netwerkdigram



WLC-configuratie

Stap 1. Open de grafische gebruikersinterface (GUI) van WLC en navigeer naar **CONTROLLER > Interfaces** om de huidige dynamische interfaces op de WLC te verifiëren. Als de benodigde VLAN's nog niet zijn geconfigureerd, klik dan op **Nieuw** en voeg de benodigde interfaces toe.

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 | |
| v... | 2... | ... | 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 | <input type="text" value="vlan210"/> |
| VLAN Id | <input type="text" value="210"/> |

Voer de informatie over de interface in

Interfaces > Edit **< Back** **Apply**

General Information

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

Configuration

Guest Lan:
 Quarantine:
 Quarantine Vlan Id:
 NAS-ID:

Physical Information

Port Number:
 Backup Port:
 Active Port: 0
 Enable Dynamic AP Management:

Interface Address

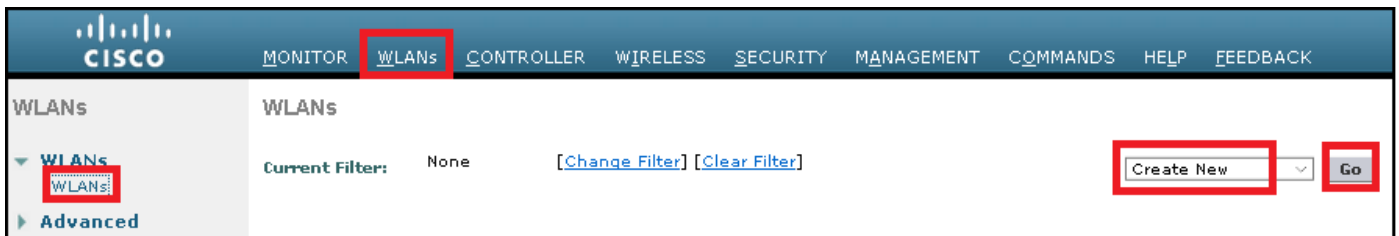
VLAN Identifier:
 IP Address:
 Netmask:
 Gateway:

DHCP Information

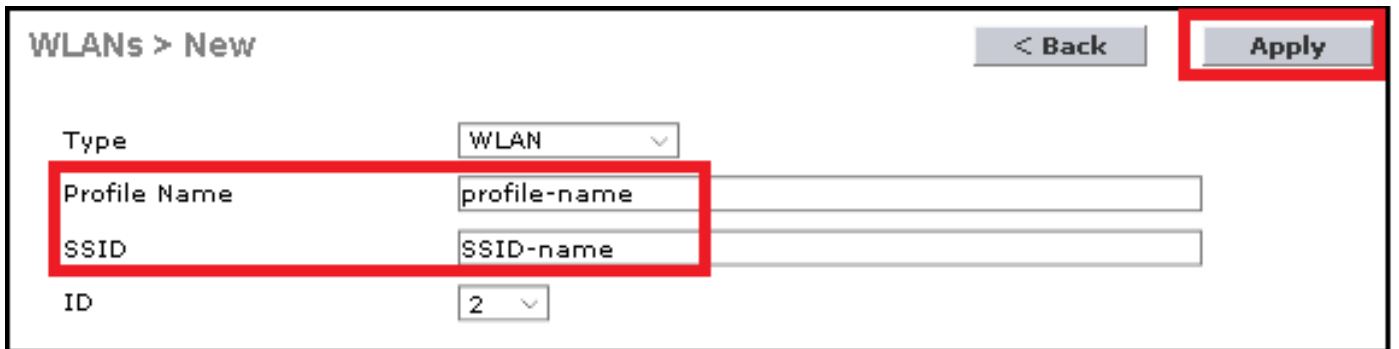
Primary DHCP Server:
 Secondary DHCP Server:

Opmerking: als uw WLC Link Aggregation (LAG) ingeschakeld heeft, kunt u geen poortnummer selecteren.

Stap 2. Navigeer naar WLAN's > Nieuw maken > Ga.



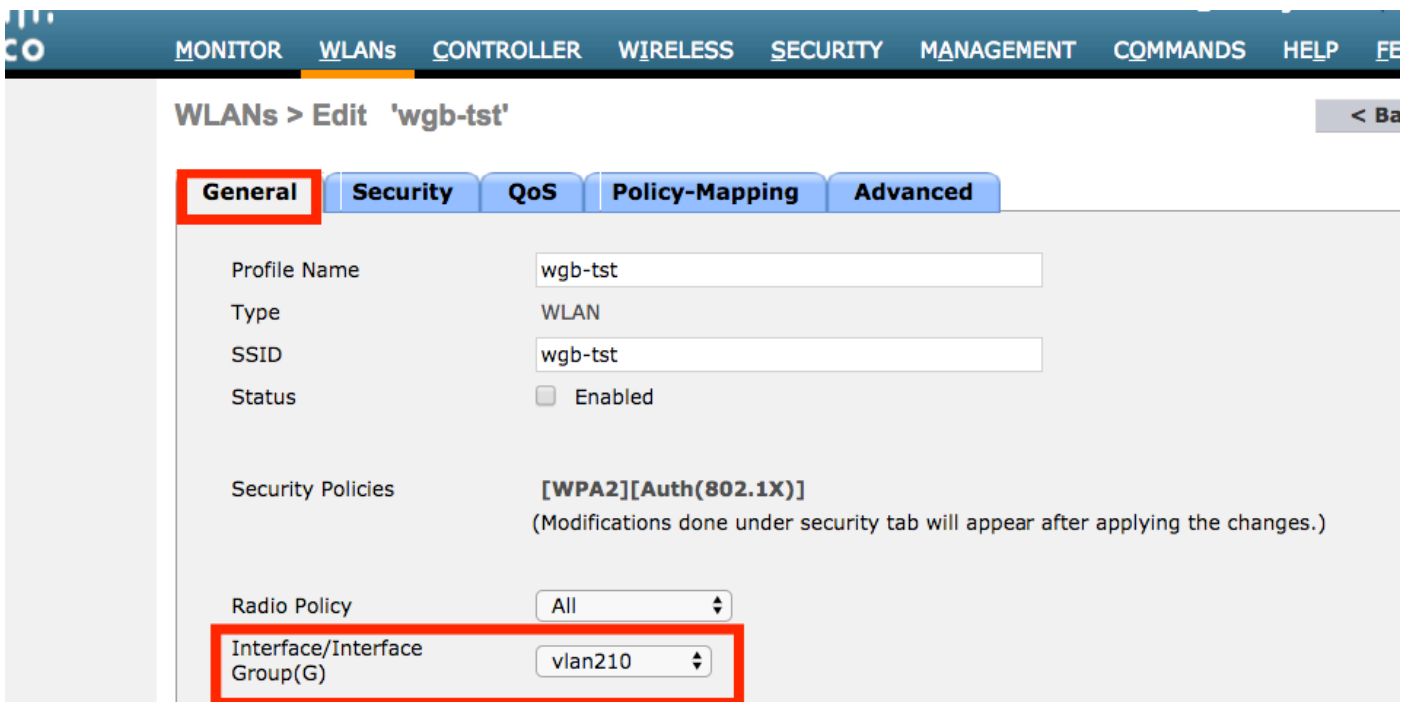
Stap 3. Kies een naam voor de SSID en het profiel en klik vervolgens op **Toepassen**.



CLI:

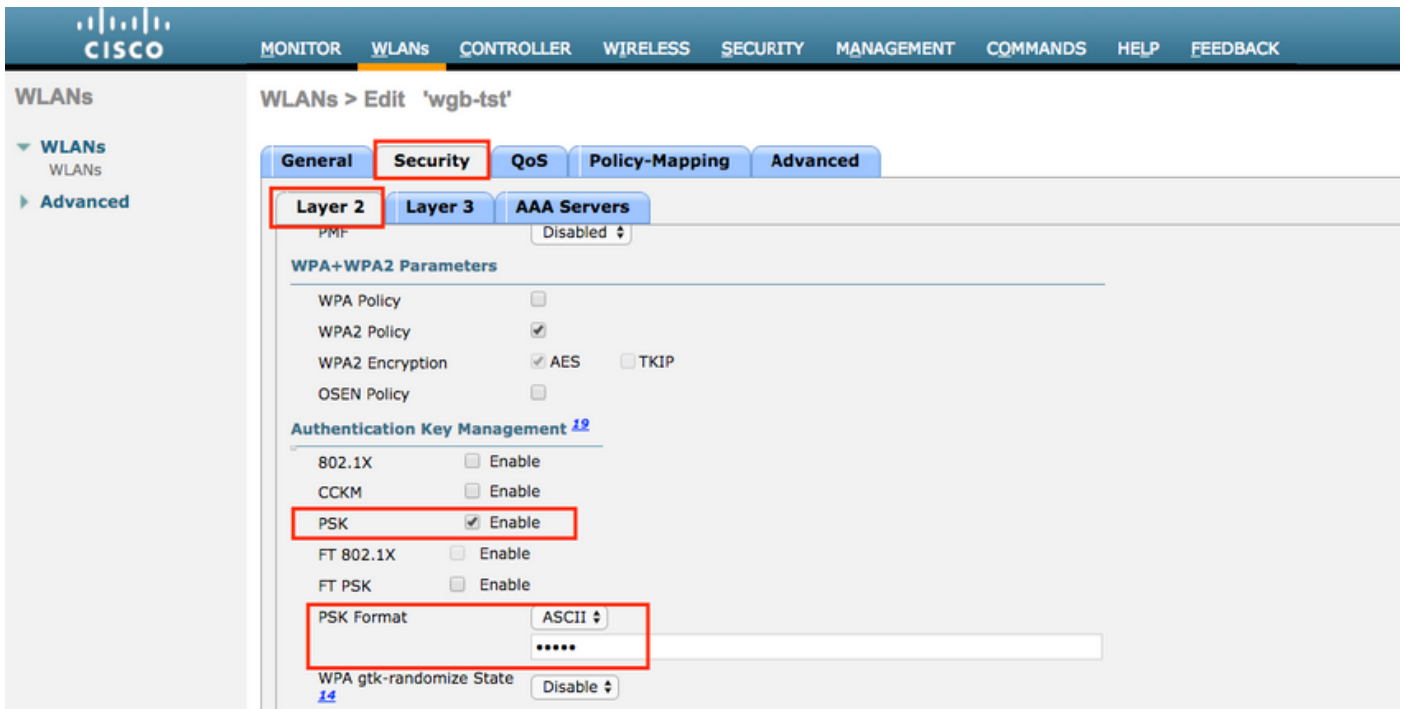
```
> config wlan create <id> <profile-name> <ssid-name>
```

Stap 4. Wijs het WGB native VLAN toe aan het WLAN

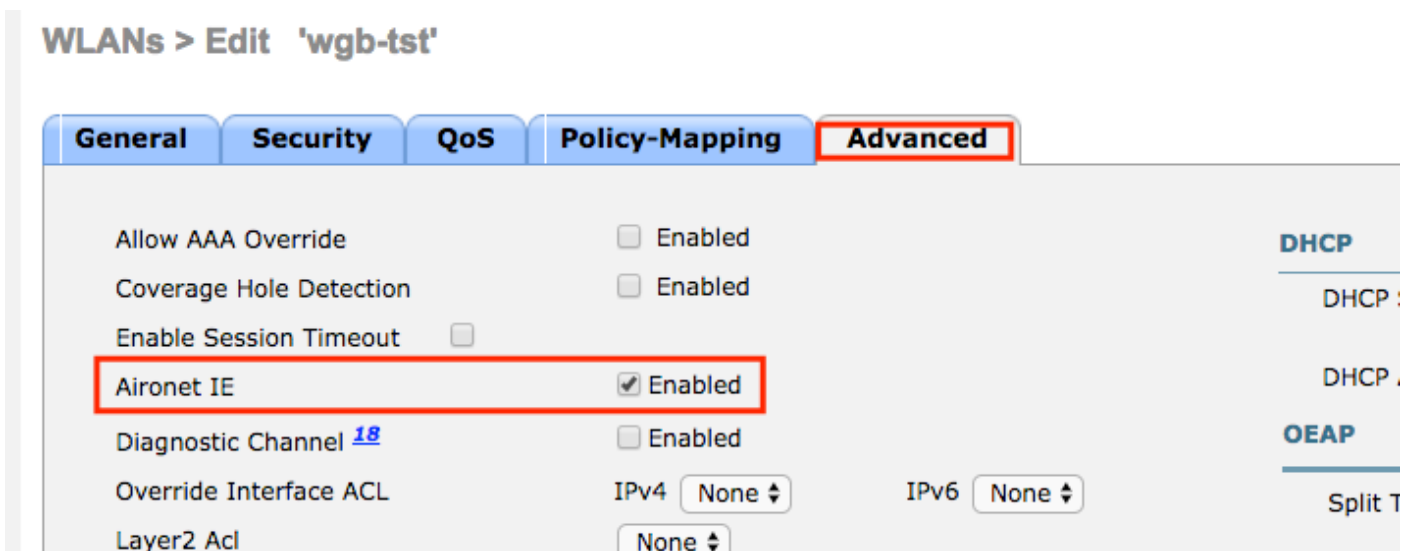


Stap 5. Wijs de Vooraf Gedeelde Sleutel toe die WGB gebruikt om aan SSID te associëren.

Navigeer naar **Security > Layer 2 > Verificatiesleutelbeheer**. Selecteer **PSK** en vul het wachtwoord in.



Stap 6. Zorg ervoor dat het WLAN **Aironet IE** heeft ingeschakeld, anders kan WGB geen verbinding maken.



Opmerking: in dit voorbeeld gebruikt de SSID WPA2/PSK-beveiliging, als u het WLAN moet configureren met een sterkere beveiligingsmethode zoals WPA2/802.1x, kunt u de volgende link raadplegen: [802.1x-verificatie met PEAP, ISE 2.1 en WLC 8.3](#)

Stap 7. Schakel de WLC in om meerdere VLAN's vanaf een WGB te ondersteunen

```
>config wgb vlan enable
```

WGB-configuratie

Stap 1. Voeg de benodigde subinterfaces per VLAN toe. In dit voorbeeld worden VLAN's 210 (Native), 2601 en 2602 toegevoegd aan de WGB-configuratie.

```
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
```

Opmerking: Bruggroep van subinterfaces 2601 en 2602 zijn 21 en 22 omdat het geldige bereik voor bruggroepen van 1 tot 255 is.

Opmerking: Bridge Group voor subinterface 210 is niet opgegeven omdat wanneer het native VLAN is toegewezen aan een subinterface, het automatisch bruggroep 1 toewijst.

Stap 2. Maak de Service Set Identifier (SSID) aan.

In dit voorbeeld gebruikt de SSID WPA2/PSK, als u de WGB nodig hebt om te koppelen aan een SSID met een sterkere beveiligingsmethode zoals WPA2/802.1x kunt u deze link raadplegen:

[Voorbeeld van configuratie van werkgroepbruggen met PEAP-verificatie](#)

```
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
```

Stap 3. Voeg de SSID toe aan de interface die wordt gebruikt voor de koppeling aan het CAPWAP-toegangspunt.

In deze stap wordt de AP ook ingesteld als werkgroepbridge met de **werkgroepbridge van het opdrachtstation**.

Opmerking: in dit voorbeeld gebruikt de WGB zijn 2.4GHz interface om te koppelen aan de CAPWAP AP, als je de WGB nodig hebt om te associëren met zijn 5GHz interface voeg deze configuratie toe aan de 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
```

Stap 4. Schakel de functie WGB Unified VLAN in.

Met deze opdracht kan de WGB de WLC inlichten waarin VLAN aan de clients moet worden toegewezen.

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

Switchconfiguratie

Stap 1. Maak de VLAN's.

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

Stap 2. Configureer de poort waar de WGB is ingestopt.

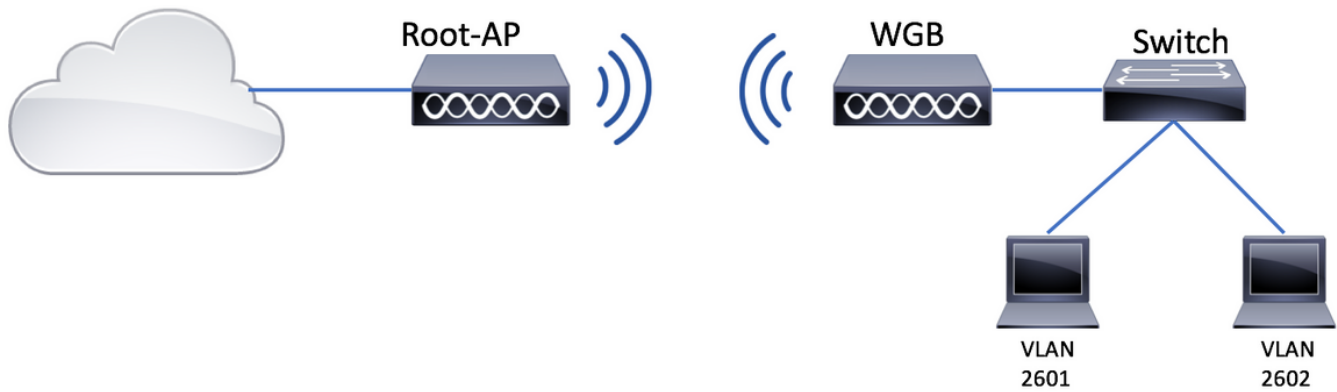
```
SW# config t
SW# interface <interface-id>
SW# switchport mode trunk
SW# switchport trunk native vlan 210
SW# switchport trunk allowed vlan 210, 2601, 2602
```

Stap 3. Wijs de interfaces toe waar de clients zijn aangesloten op het benodigde VLAN.

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

WGB met 802.1q Switch erachter en meerdere VLAN's gekoppeld aan een Autonomous AP in Root Mode.

Netwerkdigram



Configuratie van basismap

Stap 1. Voeg de benodigde subinterfaces per VLAN toe.

In dit voorbeeld worden VLAN's 210 (Native), 2601 en 2602 toegevoegd aan de Root AP-configuratie zoals geïnstrueerd in Stap 1 van [WGB met meerdere VLAN's die gekoppeld zijn aan een CAPWAP AP - WGB Configuration](#).

Stap 2. Maak de Service Set Identifier (SSID) aan.

In dit voorbeeld gebruikt de SSID WPA2/PSK, als u de Root AP met een SSID met een sterkere beveiligingsmethode zoals WPA2/802.1x moet configureren kunt u de volgende link raadplegen:

[SSID's en VLAN's configureren op autonome AP's](#)

```
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
```

Stap 3. Voeg de SSID toe aan de interface die Root AP zal gebruiken om de SSID uit te zenden.

Opmerking: in dit voorbeeld gebruikt de Root-AP zijn 2.4GHz interface om de SSID uit te zenden, als je de Root-AP nodig hebt om het uit te zenden met zijn 5GHz interface voeg deze configuratie toe aan de 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
```


Met de opdrachtinfrastructuurclient kan Root AP de VLAN-toewijzing respecteren die WGB heeft voor zijn bekabelde clients. Zonder dit bevel, zal AP van de Wortel alle cliënten aan inheems VLAN toewijzen.

WGB-configuratie

Stap 1. Voeg de benodigde subinterfaces per VLAN toe.

In dit voorbeeld worden VLAN's 210 (Native), 2601 en 2602 toegevoegd aan de Root AP-configuratie zoals geïnstrueerd in Stap 1 van [WGB met meerdere VLAN's die gekoppeld zijn aan een CAPWAP AP - WGB Configuration](#).

Stap 2. Maak de Service Set Identifier (SSID) aan.

In dit voorbeeld gebruikt de SSID WPA2/PSK, als u de WGB nodig hebt om te koppelen aan een SSID met een sterkere beveiligingsmethode zoals WPA2/802.1x kunt u de volgende link raadplegen:

[Voorbeeld van configuratie van werkgroepbruggen met PEAP-verificatie](#)

```
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
```

Stap 3. Voeg de SSID toe aan de interface die wordt gebruikt voor de koppeling aan het CAPWAP-toegangspunt.

In deze stap wordt de AP ook ingesteld als werkgroepbridge met de **werkgroepbridge van het opdrachtstation**.

Opmerking: in dit voorbeeld gebruikt de WGB zijn 2.4GHz interface om te koppelen aan de CAPWAP AP, als je de WGB nodig hebt om te associëren met zijn 5GHz interface voeg deze configuratie toe aan de 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
```

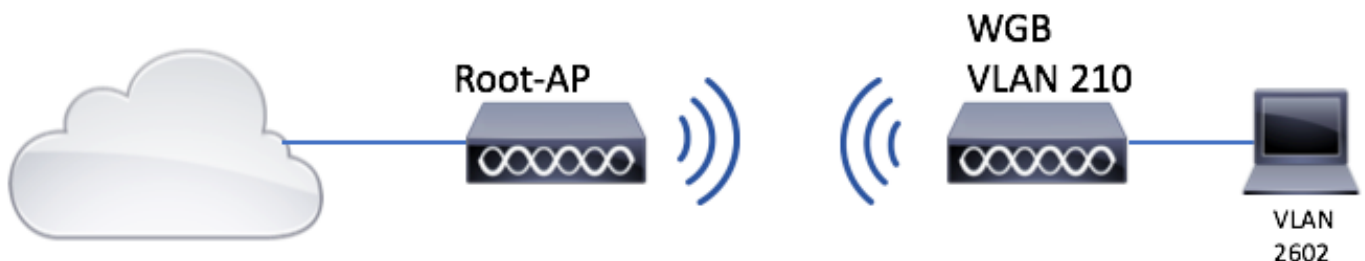
Switchconfiguratie

U kunt dezelfde configuratie voor switch op [WGB](#) volgen [met meerdere VLAN's die aan een CAPWAP zijn gekoppeld](#).

WGB zonder Switch erachter en meervoudige VLAN's die zijn gekoppeld aan een autonoom AP in Root Mode.

Dit voorbeeld staat WGB toe om 2 verschillende VLAN's (native en een andere) te gebruiken, als je meer dan twee VLAN's nodig hebt, dan zal je een 802.1q switch moeten toevoegen die geschikt is achter de WGB en de clients erop aan te sluiten. Volg vervolgens de aanwijzingen op [WGB met de 802.1q-Switch erachter en meerdere VLAN's die zijn gekoppeld aan een Autonoom AP in Root Mode](#).

Netwerkdigram



Configuratie van basismap

Stap 1. Voeg de benodigde subinterfaces per VLAN toe.

De configuratie van subinterfaces is hetzelfde als in stap 1 van [WGB met meerdere VLAN's die aan een CAPWAP AP - WGB Configuration zijn gekoppeld](#), maar in dit geval hoeft u alleen VLAN 210 (native) en VLAN 2602 (client VLAN) te configureren.

Stap 2. Maak de Service Set Identifier (SSID) aan.

In dit voorbeeld gebruikt de SSID WPA2/PSK, als u de Root AP met een SSID met een sterkere beveiligingsmethode zoals WPA2/802.1x moet configureren kunt u de volgende link raadplegen:

[SSID's en VLAN's configureren op autonome AP's](#)

```
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
```

Stap 3. Voeg de SSID toe aan de interface die Root AP zal gebruiken om de SSID uit te zenden.

Opmerking: in dit voorbeeld gebruikt de Root-AP zijn 2.4GHz interface om de SSID uit te zenden, als je de Root-AP nodig hebt om het uit te zenden met zijn 5GHz interface voeg deze configuratie toe aan de 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
```

Het commando **infrastructuurclient** Hiermee kan Root AP de VLAN-toewijzing respecteren die WGB heeft voor de bekabelde clients. Zonder dit bevel, wijst AP van de Wortel alle cliënten aan inheems VLAN toe.

WGB-configuratie

Stap 1. Voeg de benodigde subinterfaces per VLAN toe. In dit voorbeeld worden VLAN's 210 (Native) en 2601 toegevoegd aan de WGB-configuratie.

De configuratie van subinterfaces is gelijk aan de configuratie op Stap 1 van [WGB met meerdere VLAN's gekoppeld aan een CAPWAP AP - WGB Configuration](#) Maar in dit geval hoeft u VLAN 210 (native) en VLAN 2602 (client-VLAN) alleen te configureren.

Stap 2. Maak de Service Set Identifier (SSID) aan.

In dit voorbeeld gebruikt de SSID WPA2/PSK, als u de WGB nodig hebt om te koppelen aan een SSID met een sterkere beveiligingsmethode zoals WPA2/802.1x kunt u de volgende link raadplegen:

[Voorbeeld van configuratie van werkgroepbruggen met PEAP-verificatie](#)

```
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
```

Stap 3. Voeg de SSID toe aan de interface die wordt gebruikt voor de koppeling aan het CAPWAP-toegangspunt.

In deze stap wordt de AP ook ingesteld als werkgroepbride met de **werkgroepbride van het opdrachtstation**.

Opmerking: in dit voorbeeld gebruikt de WGB zijn 2.4GHz interface om te koppelen aan de CAPWAP AP, als je de WGB nodig hebt om te associëren met zijn 5GHz interface voeg deze configuratie toe aan de 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
```

Stap 4. Specificeer de client-VLAN.

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

Verifiëren

Voer deze opdracht uit om te controleren of WGB is gekoppeld aan Root AP en dat Root AP de bekabelde clients kan zien die zijn aangesloten achter de 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 | | | |

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.