

在Catalyst 9800上設定WLAN錨點行動功能

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[9800 WLC之間的外部/錨點案例](#)

[網路圖表：兩個Catalyst 9800 WLC](#)

[使用9800錨點設定9800外部](#)

[外部9800 WLC — 錨點AireOS](#)

[Catalyst 9800外部 — AireOS錨點網路圖](#)

[使用AireOS錨點配置9800外部](#)

[外部AireOS — 錨點9800 WLC](#)

[帶9800錨點網路圖的AireOS Foreign](#)

[使用AireOS錨點配置9800外部](#)

[驗證](#)

[在9800 WLC上驗證](#)

[在AireOS WLC上驗證](#)

[疑難排解](#)

[條件式偵錯和無線電主動式追蹤](#)

[驗證AireOS WLC](#)

簡介

本文說明如何使用Catalyst 9800無線控制器在外部/錨點方案上設定無線區域網路(WLAN)。

必要條件

需求

思科建議您瞭解以下主題：

- 對無線控制器的命令列介面(CLI)或圖形使用者介面(GUI)訪問
- 思科無線LAN控制器(WLC)上的行動化
- 9800無線控制器
- AireOS WLC

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AireOS WLC版本8.8 MR2(您還可以使用版本間控制器移動(IRCM)特殊8.5映像)
- 9800 WLC v16.10或更高版本
- 9800 WLC組態型號

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

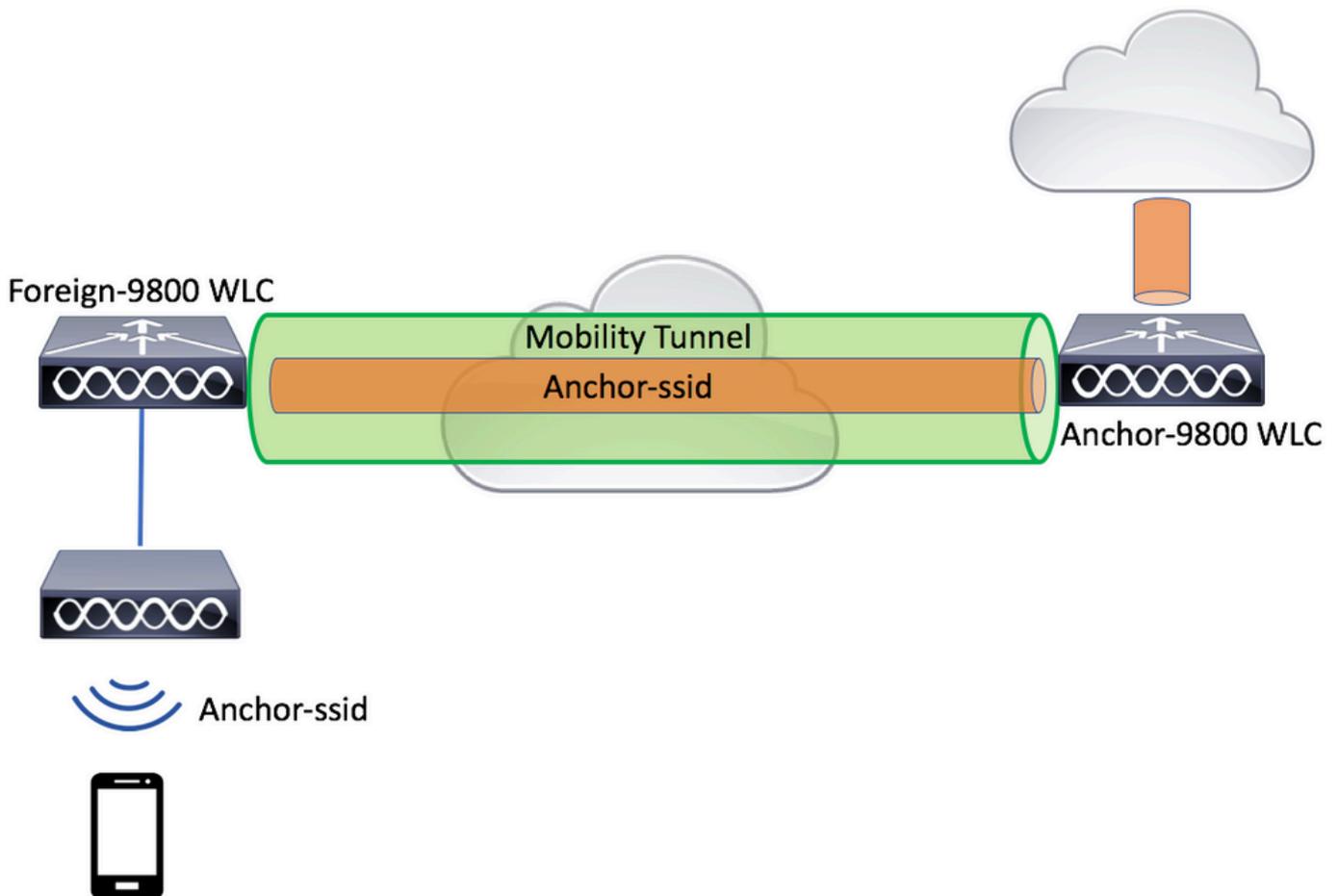
設定

此功能通常用於Guest訪問方案，用於將來自客戶端的所有流量終止到單個L3出口點，即使客戶端來自不同的控制器和物理位置也是如此。移動隧道提供了一種機制，使流量在穿越網路時保持隔離。

9800 WLC之間的外部/錨點案例

此案例說明使用的是兩部Catalyst 9800。

網路圖表：兩個Catalyst 9800 WLC



對於行動化訪客案例，有兩個主要控制器角色：

- 外部控制器：此WLC擁有第2層或無線端。它有接入點。錨點WLAN的所有使用者端流量都會封裝到行動通道中，以傳送至錨點。它不會在本地退出。

- 錨點控制器：這是第3層出口點。它接收來自外部控制器的行動通道，並對進入出口點 (VLAN)的客戶端流量解除封裝或終止。這是網路中可見客戶端的點，因此是錨點名稱。

外部WLC上的接入點廣播WLAN SSID，並分配了將WLAN配置檔案與相應策略配置檔案連結起來的策略標籤。當無線客戶端連線到此SSID時，外部控制器將兩者都作為客戶端資訊的一部分將SSID名稱和策略配置檔案傳送到錨點WLC。收到錨點WLC後，會檢查其自己的配置，以匹配SSID名稱以及策略配置檔名稱。錨點WLC找到相符專案後，會將與其對應的組態和退出點套用到無線使用者端。因此，除了策略配置檔案下的VLAN外，外來9800 WLC和錨點9800 WLC上的WLAN和策略配置檔名稱和配置必須匹配。

 注意:9800錨點和9800外部WLC上的WLAN配置檔案和策略配置檔名稱都可以匹配。

使用9800錨點設定9800外部

步驟 1. 在外部9800 WLC和錨點9800 WLC之間建立行動通道。

請參閱以下檔案：[在Catalyst 9800上設定行動化拓撲](#)

步驟 2.在兩台9800 WLC上建立所需的SSID。

支援的安全方法：

- 未解決
- MAC過濾器
- PSK
- Dot1x
- 本地/外部Web驗證(LWA)
- 中央Web驗證(CWA)

 註：兩個9800 WLC必須具有相同型別的配置，否則錨點無法使用。

步驟 3.登入到外部9800 WLC並在策略配置檔案下定義錨點9800 WLC IP地址。

導航至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-profile"/>	WLAN Switching Policy
Description	<input type="text" value="Enter Description"/>	Central Switching <input checked="" type="checkbox"/>
Status	<input checked="" type="checkbox"/> ENABLED	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"/>	

在選Mobility項卡上，選擇錨點9800 WLC的IP地址。

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

步驟 4. 將策略配置檔案與分配給與此WLAN服務的外部控制器相關聯的AP的策略標籤內的WLAN連結。

導覽至 Configuration > Tags & Profiles > Tags 並建立一個新系統或使用現有的系統。

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 ✓

確保選擇 Update & Apply to Device 將更改應用到策略標籤。

Edit Policy Tag ✕

Name*

Description

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

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

步驟 5. (選用) 將策略標籤分配給AP或驗證它是否已經擁有該標籤。

導航至 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

注意:請注意，如果您在選擇Update & Apply to Device後對AP標籤執行更改，則AP會重新啟動其隧道CAPWAP，因此它將與9800 WLC失去關聯，然後恢復該關聯。

在CLI上：

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

```

步驟 6. 登入到錨點9800 WLC並建立錨點原則設定檔。確保其與您在外部9800 WLC上使用的名稱完全相同。

導航至 Configuration > Tags & Profiles > Policy > + Add。

導覽至 Mobility 索引標籤並啟用 Export Anchor。這指示9800 WLC是使用該原則設定檔的任何WLAN的錨點9800 WLC。當外部9800 WLC將使用者端傳送到錨點9800 WLC時，它會通知有關使用者端所指的WLAN和原則設定檔，因此錨點9800 WLC知道使用哪個本地原則設定檔。

 註：不能同時配置移動對等體和匯出錨點。這是無效的配置方案。

 注意：對於與具有接入點的控制器上的WLAN配置檔案關聯的任何策略配置檔案，不得使用「匯出錨點」設定。這將阻止廣播SSID，因此此策略必須專門用於錨點功能。

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 →		

在CLI上：

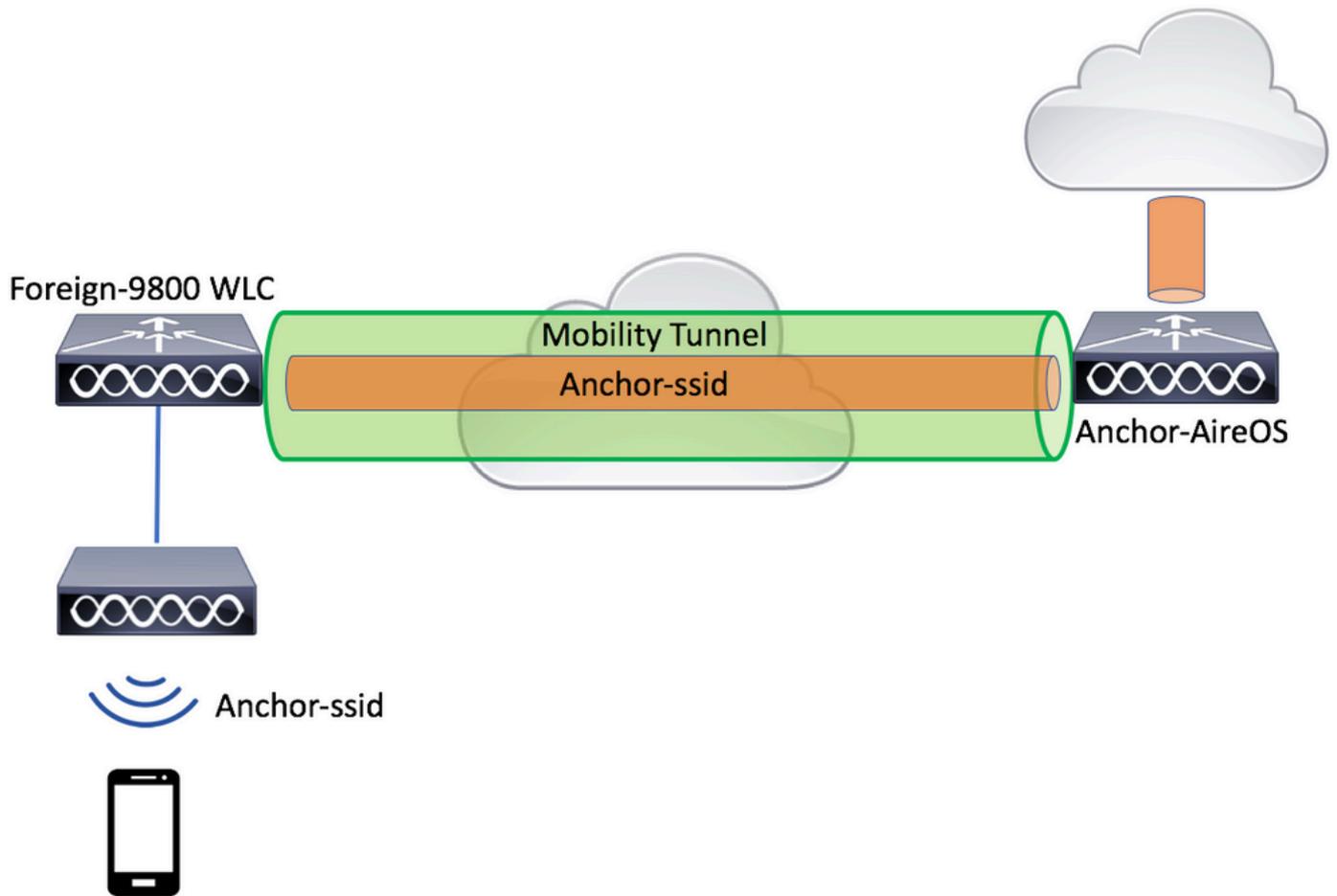
Anchor 9800 WLC

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

外部9800 WLC — 錨點AireOS

此設定描述以下情況：將Catalyst 9800 WLC用作外部，將AireOS Unified WLC用作錨點。

Catalyst 9800外部 — AireOS錨點網路圖



使用AireOS錨點配置9800外部

步驟 1. 在外部9800 WLC和錨點AireOS WLC之間建立行動通道。

請參閱本檔案：在[Catalyst 9800上設定行動化拓撲](#)

步驟 2. 在兩個WLC上建立所需的WLAN。

支援的安全方法：

- 未解決
- MAC過濾器
- PSK
- Dot1x
- 本地/外部Web驗證(LWA)
- 中央Web驗證(CWA)

 註:AireOS WLC和9800 WLC必須具有相同的配置型別，否則錨點無法正常工作。

步驟 3. 登入9800 WLC (作為外部使用) 並建立錨點原則設定檔。

導航至 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"/>		

導覽至 Mobility 索引標籤，並選擇錨點 AireOS WLC。9800 WLC 將與此原則設定檔關聯的 SSID 流量轉送到選定的錨點。

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: 2px;">  10.88.173.105 Tertiary ... <input type="button" value="←"/> </div>

步驟 4. 將策略配置檔案與分配給與此WLAN服務的外部控制器相關聯的AP的策略標籤內的WLAN連結。

導覽至 Configuration > Tags & Profiles > Tags 並建立一個新系統或使用現有的系統。

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*

確保選擇 Update & Apply to Device 將更改應用到策略標籤。

Edit Policy Tag ✕

Name*

Description

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

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

步驟 5. (選用) 將站點分配給 AP 或驗證它是否已經擁有該站點。

導航至 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

注意：請注意，如果您在選擇 Update & Apply to Device 後對 AP 標籤執行更改，則 AP 會重新啟動其隧道 CAPWAP，因此它將與 9800 WLC 失去關聯，然後恢復它。

在 CLI 上：

```
# 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
```

步驟 6.將AireOS WLC配置為錨點。

登入到AireOS並導航至WLANs > WLANs。選擇WLAN行右端的箭頭，以導航到下拉選單並選擇Mobility Anchors。

The screenshot shows the Cisco AireOS configuration interface for WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' tab is active. On the left, a sidebar shows 'WLANs' and 'Advanced' options. The main content area displays a table of WLANs with columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. The table contains five entries. The fifth entry, 'anchor-ssid', is selected, and a dropdown menu is open, showing 'Mobility Anchors' as the selected option. Other options in the dropdown include 'Remove', '802.11u', 'Foreign Maps', 'Service Advertisements', and 'Hotspot 2.0'.

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)]

將其設定為本地錨點。

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority ¹

3

Foot Notes

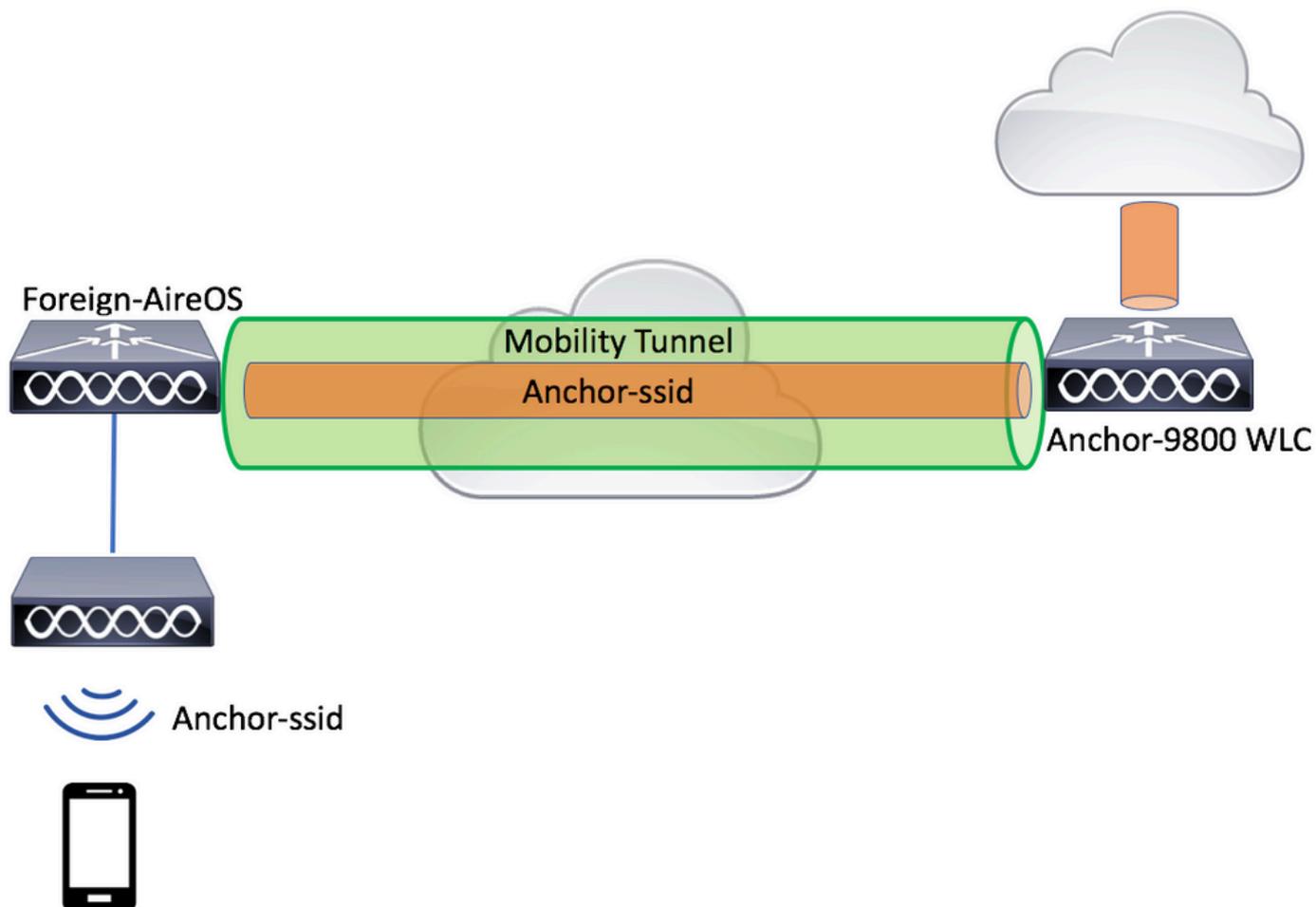
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

在CLI上：

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

外部AireOS — 錨點9800 WLC

帶9800錨點網路圖的AireOS Foreign



使用AireOS錨點配置9800外部

步驟 1. 在外部9800 WLC和錨點AireOS WLC之間建立行動通道。

請參閱以下檔案：[在Catalyst 9800上設定行動化拓撲](#)

步驟 2. 在兩台WLC上建立所需的SSID。

支援的安全方法：

- 未解決
- MAC過濾器
- PSK
- Dot1x
- 本地/外部Web驗證(LWA)
- 中央Web驗證(CWA)



註:AireOS WLC和9800 WLC必須具有相同的配置型別，否則錨點無法正常工作。

步驟 3. 登入9800 WLC (充當錨點) 並建立錨點原則設定檔。

導覽至Configuration > Tags & Profiles > Policy > + Add。確保9800上的原則設定檔名稱與AireOS WLC上的設定檔名稱完全相同，否則無法使用。

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*

anchor-ssid

Description

Enter Description

Status

ENABLED



Passive Client



DISABLED

Encrypted Traffic Analytics



DISABLED

CTS Policy

Inline Tagging



SGACL Enforcement



Default SGT

2-65519

WLAN Switching Policy

Central Switching



Central Authentication



Central DHCP



Central Association



Flex NAT/PAT



Cancel

Save & Apply to Device

導覽至Mobility索引標籤並啟用Export Anchor。這指示9800 WLC是使用該原則設定檔的任何WLAN的錨點9800 WLC。當外部AireOS WLC將使用者端傳送到錨點9800 WLC時，它會通知有關使用者端所指派的WLAN名稱的資訊，因此錨點9800 WLC知道要使用的本地WLAN組態，並且它也會使用此名稱來知道要使用的本地原則設定檔。

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 style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 80%;">Anchor IP</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;"> 172.16.0.5</td> <td style="text-align: center; vertical-align: middle;">→</td> </tr> <tr> <td style="padding: 5px;"> 10.88.173.49</td> <td style="text-align: center; vertical-align: middle;">→</td> </tr> </tbody> </table>	Anchor IP		172.16.0.5	→	10.88.173.49	→	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; border-bottom: 1px solid #ccc;">Anchor IP</th> <th style="width: 50%; border-bottom: 1px solid #ccc;">Anchor Priority</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center; height: 100px; vertical-align: middle;">Anchors not assigned</td> </tr> </tbody> </table>	Anchor IP	Anchor Priority	Anchors not assigned	
Anchor IP											
172.16.0.5	→										
10.88.173.49	→										
Anchor IP	Anchor Priority										
Anchors not assigned											

↶ Cancel

Save & Apply to Device

注意：請確保專門使用此策略配置檔案來接收來自外部控制器的流量。

在CLI上：

```
Anchor 9800 WLC

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

步驟 4.將AireOS WLC配置為外部。

登入到AireOS並導航到WLANs > WLANs。導航到WLAN行末尾的箭頭並選擇Mobility AnchorS。

WLANs

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

將9800 WLC設定為此SSID的錨點。

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).

在CLI上：

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

驗證

可以使用這些命令來檢驗使用外部/錨點SSID的無線客戶端的配置和狀態。

在9800 WLC上驗證

```
# 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>
```

在AireOS WLC上驗證

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

疑難排解

WLC 9800 提供永不間斷的追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別消息均被持續記錄，並且您可在事件或故障條件發生後檢視事件。



注意：根據生成的日誌量，您可以將時間從幾小時縮短到幾天。

若要檢視9800 WLC在預設情況下蒐集的追蹤，可以透過SSH/Telnet連線至9800 WLC，並參考以下步驟。（確保您將會話記錄到文本檔案）

步驟 1. 檢查控制器的當前時間，以便可以跟蹤問題發生時的記錄。

```
# show clock
```

步驟 2. 根據系統配置的指示，從控制器緩衝區或外部系統日誌中收集系統日誌。這樣可以快速檢視系統運行狀況和錯誤（如果有）。

```
# show logging
```

步驟 3. 收集特定MAC或IP地址的「永遠線上」通知級別跟蹤。如果懷疑移動隧道有問題，或者無線客戶端MAC地址，遠端移動對等裝置可以過濾此資訊。

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

步驟 4. 您可顯示作業階段中的內容，或可將檔案複製到外部 TFTP 伺服器。

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

條件式偵錯和無線電主動式追蹤

如果永遠線上(always-on)跟蹤未為您提供足夠的資訊來確定所調查問題的觸發因素，則可以啟用條件調試並捕獲無線活動(RA)跟蹤，該跟蹤為與指定條件（本例中為客戶端mac地址）互動的所有進程提供調試級別跟蹤。要啟用條件調試，請參閱以下步驟。

步驟 5. 確保未啟用調試條件。

```
# clear platform condition all
```

步驟 6. 為要監控的無線客戶端mac地址啟用調試條件。

以下命令會開始監控提供的 MAC 位址 30 分鐘（1800 秒）。您可選擇將此時間增加至

2085978494 秒。

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

 附註：若要同時監控多個用戶端，請針對每個 MAC 位址執行 `debug wireless mac <aaaa.bbbb.cccc>` 指令。

 注意：您看不到終端會話上客戶端活動的輸出，因為所有內容都在內部緩衝，供以後檢視。

步驟 7. 重現您要監控的問題或行為。

步驟 8. 如果在預設或配置的監控器時間開啟之前重現問題，則停止調試。

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

監控時間過後或偵錯無線功能停止後，9800 WLC 會產生具有以下名稱的本地檔案

： `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

步驟 9. 收集 MAC 位址活動的檔案。 可以將 RA 跟蹤複製到 `.log` 外部伺服器，也可以直接在螢幕上顯示輸出。

檢查 RA 追蹤檔案的名稱：

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

將檔案複製到外部伺服器：

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

顯示內容：

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

步驟 10. 如果根本原因仍不明顯，請收集內部日誌，這些日誌是調試級別日誌的更詳細檢視。不需要再次調試客戶端，因為日誌已寫入控制器記憶體中，並且您只需要填充更詳細的日誌檢視。

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

 注意：此命令輸出返回所有進程的所有日誌記錄級別的跟蹤，而且非常大。聯絡Cisco TAC以幫助分析這些跟蹤。

您可以將複製到ra-internal-FILENAME.txt外部伺服器，或者直接在螢幕上顯示輸出。

將檔案複製到外部伺服器：

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

顯示內容：

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

步驟 11. 移除偵錯條件。

```
# clear platform condition all
```

 注意：請確保在故障排除會話後始終刪除調試條件。

驗證AireOS WLC

您可以運行此命令來監控AireOS WLC上無線客戶端的活動。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。