Configurazione del supporto di più VLAN con Work Group Bridge (WGB)

Sommario

Introduzione

In questo documento viene spiegato come configurare un WGB in modo che supporti più VLAN (Virtual Local Area Network) in scenari diversi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base di AireOS Wireless LAN Controller (WLC) e Access Point (AP) in configurazione in modalità autonoma.

Componenti usati

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

- Controllo e provisioning dei punti di accesso wireless (CAPWAP)
- Compatibilità con lo switch 802.1q

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

WGB con più VLAN associate a un CAPWAP AP

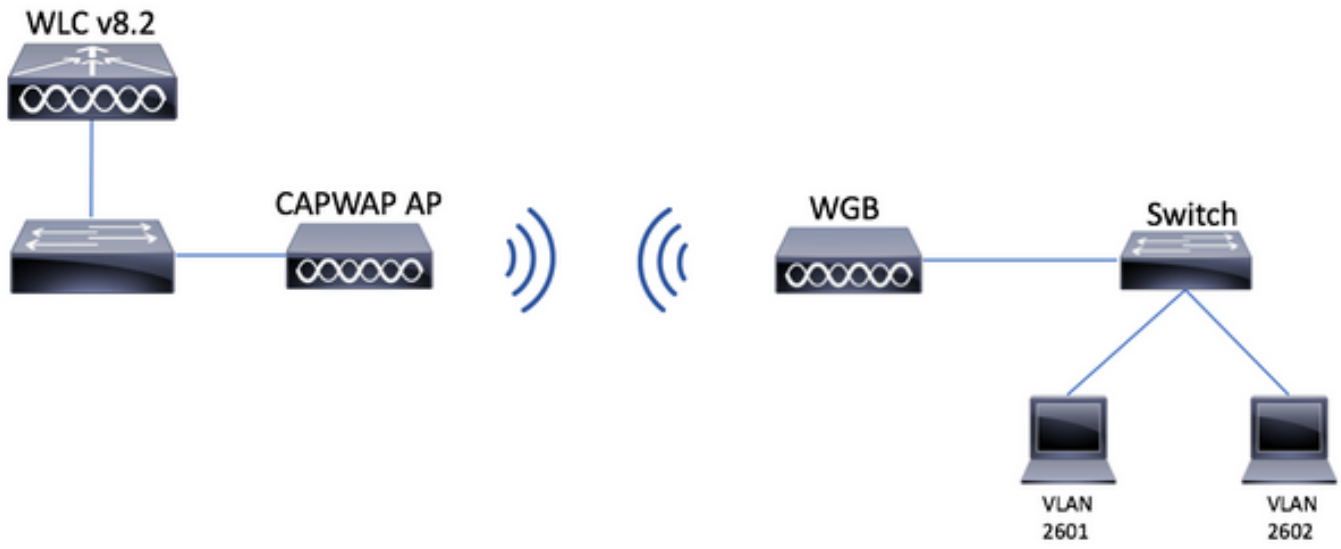
Nell'esempio viene spiegato come configurare un WGB che supporti più VLAN, associato a un CAPWAP. Il punto di accesso può essere in modalità locale o in modalità ponte (Mesh). Per questo scenario, è necessario che il WGB sia collegato a uno switch che supporta 802.1q. In caso contrario, il WGB non può supportare più VLAN. Nell'esempio, il WGB è collegato a uno switch Cisco 3560.

Se lo switch non supporta 802.1q, tutti i client verranno assegnati alla VLAN nativa.

In questo esempio, la porta WGB è assegnata alla VLAN 210 e i client collegati allo switch dietro la porta WGB sono assegnati alla VLAN 2601 e alla VLAN 2602.

Il WLC deve inoltre avere interfacce dinamiche configurate che appartengono alla vlan del client. Nell'esempio, il WLC deve avere interfacce dinamiche sulle VLAN 2601, 2602 e 2610.

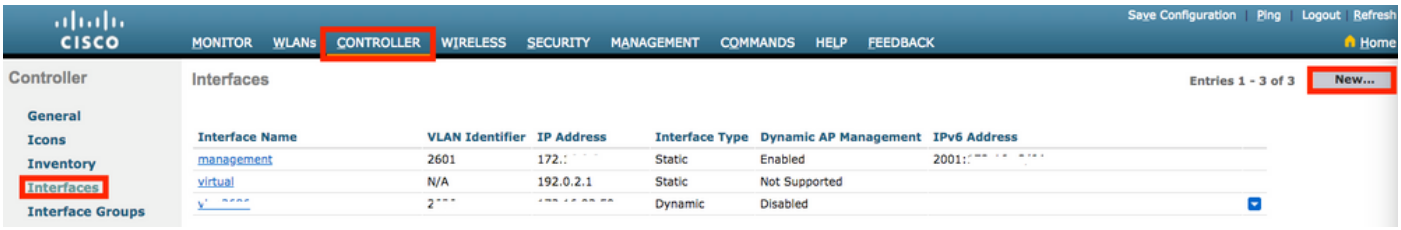
Esempio di rete

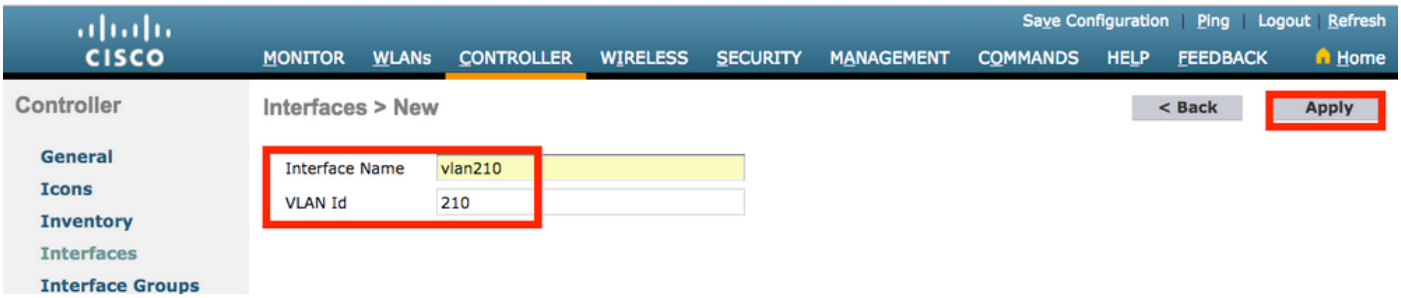


Configurazione WLC

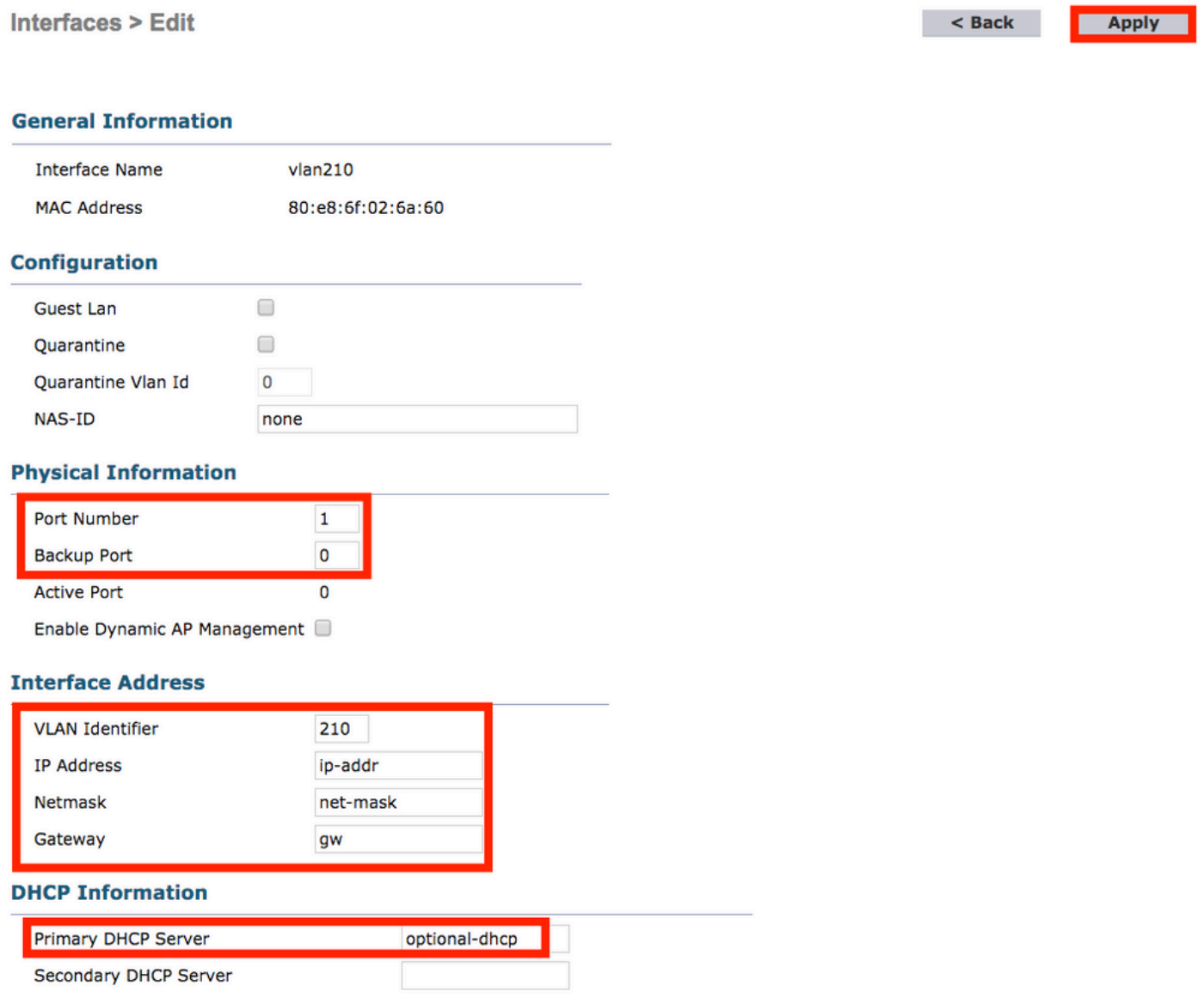
Passaggio 1. Aprire l'interfaccia grafica dell'utente (GUI) del WLC e selezionare CONTROLLER > Interfacce per verificare le interfacce dinamiche attualmente configurate sul WLC.Se le vlan

richieste non sono già state configurate, fare clic su New (Nuova) e aggiungere quelle necessarie.



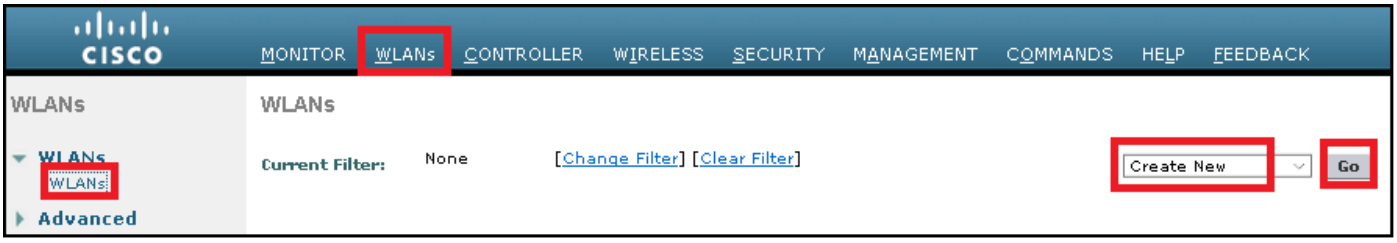


Immettere le informazioni sull'interfaccia

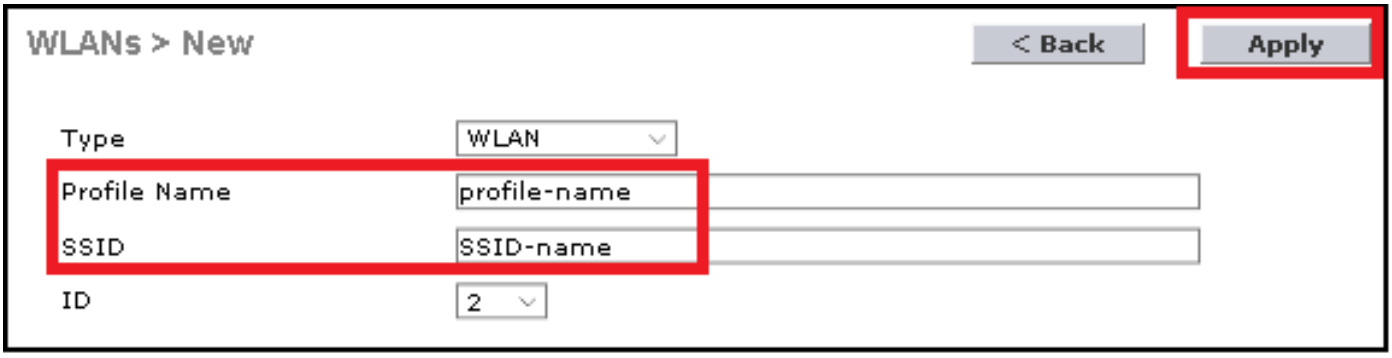


Nota: se il WLC ha il LAG (Link Aggregation) abilitato, non è possibile selezionare un numero di porta.

Passaggio 2. Selezionare WLAN > Crea nuovo > Vai.



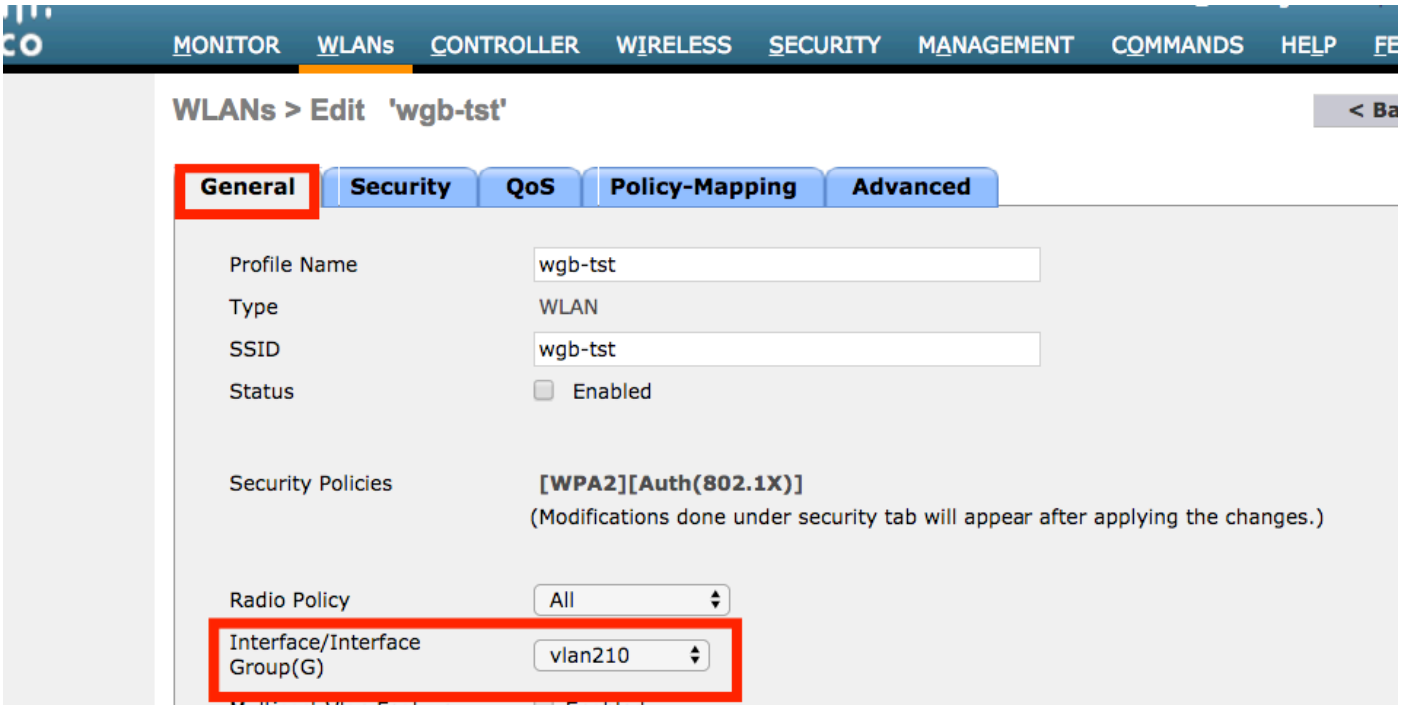
Passaggio 3. Scegliere un nome per il SSID e il profilo, quindi fare clic su Applica.



CLI:

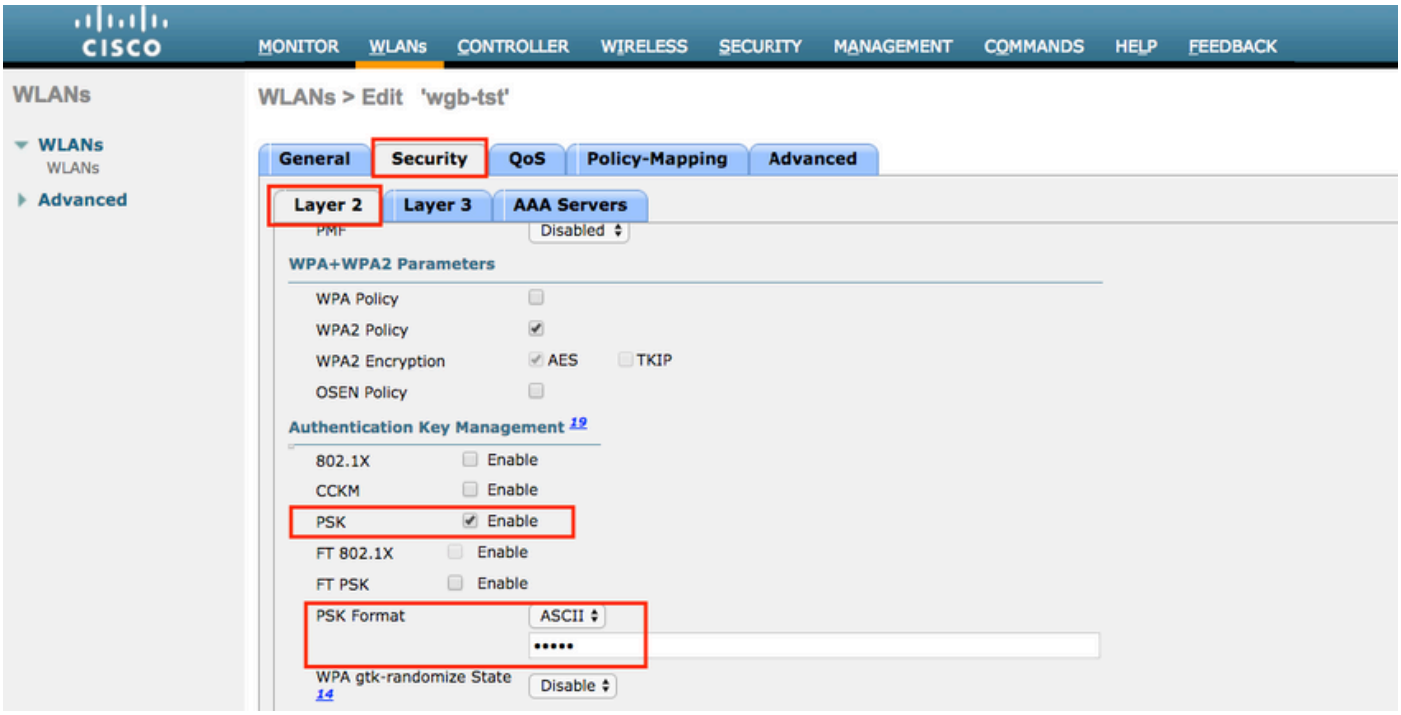
```
> config wlan create <id> <profile-name> <ssid-name>
```

Passaggio 4. Assegnare la VLAN nativa del WGB alla WLAN

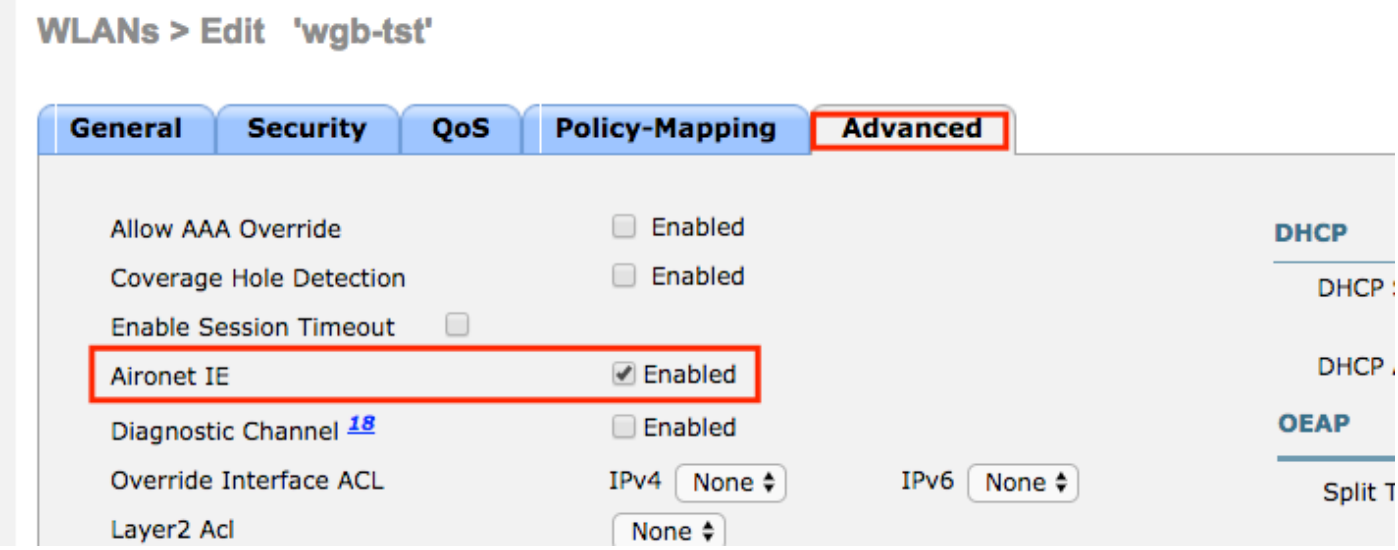


Passaggio 5. Assegnare la chiave già condivisa utilizzata da WGB per l'associazione all'SSID.

Selezionare Sicurezza > Layer 2 > Gestione delle chiavi di autenticazione. Selezionare PSK e immettere la password.



Passaggio 6. Verificare che la WLAN abbia Aironet IE abilitato, altrimenti WGB non sarà in grado di associarla.



Nota: nell'esempio, l'SSID usa la sicurezza WPA2/PSK. Per configurare la WLAN con un metodo di sicurezza più avanzato, come WPA2/802.1x, consultare il seguente collegamento: [autenticazione 802.1x con PEAP, ISE 2.1 e WLC 8.3]

Passaggio 7. Abilitare il WLC al supporto di più VLAN da un WGB

```
>config wgb vlan enable
```

Configurazione WGB

Passaggio 1. Aggiungere le sottointerfacce necessarie per ciascuna VLAN. Nell'esempio, le VLAN 210 (native), 2601 e 2602 vengono aggiunte alla configurazione 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
```

Nota: il gruppo di bridge di sottointerfacce 2601 e 2602 è 21 e 22, poiché l'intervallo valido per i gruppi di bridge è compreso tra 1 e 255.

Nota: il gruppo di bridge per la sottointerfaccia 210 non è specificato perché quando la VLAN nativa viene assegnata a una sottointerfaccia, assegna automaticamente il gruppo di bridge 1.

Passaggio 2. Creare l'SSID (Service Set Identifier).

In questo esempio l'SSID utilizza WPA2/PSK. Se è necessario che WGB venga associato a un SSID con un metodo di protezione più avanzato come WPA2/802.1x, è possibile consultare questo collegamento:

Esempio di configurazione dei bridge per gruppi di lavoro con autenticazione 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
```

Passaggio 3. Aggiungere il SSID all'interfaccia utilizzata per l'associazione al CAPWAP AP.

In questo passaggio viene inoltre impostato l'access point come bridge di gruppi di lavoro con il comando station-role workgroup-bridge.

Nota: nell'esempio, il WGB utilizza l'interfaccia da 2,4 GHz per l'associazione al CAPWAP AP. Se si desidera che il WGB venga associato all'interfaccia da 5 GHz, aggiungere questa configurazione all'interfaccia Dot11Radio1.

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

Passaggio 4. Abilitare la funzione WGB Unified VLAN.

Questo comando consentirà al WGB di informare il WLC in cui la VLAN sui client deve essere assegnata.

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

Configurazione degli switch

Passaggio 1. Creare le VLAN.

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

Passaggio 2. Configurare la porta a cui è collegato il WGB.

```
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
```

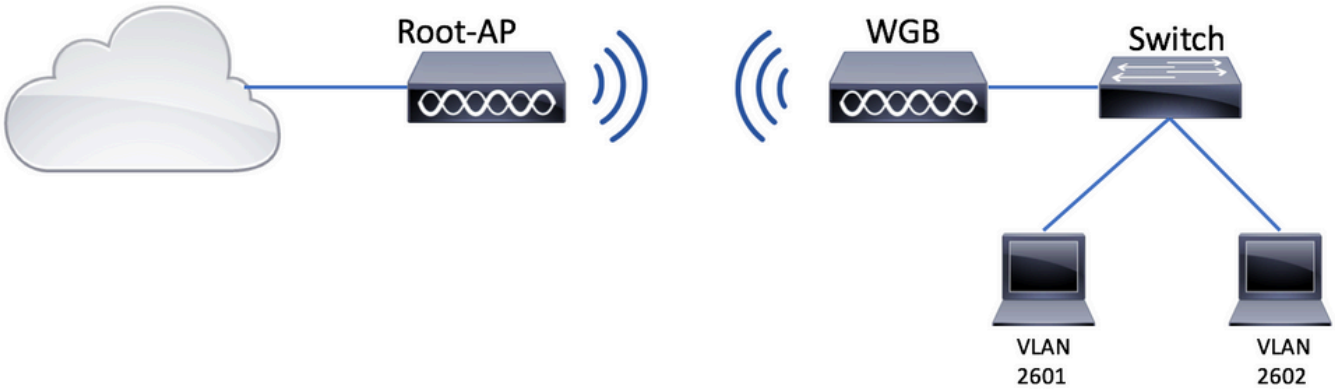
Passaggio 3. Assegnare le interfacce su cui i client sono collegati alla VLAN necessaria.

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

WGB con switch 802.1q dietro e VLAN multiple associate a un access point

autonomo in modalità radice.

Esempio di rete



Configurazione punto di accesso principale

Passaggio 1. Aggiungere le sottointerfacce necessarie per ciascuna VLAN.

Nell'esempio, le VLAN 210 (native), 2601 e 2602 vengono aggiunte alla configurazione dell'access point radice come indicato nel passaggio 1 del protocollo WGB con più VLAN associate a una configurazione CAPWAP - WGB.

Passaggio 2. Creare l'SSID (Service Set Identifier).

In questo esempio il SSID utilizza WPA2/PSK. Se è necessario configurare l'access point radice con un SSID con un metodo di sicurezza più avanzato, come WPA2/802.1x, è possibile consultare questo collegamento:

Configurazione di SSID e VLAN su access point autonomi

```
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
```

Passaggio 3. Aggiungere il SSID all'interfaccia che verrà utilizzata dall'access point radice per trasmettere il SSID.

Nota: nell'esempio, il Root-AP usa l'interfaccia da 2,4 GHz per trasmettere il SSID. Se è necessario che il Root-AP lo trasmetta con l'interfaccia da 5 GHz, aggiungere questa configurazione all'interfaccia 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
```

Il comando infrastructure-client permette all'access point radice di rispettare l'assegnazione della VLAN che i WGB hanno per i propri client cablati. Senza questo comando, l'access point radice assegnerà tutti i client alla VLAN nativa.

Configurazione WGB

Passaggio 1. Aggiungere le sottointerfacce necessarie per ciascuna VLAN.

Nell'esempio, le VLAN 210 (native), 2601 e 2602 vengono aggiunte alla configurazione dell'access point radice come indicato nel passaggio 1 del protocollo WGB con più VLAN associate a una configurazione CAPWAP - WGB.

Passaggio 2. Creare l'SSID (Service Set Identifier).

In questo esempio l'SSID utilizza WPA2/PSK. Se è necessario che WGB venga associato a un SSID con un metodo di protezione più avanzato, ad esempio WPA2/802.1x, è possibile consultare il seguente collegamento:

Esempio di configurazione dei bridge per gruppi di lavoro con autenticazione 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
```

Passaggio 3. Aggiungere il SSID all'interfaccia utilizzata per l'associazione al CAPWAP AP.

In questo passaggio viene inoltre impostato l'access point come bridge di gruppi di lavoro con il comando station-role workgroup-bridge.

Nota: nell'esempio, il WGB utilizza l'interfaccia da 2,4 GHz per l'associazione al CAPWAP AP. Se si desidera che il WGB venga associato all'interfaccia da 5 GHz, aggiungere questa configurazione all'interfaccia 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
```

Configurazione degli switch

È possibile seguire la stessa configurazione per lo switch su WGB con più VLAN associate a un CAPWAP AP.

WGB senza switch in background e VLAN multiple associate a un access point autonomo in modalità radice.

Questo esempio consente a WGB di utilizzare 2 VLAN diverse (native e un'altra). Se si devono avere più di due VLAN, è necessario aggiungere uno switch 802.1q compatibile con WGB e collegare i client a tale switch. Quindi, seguire le istruzioni su WGB con switch 802.1q dietro e più VLAN associate a un access point autonomo in modalità radice.

Esempio di rete

Configurazione punto di accesso principale

Passaggio 1. Aggiungere le sottointerfacce necessarie per ciascuna VLAN.

La configurazione delle sottointerfacce è simile a quella del passo 1 del WGB con più VLAN associate a una configurazione CAPWAP AP - WGB, ma in questo caso è necessario configurare solo la VLAN 210 (nativa) e la VLAN 2602 (VLAN client).

Passaggio 2. Creare l'SSID (Service Set Identifier).

In questo esempio il SSID utilizza WPA2/PSK. Se è necessario configurare l'access point radice con un SSID con un metodo di sicurezza più avanzato, come WPA2/802.1x, è possibile consultare questo collegamento:

Configurazione di SSID e VLAN su access point autonomi

```
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
```

Passaggio 3. Aggiungere il SSID all'interfaccia che verrà utilizzata dall'access point radice per trasmettere il SSID.

Nota: nell'esempio, il Root-AP usa l'interfaccia da 2,4 GHz per trasmettere il SSID. Se è necessario che il Root-AP lo trasmetta con l'interfaccia da 5 GHz, aggiungere questa configurazione all'interfaccia 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
```

Il comando client-infrastruttura consente all'access point radice di rispettare l'assegnazione della VLAN che i WGB hanno per i propri client cablati. Senza questo comando, il punto di accesso radice assegna tutti i client alla VLAN nativa.

Configurazione WGB

Passaggio 1. Aggiungere le sottointerfacce necessarie per ciascuna VLAN. Nell'esempio, le VLAN 210 (native) e 2601 vengono aggiunte alla configurazione WGB.

La configurazione delle sottointerfacce è la stessa di quella visualizzata in Passaggio 1 di WGB con più VLAN associate a un CAPWAP AP AP - configurazione WGB, ma in questo caso sarà sufficiente configurare la VLAN 210 (nativa) e la VLAN 2602 (VLAN client).

Passaggio 2. Creare l'SSID (Service Set Identifier).

In questo esempio l'SSID utilizza WPA2/PSK. Se è necessario che WGB venga associato a un

SSID con un metodo di protezione più avanzato, ad esempio WPA2/802.1x, è possibile consultare il seguente collegamento:

Esempio di configurazione dei bridge per gruppi di lavoro con autenticazione 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
```

Passaggio 3. Aggiungere il SSID all'interfaccia utilizzata per l'associazione al CAPWAP AP.

In questo passaggio viene inoltre impostato l'access point come bridge di gruppi di lavoro con il comando station-role workgroup-bridge.

Nota: nell'esempio, il WGB utilizza l'interfaccia da 2,4 GHz per l'associazione al CAPWAP AP. Se si desidera che il WGB venga associato all'interfaccia da 5 GHz, aggiungere questa configurazione all'interfaccia 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
```

Passaggio 4. Specificare la VLAN client.

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

Verifica

Eseguire questo comando per verificare che WGB sia associato all'access point radice e che quest'ultimo sia in grado di visualizzare i client cablati connessi dietro l'access point 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).