

Configurazione della funzione WLAN Anchor Mobility su Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Scenario esterno/ancora tra 9800 WLC](#)

[Esempio di rete: due Catalyst 9800 WLC](#)

[Configurazione di un elemento esterno 9800 con un ancoraggio 9800](#)

[Esterno 9800 WLC - Anchor AireOS](#)

[Catalyst 9800 Foreign - Diagramma di rete ancoraggio AireOS](#)

[Configurazione di 9800 Foreign con AireOS Anchor](#)

[AireOS esterno - Anchor 9800 WLC](#)

[AireOS Foreign con diagramma reticolare ancoraggio 9800](#)

[Configurazione di un router esterno 9800 con ancoraggio AireOS](#)

[Verifica](#)

[Verifica sul WLC 9800](#)

[Verifica sul WLC di AireOS](#)

[Risoluzione dei problemi](#)

[Debug condizionale e traccia Radioactive \(RA\)](#)

[Verifica del WLC di AireOS](#)

Introduzione

In questo documento viene descritto come configurare una WLAN (Wireless Local Area Network) su uno scenario esterno/di ancoraggio con i controller wireless Catalyst 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso ai controller wireless tramite interfaccia a riga di comando (CLI) o interfaccia grafica utente (GUI)
- Mobilità sui Cisco Wireless LAN Controller (WLC)
- 9800 Wireless Controller
- WLC AireOS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AireOS WLC versione 8.8 MR2 (è possibile utilizzare anche le immagini speciali 8.5 di Inter Release Controller Mobility (IRCM))
- 9800 WLC v16.10 o versioni successive
- Modello di configurazione 9800 WLC

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.

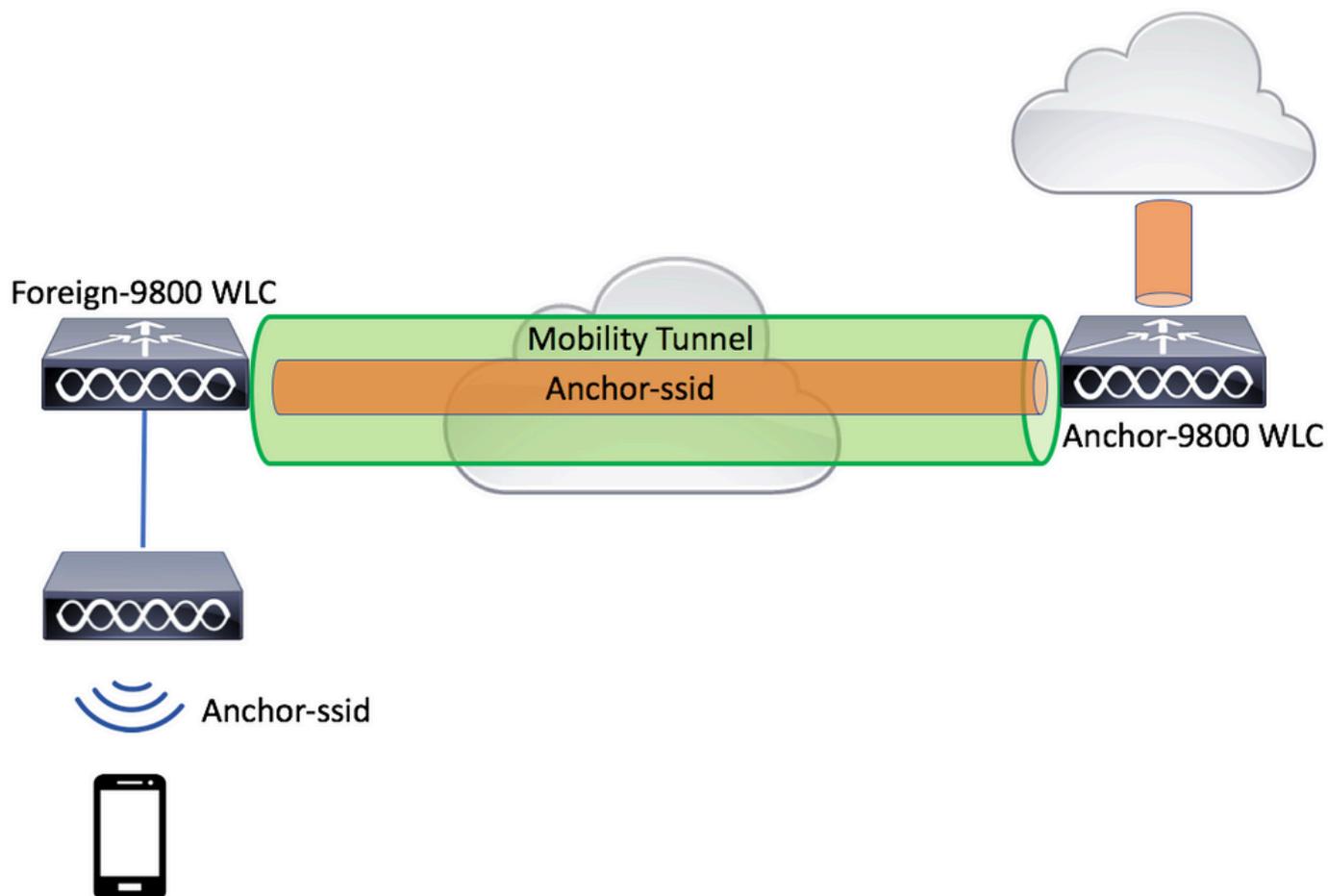
Configurazione

Si tratta di una funzione normalmente utilizzata per gli scenari di accesso guest, per terminare tutto il traffico proveniente dai client in un singolo punto di uscita L3, anche se i client provengono da controller e posizioni fisiche diversi. Il tunnel per la mobilità fornisce un meccanismo per mantenere il traffico isolato mentre attraversa la rete.

Scenario esterno/ancora tra 9800 WLC

In questo scenario vengono illustrati i due Catalyst 9800 utilizzati.

Esempio di rete: due Catalyst 9800 WLC



Per gli scenari di mobilità guest, sono disponibili due ruoli controller principali:

- Controller esterno: questo WLC è proprietario del layer 2 o del lato wireless. Sono collegati dei punti di accesso. Tutto il traffico client per le WLAN ancorate viene incapsulato nel tunnel per la mobilità da inviare all'ancoraggio. Non esiste localmente.
- Controller di ancoraggio: questo è il punto di uscita di livello 3. Riceve i tunnel di mobilità dai controller esterni e decapsula o termina il traffico client nel punto di uscita (VLAN). È il punto in cui i client vengono visualizzati nella rete, quindi il nome dell'ancoraggio.

I punti di accesso sul WLC esterno trasmettono gli SSID WLAN e hanno un tag di policy assegnato che collega il profilo WLAN al profilo di policy appropriato. Quando un client wireless si connette a questo SSID, il controller esterno invia entrambi, il nome SSID e il profilo dei criteri come parte delle informazioni del client al WLC di ancoraggio. Al momento della ricezione, il WLC di ancoraggio controlla la propria configurazione in modo che corrisponda al nome dell'SSID e al nome del profilo dei criteri. Quando il WLC di ancoraggio trova una corrispondenza, applica la configurazione corrispondente e un punto di uscita al client wireless. Pertanto, è obbligatorio che i nomi e le configurazioni del profilo WLAN e del profilo delle policy corrispondano su entrambi i dispositivi esterno 9800 WLC e ancoraggio 9800 WLC, ad eccezione della VLAN in Policy Profile.

 Nota: i nomi dei profili WLAN e dei profili delle policy possono corrispondere sia su 9800 Anchor che su 9800 Foreign WLC.

Configurazione di un elemento esterno 9800 con un ancoraggio 9800

Passaggio 1. Costruire un tunnel per la mobilità tra il WLC di Foreign 9800 e il WLC di Anchor 9800.

È possibile fare riferimento a questo documento: [Configurazione delle topologie di mobilità su Catalyst 9800](#)

Passaggio 2. Creare l'SSID desiderato su entrambi i WLC del 9800.

Metodi di protezione supportati:

- Open (Aperto)
- Filtro MAC
- Chiave primaria
- Punto1x
- Autenticazione Web locale/esterna (LWA)
- Autenticazione Web centrale (CWA)



Nota: entrambi i WLC del 9800 devono avere lo stesso tipo di configurazione, altrimenti l'ancoraggio non funziona.

Passaggio 3. Accedere al WLC 9800 esterno e definire l'indirizzo IP dell'ancoraggio 9800 WLC nel profilo dei criteri.

Passare a [Configuration > Tags & Profiles > Policy > + Add.](#)

Add Policy Profile
✕

General
Access Policies
QOS and AVC
Mobility
Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

<p>Name* <input style="width: 90%;" type="text" value="anchor-policy-profile"/></p> <p>Description <input style="width: 90%;" type="text" value="Enter Description"/></p> <p>Status ENABLED <input checked="" type="checkbox"/></p> <p>Passive Client <input type="checkbox"/> DISABLED</p> <p>Encrypted Traffic Analytics <input type="checkbox"/> DISABLED</p>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> WLAN Switching Policy </div> <p>Central Switching <input checked="" type="checkbox"/></p> <p>Central Authentication <input checked="" type="checkbox"/></p> <p>Central DHCP <input checked="" type="checkbox"/></p> <p>Central Association <input checked="" type="checkbox"/></p> <p>Flex NAT/PAT <input type="checkbox"/></p>
CTS Policy	
<p>Inline Tagging <input type="checkbox"/></p> <p>SGACL Enforcement <input type="checkbox"/></p> <p>Default SGT <input style="width: 90%;" type="text" value="2-65519"/></p>	

↶ Cancel

📄
Save & Apply to Device

Nella Mobility scheda, scegliere l'indirizzo IP dell'ancoraggio 9800 WLC.

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (1)
Anchor IP 172.16.0.5	Anchor IP Anchor Priority 10.88.173.49 Tertiary ...

Cancel Save & Apply to Device

Passaggio 4. Collegare il profilo dei criteri alla WLAN all'interno del tag dei criteri assegnato agli access point associati al controller esterno che gestisce la WLAN.

Passare a Configuration > Tags & Profiles > Tags e crearne uno nuovo o utilizzare quello esistente.

Edit Policy Tag

Name* PT1

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Map WLAN and Policy

WLAN Profile* anchor-ssid Policy Profile* anchor-policy

x ✓

Accertarsi di scegliere **Update & Apply to Device** di applicare le modifiche al tag dei criteri.

Edit Policy Tag ✕

Name*

Description

+ Add

	WLAN Profile	Policy Profile
<input type="checkbox"/>	anchor-ssid	anchor-policy

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Passaggio 5 (facoltativo). Assegnare il tag dei criteri a un punto di accesso o verificare che ne sia già dotato.

Passare a [Configuration > Wireless > Access Points > AP name > General](#).

✕
Edit AP

General
Interfaces
High Availability
Inventory
Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>	Primary Software Version	8.5.97.110
Location*	<input type="text" value="default-location"/>	Predownloaded Status	N/A
Base Radio MAC	000a.ad00.1f00	Predownloaded Version	N/A
Ethernet MAC	000a.ad00.1ff0	Next Retry Time	N/A
Admin Status	<input style="border: 1px solid #ccc; width: 100%;" type="button" value="Enabled"/>	Boot Version	8.5.97.110
AP Mode	<input style="border: 1px solid #ccc; width: 100%;" type="button" value="Local"/>	IOS Version	
Operation Status	Registered	Mini IOS Version	0.51.0.3
Fabric Status	Disabled	IP Config	

Tags

Policy	<input style="border: 1px solid #ccc; width: 100%;" type="button" value="PT1"/>
Site	<input style="border: 1px solid #ccc; width: 100%;" type="button" value="ST1"/>
RF	<input style="border: 1px solid #ccc; width: 100%;" type="button" value="RT1"/>

CAPWAP Preferred Mode	Not Configured
Static IPv4 Address	11.11.0.39
Static IP (IPv4/IPv6)	<input checked="" type="checkbox"/>
Static IP (IPv4/IPv6)	<input type="text" value="11.11.0.39"/>
Netmask	<input type="text" value="255.255.0.0"/>
Gateway (IPv4/IPv6)	<input type="text" value="11.11.0.1"/>
DNS IP Address (IPv4/IPv6)	<input type="text" value="0.0.0.0"/>
Domain Name	<input type="text" value="Cisco"/>

Time Statistics

Up Time	3 days 0 hrs 34 mins 26 secs
---------	------------------------------

↶ Cancel

📄 Update & Apply to Device

Nota: se si modifica il tag AP dopo averlo scelto **Update & Apply to Device**, l'access point riavvia il relativo tunnel CAPWAP, perdendo l'associazione con il WLC 9800 e quindi lo ripristina.

Dalla CLI:

Foreign 9800 WLC

```

# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit

# ap aaaa.bbbb.dddd
# site-tag PT1
# exit

```

Passaggio 6. Accedere all'ancoraggio 9800 WLC e creare il profilo dei criteri di ancoraggio. Accertatevi che abbia lo stesso nome che avete usato sui WLC stranieri 9800.

Passare a Configuration > Tags & Profiles > Policy > + Add.

Add Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association

Flex NAT/PAT

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

Passare alla Mobility scheda e abilitare Export Anchor. In questo modo, il WLC 9800 diventa il WLC di ancoraggio 9800 per qualsiasi WLAN che utilizzi quel profilo di policy. Quando il WLC esterno 9800 invia i clienti all'ancoraggio 9800 WLC, informa sulla WLAN e sul Profilo criterio a cui il client

è assegnato, in modo che l'ancoraggio 9800 WLC sappia a quale Profilo criterio locale utilizzare.

 Nota: non è necessario configurare i peer mobilità ed esportare l'ancoraggio contemporaneamente. Scenario di configurazione non valido.

 Nota: non utilizzare l'impostazione Esporta ancoraggio per i profili di criteri associati a un profilo WLAN su un controller con access point. In questo modo si impedisce la trasmissione dell'SSID, pertanto questo criterio deve essere utilizzato esclusivamente per la funzionalità di ancoraggio.

Add Policy Profile ✕

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)	Selected (0)					
<table><thead><tr><th>Anchor IP</th><th>Anchor Priority</th></tr></thead><tbody><tr><td> 172.16.0.5 →</td><td rowspan="2">Anchors not assigned</td></tr><tr><td> 10.88.173.49 →</td></tr></tbody></table>	Anchor IP	Anchor Priority	 172.16.0.5 →	Anchors not assigned	 10.88.173.49 →	
Anchor IP	Anchor Priority					
 172.16.0.5 →	Anchors not assigned					
 10.88.173.49 →						

Dalla CLI:

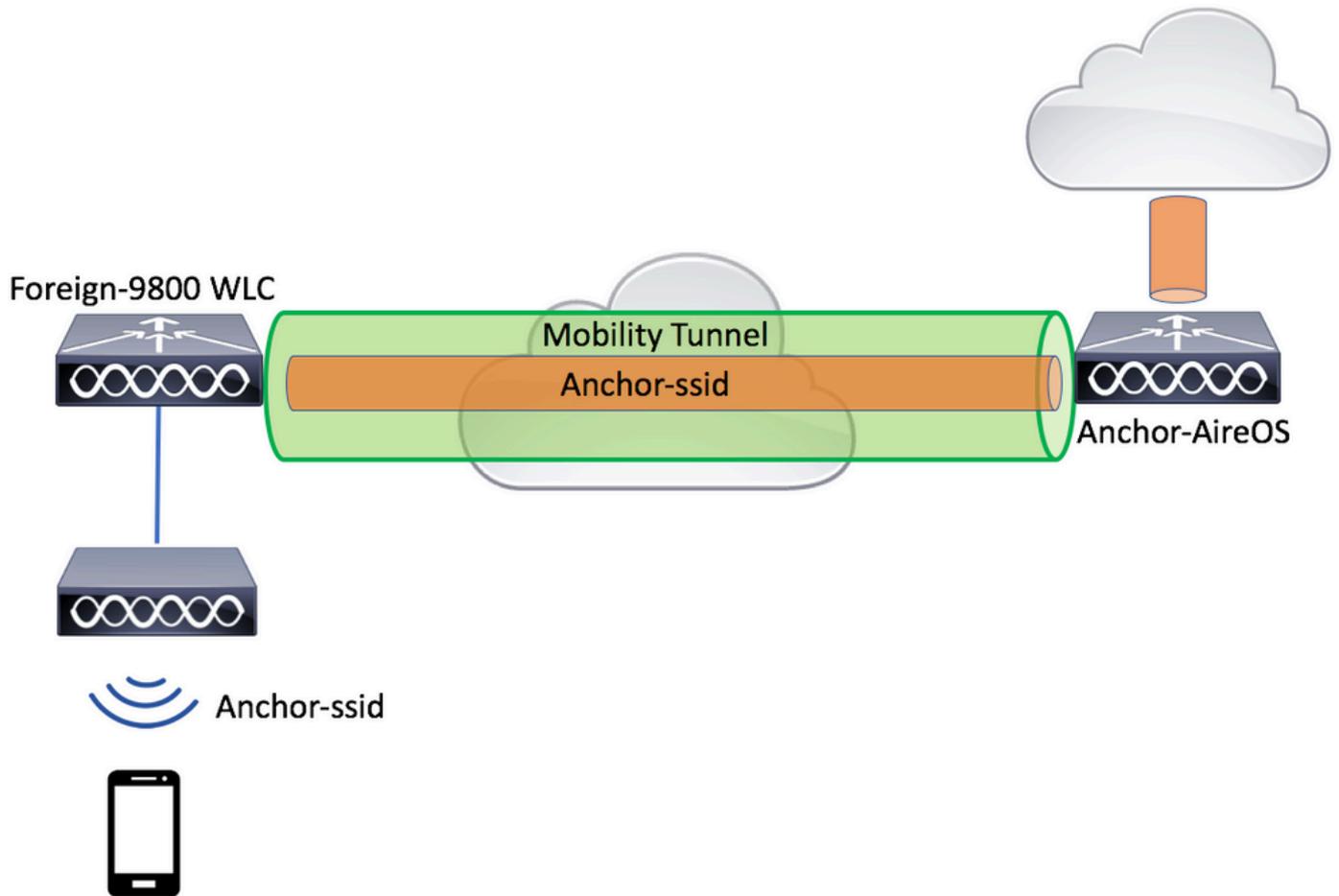
Anchor 9800 WLC

```
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Esterno 9800 WLC - Anchor AireOS

In questa configurazione viene illustrato lo scenario in cui un Catalyst 9800 WLC viene utilizzato come dispositivo esterno con un AireOS Unified WLC utilizzato come ancoraggio.

Catalyst 9800 Foreign - Diagramma di rete ancoraggio AireOS



Configurazione di 9800 Foreign con AireOS Anchor

Passaggio 1. Costruire un tunnel per la mobilità tra il WLC Foreign 9800 e il WLC Anchor AireOS.

Fare riferimento a questo documento: [Configurazione delle topologie di mobilità su Catalyst 9800](#)

Passaggio 2. Creare le WLAN desiderate su entrambi i WLC.

Metodi di protezione supportati:

- Open (Aperto)
- Filtro MAC
- Chiave primaria
- Punto1x
- Autenticazione Web locale/esterna (LWA)

- Autenticazione Web centrale (CWA)

 Nota: i WLC AireOS e 9800 devono avere entrambi lo stesso tipo di configurazione, altrimenti l'ancoraggio non funziona.

Passaggio 3. Accedere al WLC 9800 (che agisce come dispositivo esterno) e creare il profilo della policy di ancoraggio.

Passare a Configuration > Tags & Profiles > Policy > + Add.

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	<input type="text" value="anchor-policy"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox"/>
Status	ENABLED <input checked="" type="checkbox"/>	Central Authentication	<input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association	<input checked="" type="checkbox"/>
CTS Policy		Flex NAT/PAT	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Passare alla Mobility scheda e scegliere il WLC AireOS di ancoraggio. Il WLC 9800 inoltra il traffico dell'SSID associato a questo Profilo criteri all'ancoraggio scelto.

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)	Selected (1)
Anchor IP	Anchor IP Anchor Priority
No anchors available	<div style="border: 2px solid red; padding: 5px;">  10.88.173.105 Tertiary ... <input type="button" value="←"/> </div>

Passaggio 4. Collegare il profilo dei criteri alla WLAN all'interno del tag dei criteri assegnato agli access point associati al controller esterno che gestisce la WLAN.

Passare a Configuration > Tags & Profiles > Tags e crearne uno nuovo o utilizzare quello esistente.

Edit Policy Tag

Name*

Description

WLAN Profile Policy Profile

◀ ◁ 0 ▷ ▶ 10 items per page No items to display

Map WLAN and Policy

WLAN Profile*

Policy Profile*

Accertarsi di scegliere **Update & Apply to Device** di applicare le modifiche al tag dei criteri.

Edit Policy Tag ✕

Name*

Description

+ Add

	WLAN Profile	Policy Profile
<input type="checkbox"/>	anchor-ssid	anchor-policy

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Passaggio 5 (facoltativo). Assegnare il sito a un punto di accesso o verificare che ne sia già dotato.

Passare a [Configuration > Wireless > Access Points > AP name > General](#).

✕
Edit AP

General
Interfaces
High Availability
Inventory
Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>	Primary Software Version	8.5.97.110
Location*	<input type="text" value="default-location"/>	Predownloaded Status	N/A
Base Radio MAC	000a.ad00.1f00	Predownloaded Version	N/A
Ethernet MAC	000a.ad00.1ff0	Next Retry Time	N/A
Admin Status	<input type="text" value="Enabled"/>	Boot Version	8.5.97.110
AP Mode	<input type="text" value="Local"/>	IOS Version	
Operation Status	Registered	Mini IOS Version	0.51.0.3
Fabric Status	Disabled		

Tags

Policy	<input type="text" value="PT1"/>
Site	<input type="text" value="ST1"/>
RF	<input type="text" value="RT1"/>

IP Config

CAPWAP Preferred Mode	Not Configured
Static IPv4 Address	11.11.0.39
Static IP (IPv4/IPv6)	<input checked="" type="checkbox"/>
Static IP (IPv4/IPv6)	<input type="text" value="11.11.0.39"/>
Netmask	<input type="text" value="255.255.0.0"/>
Gateway (IPv4/IPv6)	<input type="text" value="11.11.0.1"/>
DNS IP Address (IPv4/IPv6)	<input type="text" value="0.0.0.0"/>
Domain Name	<input type="text" value="Cisco"/>

Time Statistics

Up Time	3 days 0 hrs 34 mins 26 secs
---------	------------------------------

↶ Cancel

Update & Apply to Device

Nota: se si modifica il tag AP dopo averlo scelto, l'Update & Apply to Device access point riavvia il relativo tunnel CAPWAP, quindi perde l'associazione con il WLC 9800 e lo ripristina.

Dalla CLI:

```
# config t
```

```
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit
```

```
# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit
```

```
# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

Passaggio 6. Configurare il WLC di AireOS come ancoraggio.

Accedere a AireOS e selezionare WLANs > WLANs. Scegliere la freccia all'estremità destra della riga WLAN per accedere al menu a discesa e scegliere Mobility Anchors.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN			Enabled	[WPA2][Auth(PSK)]
2	Remote LAN			Enabled	None
3	WLAN			Enabled	Web-Passthrough
4	Remote LAN			Disabled	802.1X, MAC Filtering
5	WLAN	anchor-ssid	anchor-ssid	Disabled	[WPA2][Auth(802.1X)]

Impostatelo come ancoraggio locale.

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority 1

3

Foot Notes

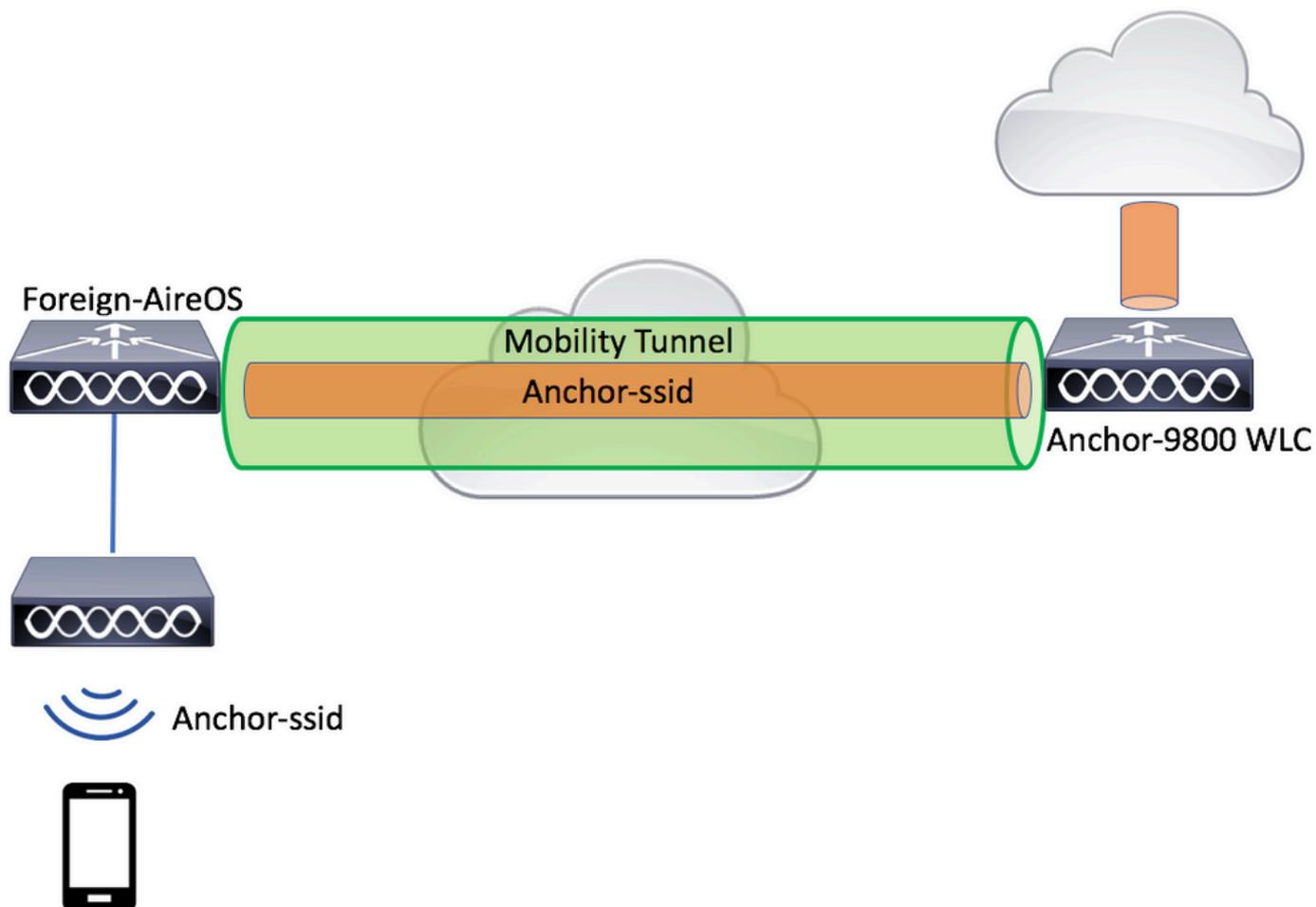
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Dalla CLI:

```
> config wlan disable <wlan-id>  
> config wlan mobility anchor add <wlan-id> <AireOS-WLC's-mgmt-interface>  
> config wlan enable <wlan-id>
```

AireOS esterno - Anchor 9800 WLC

AireOS Foreign con diagramma reticolare ancoraggio 9800



Configurazione di un router esterno 9800 con ancoraggio AireOS

Passaggio 1. Costruire un tunnel per la mobilità tra il WLC Foreign 9800 e il WLC Anchor AireOS.

È possibile fare riferimento a questo documento: [Configurazione delle topologie di mobilità su Catalyst 9800](#)

Passaggio 2. Creare il SSID desiderato su entrambi i WLC.

Metodi di protezione supportati:

- Open (Aperto)
- Filtro MAC
- Chiave primaria
- Punto1x
- Autenticazione Web locale/esterna (LWA)
- Autenticazione Web centrale (CWA)

 Nota: i WLC AireOS e 9800 devono avere entrambi lo stesso tipo di configurazione, altrimenti l'ancoraggio non funziona.

Passaggio 3. Accedere al WLC 9800 (che funge da ancoraggio) e creare il profilo dei criteri di ancoraggio.

Passare a Configuration > Tags & Profiles > Policy > + Add. Assicurarsi che il nome del profilo della policy su 9800 sia esattamente lo stesso nome del profilo sul WLC di AireOS, altrimenti non funzionerà.

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	<input type="text" value="anchor-ssid"/>	WLAN Switching Policy Central Switching <input checked="" type="checkbox"/> Central Authentication <input checked="" type="checkbox"/> Central DHCP <input checked="" type="checkbox"/> Central Association <input checked="" type="checkbox"/> Flex NAT/PAT <input type="checkbox"/>
Description	<input type="text" value="Enter Description"/>	
Status	<input checked="" type="checkbox"/> ENABLED	
Passive Client	<input type="checkbox"/> DISABLED	
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	
CTS Policy		
Inline Tagging	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	
Default SGT	<input type="text" value="2-65519"/>	

Passare alla Mobility scheda e abilitare Export Anchor. In questo modo, il WLC 9800 diventa il WLC di ancoraggio 9800 per qualsiasi WLAN che utilizzi quel profilo di policy. Quando il WLC esterno di AireOS invia i client all'ancoraggio 9800 WLC, informa sul nome della WLAN a cui è assegnato il client, in modo che il WLC dell'ancoraggio 9800 sappia a quale configurazione WLAN locale utilizzare e utilizzi questo nome anche per sapere quale profilo dei criteri locali utilizzare.

Add Policy Profile ✕

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
 172.16.0.5 →	Anchors not assigned	
 10.88.173.49 →		

 **Nota:** assicurarsi di utilizzare questo profilo dei criteri esclusivamente per ricevere traffico da controller esterni.

Dalla CLI:

Anchor 9800 WLC

```
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Passaggio 4. Configurare il WLC di AireOS come dispositivo esterno.

Accedere a AireOS e selezionare **WLANs > WLANs**. Passare alla freccia in giù alla fine della riga **WLAN** e selezionare **Mobility AnchorS**.

WLANs

WLANs

WLANs

Advanced

WLANs

Current Filter: None [Change Filter] [Clear Filter]

Create New [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN			Enabled	[WPA2][Auth(PSK)]
2	Remote LAN		---	Enabled	None
3	WLAN			Enabled	Web-Passthrough
4	Remote LAN		---	Disabled	802.1X, MAC Filtering
5	WLAN	anchor-ssid	anchor-ssid	Disabled	[WPA2][Auth(802.1X)]

- Remove
- Mobility Anchors
- 802.11u
- Foreign Maps
- Service Advertisements
- Hotspot 2.0

Impostare il WLC 9800 come ancoraggio per questo SSID.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor) 10.88.173.105

Priority 3

Foot Notes

1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Dalla CLI:

```
> config wlan disable <wlan-id>
> config wlan mobility anchor add <wlan-id> <9800 WLC's-mgmt-interface>
> config wlan enable <wlan-id>
```

Verifica

È possibile utilizzare questi comandi per verificare la configurazione e lo stato dei client wireless con un SSID di ancoraggio/esterno.

Verifica sul WLC 9800

```
# show run wlan
# show wlan summary
# show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <ap-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Verifica sul WLC di AireOS

```
> show client summary
> show client detail <client-mac-addr>
> show wlan summary
> show wlan <wlan-id>
```

Risoluzione dei problemi

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori, gli avvisi e i messaggi relativi alla connettività del client vengono costantemente registrati ed è possibile visualizzare gli eventi relativi a un evento imprevisto o a una condizione di errore dopo che si è verificato.



Nota: a seconda del volume di log generato, è possibile tornare indietro di alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal 9800 WLC, è possibile connettersi al 9800 WLC tramite SSH/Telnet e fare riferimento a queste procedure. (Accertatevi di registrare la sessione in un file di testo)

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei log nel tempo che precede il momento in cui si è verificato il problema.

```
# show clock
```

Passaggio 2. Raccogliere syslog dal buffer del controller o dal syslog esterno come richiesto dalla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato del sistema e gli eventuali errori.

```
# show logging
```

Passaggio 3. Raccogliere le tracce del livello di avviso sempre attive per l'indirizzo MAC o IP specifico. Il peer per la mobilità remota può filtrare questa condizione se si sospetta un problema del tunnel per la mobilità o in base all'indirizzo MAC del client wireless.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

Passaggio 4. È possibile visualizzare il contenuto della sessione oppure copiare il file su un server TFTP esterno.

```
# more bootflash:always-on-<FILENAME.txt>  
or  
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Debug condizionale e traccia Radioactive (RA)

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire le tracce Radio attive (RA), che forniscono le tracce a livello di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug

condizionale, eseguire la procedura seguente.

Passaggio 5. Verificare che non vi siano condizioni di debug abilitate.

```
# clear platform condition all
```

Passaggio 6. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare.

Questi comandi iniziano a monitorare l'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 Nota: per monitorare più client alla volta, eseguire il comando `debug wireless mac <aaa.bbbb.ccc>` per ogni indirizzo MAC.

 Nota: non si visualizza l'output dell'attività del client nella sessione terminale, in quanto tutto viene memorizzato internamente per essere visualizzato successivamente.

Passaggio 7. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 8. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Allo scadere del tempo di monitoraggio o dopo aver interrotto il debug wireless, il WLC 9800 genera un file locale con il nome: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Passaggio 9. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare la traccia dell'Autorità registrazione.log su un server esterno oppure visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA:

```
# dir bootflash: | inc ra_trace
```

Copiare il file su un server esterno:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Visualizzare il contenuto:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 10. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log a livello di debug. Non è necessario eseguire di nuovo il debug del client, in quanto i log sono già stati scritti nella memoria del controller ed è sufficiente compilarne una visualizzazione più dettagliata.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

 Nota: questo output del comando restituisce tracce per tutti i livelli di registrazione per tutti i processi ed è piuttosto voluminoso. Coinvolgere Cisco TAC per analizzare queste tracce.

È possibile copiare il file `ra-internal-FILENAME.txt` su un server esterno oppure visualizzarlo direttamente sullo schermo.

Copiare il file su un server esterno:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Visualizzare il contenuto:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Passaggio 11. Rimuovere le condizioni di debug.

```
# clear platform condition all
```



Nota: assicurarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

Verifica del WLC di AireOS

È possibile eseguire questo comando per monitorare l'attività di un client wireless su un WLC AireOS.

```
> debug client <client-mac-add>
```

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).