# Configuración de la función de movilidad de anclaje WLAN en Catalyst 9800

# Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Configurar Escenario externo/de anclaje entre 9800 WLC Diagrama de red: dos WLC Catalyst 9800 Configuración de un 9800 Foreign con un 9800 Anchor WLC Foreign 9800: Anchor AireOS Diagrama de red de anclaje de Catalyst 9800 externo - AireOS Configuración de 9800 Foreign con AireOS Anchor Foreign AireOS - Anchor 9800 WLC Diagrama de red de anclaje AireOS Foreign con 9800 Configuración de un Foreign 9800 con un Anchor AireOS Verificación Verifique en el 9800 WLC Verificar en el WLC de AireOS Troubleshoot Depuración condicional y seguimiento activo por radio Verifique el WLC de AireOS

# Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) en un escenario externo/de anclaje con los controladores inalámbricos Catalyst 9800.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso mediante interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) a los controladores inalámbricos
- Movilidad en los controladores de LAN inalámbrica (WLC) de Cisco
- Controladores inalámbricos 9800
- WLC de AireOS

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• AireOS WLC versión 8.8 MR2 (también puede utilizar Inter Release Controller Mobility (IRCM) imágenes especiales 8.5)

- 9800 WLC v16.10 o posterior
- Modelo de configuración de 9800 WLC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configurar

Esta es una función que se utiliza normalmente para escenarios de acceso de invitado, para terminar todo el tráfico de los clientes en un único punto de salida L3, incluso si los clientes provienen de diferentes controladores y ubicaciones físicas. El túnel de movilidad proporciona un mecanismo para mantener el tráfico aislado mientras atraviesa la red.

#### Escenario externo/de anclaje entre 9800 WLC

Este escenario representa los dos Catalyst 9800 utilizados.

#### Diagrama de red: dos WLC Catalyst 9800



Para los escenarios de invitados de movilidad, existen dos funciones principales de controlador:

- Controlador externo: este WLC posee la capa 2 o el lado inalámbrico. Tiene puntos de acceso conectados. Todo el tráfico del cliente para las WLANs ancladas se encapsula en el túnel de movilidad para ser enviado al anclaje. No existe localmente.
- Controlador de anclaje: este es el punto de salida de la capa 3. Recibe los túneles de movilidad de los controladores externos y desencapsula o termina el tráfico del cliente en el punto de salida (VLAN). Este es el punto donde los clientes se ven en la red, por lo tanto el nombre del ancla.

Los puntos de acceso en el WLC externo difunden los SSID de WLAN y tienen una etiqueta de política asignada que enlaza el perfil WLAN con el perfil de política apropiado. Cuando un cliente inalámbrico se conecta a este SSID, el controlador externo envía ambos, el nombre SSID y el perfil de política como parte de la información del cliente al WLC de anclaje. Tras la recepción, el WLC de anclaje verifica su propia configuración para que coincida con el nombre SSID así como el nombre del perfil de política. Una vez que el WLC del ancla encuentra una coincidencia, aplica la configuración que corresponde a él y un punto de salida al cliente inalámbrico. Por lo tanto, es obligatorio que los nombres y las configuraciones de WLAN y

del perfil de política coincidan en el WLC 9800 externo y el WLC 9800 de anclaje con la excepción de VLAN en el perfil de política.

**Nota**: Los nombres del perfil WLAN y del perfil de política pueden coincidir en el 9800 Anchor y el 9800 Foreign WLC.

#### Configuración de un 9800 Foreign con un 9800 Anchor

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor 9800.

Puede consultar este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree el SSID deseado en ambos WLC 9800.

Métodos de seguridad admitidos:

- Abierto
- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)
- Autenticación web central (CWA)

**Nota**: Ambos WLC 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 externo y defina la dirección IP del WLC 9800 de anclaje en el perfil de política.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.

A	dd Policy Profile	1			
	General	Access Policies	QOS and AV	C Mobility	Advanced
		A Configuring in enable	d state will result in los	s of connectivity for clients a	ssociated with this pro
	Name*	ancho	r-policy-profile	WLAN Switchi	ng Policy
	Description	Enter I	Description	Central Switchin	g 🗸
	Status	ENABLE	D	Central Authenti	cation 🖌
	Passive Client		ABLED	Central DHCP	
	Encrypted Traffic	Analytics DIS	ABLED	Central Associat	ion 🗹
	CTS Policy			Flex NAT/PAT	
	Inline Tagging				
	SGACL Enforcem	nent			
	Default SGT	2-655	19		
	Cancel				📄 Save a

En el Mobility, elija la dirección IP del WLC 9800 de anclaje.

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		Anchor IP	Anchor Priority				
172.16.0.5	<b>&gt;</b>	10.88.173.49	Tertiary	•			
Cancel				🖹 Save 8			

Paso 4. Enlace el perfil de política con la WLAN dentro de la etiqueta de política asignada a los AP asociados con el controlador externo que atiende a esta WLAN.

Desplácese hasta Configuration > Tags & Profiles > Tags y crear uno nuevo o utilizar el que existe.

Edit Policy Tag				
Name*	PT1			
Description	Enter Description			
+ Add × Dele	ete			
WLAN Profile		~	Policy Profile	
	10 🔻 items per pag	e		No items to di
Map WLAN and Poli	су			
WLAN Profile*	anchor-ssid 🔻		Policy Profile*	anchor-policy 🔹
		×	×	

Asegúrese de elegir Update & Apply to Device para aplicar los cambios a la etiqueta de directiva.

Ec	lit Policy Tag					
	Name*	PT1				
-	Description	Enter Description				
	+ Add X Dela	ete				
2	WLAN Profile		~	Policy Profile		
	anchor-ssid			anchor-policy		
		10 🔻 items per page	9			1 - 1 of 1 i
-						
	<b>D</b> Cancel				📑 Update a	& Apply to Dev
9						

Paso 5 (opcional). Asigne la etiqueta de política a un AP o verifique que ya la tiene.

 $Despl{a}cese\ hasta\ \ Configuration > Wireless > Access\ Points > AP\ name > General.$ 

# Edit AP

General	Interfaces	High Availability	Inventor	У	Advanced		
AP Name*		karlcisn-AP-30	Pri	imary S	oftware Version	1	8.5.97.110
Location*		default-location	Pr	Predownloaded Status			N/A
Base Radio MAC		000a.ad00.1f00	Pr	edownl	oaded Version	I	N/A
Ethernet MA	C	000a.ad00.1ff0	Ne	ext Retr	y Time	I	N/A
Admin Status	5	Enabled 🔻	Bo	ot Vers	ion	1	8.5.97.110
AP Mode		Local	10	S Versi	on		
Operation St	atus	Registered	Mi	ni IOS \	/ersion	(	0.51.0.3
Fabric Status	3	Disabled		Config	3		
Tags			CA	APWAP	Preferred Mode	Not Co	onfigured
Policy		PT1	St	atic IPv	4 Address	11.11.	0.39
Policy			Static IP (IPv4/IPv6)			$\checkmark$	
Site		<b>ST1</b>	Stat	atic IP (	IPv4/IPv6)	11.11.	0.39
RF		RT1 T	Ne	Netmask		255.25	55.0.0
			Ga	ateway	(IPv4/IPv6)	11.11.	0.1
			DN (IP	NS IP A	ddress	0.0.0.0	)
				Domain Name		Cisco	
			Time Statistics		itistics		
			Up	o Time			3 days ( mins 26
Cancel							🗄 Update 8

**Nota:** Tenga en cuenta que si realiza un cambio en la etiqueta AP después de elegir Update & Apply to Device, el AP reinicia su túnel CAPWAP, por lo que pierde la asociación con el WLC 9800 y luego lo recupera.

Desde la 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
```

Paso 6. Inicie sesión en el WLC del ancla 9800 y cree el perfil de política de anclaje. Asegúrese de que tenga exactamente el mismo nombre que utilizó en los WLC 9800 extranjeros.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.

A	Add Policy Profile						
	General	Access Policies	QOS and	AVC	Mobility	Advance	ed
		A Configuring in ena	abled state will result in	n loss of conn	ectivity for clients associa	ated with th	is pr
Name*		and	chor-policy-profile		WLAN Switching Po	licy	
	Description	Ent	ter Description		Central Switching		$\checkmark$
	Status	ENA	BLED		Central Authentication	n	$\checkmark$
	Passive Client		DISABLED		Central DHCP		V
	Encrypted Traffic	Analytics	DISABLED		Central Association		V
	CTS Policy				Flex NAT/PAT		
	Inline Tagging						
	SGACL Enforcen	nent					
	Default SGT	2-	65519				
	<b>ວ</b> Cancel					📋 Sa	ave

Desplácese hasta Mobility y activar Export Anchor. Esto indica al WLC 9800 que es el WLC 9800 de anclaje para cualquier WLAN que utilice ese perfil de política. Cuando el WLC 9800 extranjero envía los clientes al WLC 9800 de anclaje, informa sobre la WLAN y el perfil de política al que está asignado el cliente, por lo que el WLC 9800 de anclaje sabe qué perfil de política local debe utilizar.

**Nota**: No debe configurar pares de movilidad y anclaje de exportación al mismo tiempo. Se trata de un escenario de configuración no válido.

**Nota**: No debe utilizar el parámetro Export Anchor para ningún perfil de política vinculado a un perfil WLAN en un controlador con puntos de acceso. Esto impide que se transmita el SSID, por lo que esta política debe utilizarse exclusivamente para la funcionalidad de anclaje.

Add Policy Pro	ofile			
General	Access Policies	QOS and AVC	Mobility	Advanced
Mobility Anch	ors			
Export Anchor				
Static IP Mobilit	ty DISABLED			
Adding Mobility Ar disable and may re	nchors will cause the enabled we are the enabled we are the source of connectivity for a source of the source of t	<i>NLANs to momentarily some clients.</i>		
Drag and Drop/de	ouble click/click on the arrow	v to add/remove Anchors		
Available (2)		Selected (0)		
Anchor IP		Anchor IP	Anchor Priority	
172.16.0	).5 <b>&gt;</b>			
10.88.17	3.49 →		Anchors not assigne	d
Cancel				🛛 📋 Save 8
Desde la CLI:				
Anchor 9800 WLC				
<pre># config t # wireless profile # mobility anchor # vlan <vlan-id_vl #="" no="" pre="" shutdown<=""></vlan-id_vl></pre>	e policy <anchor-policy> _AN-name&gt;</anchor-policy>			

# exit

## WLC Foreign 9800: Anchor AireOS

Esta configuración representa el escenario donde un WLC de Catalyst 9800 se utiliza como externo con un

WLC de AireOS Unified utilizado como anclaje.

Diagrama de red de anclaje de Catalyst 9800 externo - AireOS



#### Configuración de 9800 Foreign con AireOS Anchor

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor AireOS.

Consulte este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree las WLAN deseadas en ambos WLC.

Métodos de seguridad admitidos:

• Abierto

- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)
- Autenticación web central (CWA)

**Nota**: Tanto el WLC de AireOS como el WLC de 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 (que actúa como externo) y cree el perfil de política de anclaje.

 $Desplácese\ hasta\ Configuration > {\tt Tags}\ \&\ Profiles > {\tt Policy} > +\ {\tt Add}\ .$ 

Ac	ld Policy Profile							
_	General	Access Policie	es QC	OS and AVC		Mobility	Advan	ced
		A Configuring in	n enabled state wi	ill result in loss c	of conne	ectivity for clients associa	ted with	this prot
	Name*		anchor-policy			WLAN Switching Po	licy	
	Description	[	Enter Description		Central Switching		$\checkmark$	
	Status	(	ENABLED			Central Authentication		$\checkmark$
	Passive Client	(	DISABLED			Central DHCP		$\checkmark$
	Encrypted Traffic	Analytics	DISABLED			Central Association		$\checkmark$
	CTS Policy					Flex NAT/PAT		
	Inline Tagging	C						
	SGACL Enforcem	ent						
	Default SGT	[	2-65519					
	Cancel						ľ	Save &

Desplácese hasta Mobility y elija el WLC AireOS ancla. El WLC 9800 reenvía el tráfico del SSID asociado con este perfil de política al anclaje elegido.

Add Policy Profile	•			
General	Access Policies	QOS and AVC	Mobility	Advanced
Mobility Anchors				
Export Anchor				
Static IP Mobility	DISABLED			
Adding Mobility Ancho disable and may result	rs will cause the enabled V in loss of connectivity for s	VLANs to momentarily some clients.		
Drag and Drop/doubl	e click/click on the arrow	to add/remove Anchors	5	
Available (0)		Selected (1)		
Anchor IP		Anchor IP	Anchor Prior	rity
		10.88.173.105	5 Т	ertiary 🔻
No anchor	s available			
Cancel				📋 Save 8

Paso 4. Enlace el perfil de política con la WLAN dentro de la etiqueta de política asignada a los AP asociados con el controlador externo que atiende a esta WLAN.

Desplácese hasta Configuration > Tags & Profiles > Tags y crear uno nuevo o utilizar el que existe.

Edi	it Policy Tag				
N	lame*	PT1			
D	Description	Enter Description			
E	+ Add X Dele	te			
	WLAN Profile		$\sim$	Policy Profile	
H	● ● ●	10 🔹 items per page			No items to d
Ma	ap WLAN and Poli	су			
M	VLAN Profile*	anchor-ssid 🔻		Policy Profile*	anchor-policy 🔹
			×	~	

Asegúrese de elegir Update & Apply to Device para aplicar los cambios a la etiqueta de directiva.

I	Edit Policy Tag				
	Name*	PT1			
	Description	Enter Description			
	+ Add X Del	ete			
	WLAN Profile		~	Policy Profile	
	anchor-ssid			anchor-policy	
		10 🔻 items per page	)		1 - 1 of 1 i
-					
	5 Cancel				& Apply to Dev

Paso 5 (opcional). Asigne el sitio a un AP o verifique que ya lo tiene.

 $Despl{a}cese\ hasta\ \ Configuration > Wireless > Access\ Points > AP\ name > General.$ 

# Edit AP

General	Interfaces	High Availability	Inventor	У	Advanced		
AP Name*		karlcisn-AP-30	Pri	imary S	oftware Version	:	8.5.97.110
Location*		default-location	Pr	Predownloaded Status		N/A	
Base Radio N	MAC	000a.ad00.1f00	Pr	edownl	oaded Version	I	N/A
Ethernet MA	C	000a.ad00.1ff0	Ne	ext Retr	y Time	l	N/A
Admin Status	5	Enabled 🔻	Bo	ot Vers	ion	1	8.5.97.110
AP Mode		Local	10	S Versi	on		
Operation St	atus	Registered	Mi	ni IOS \	/ersion		0.51.0.3
Fabric Status	3	Disabled	IP	Config	3		
Tags			CA	APWAP	Preferred Mode	Not Co	onfigured
Policy		PT1	St	atic IPv	4 Address	11.11.	.0.39
Policy			St	atic IP (	IPv4/IPv6)	$\checkmark$	
Site		<b>ST1</b>	St	atic IP (	IPv4/IPv6)	11.11.	0.39
RF		RT1 T	Ne	etmask		255.25	55.0.0
			Ga	ateway	(IPv4/IPv6)	11.11.	0.1
			DN (IP	NS IP A	ddress	0.0.0.0	)
			Do	omain N	lame	Cisco	
			Ti	me Sta	itistics		
			Up	o Time			3 days ( mins 26
Cancel							🗄 Update 8

**Nota**: Tenga en cuenta que si realiza un cambio en la etiqueta AP después de elegir Update & Apply to Device, el AP reinicia su túnel CAPWAP, por lo que pierde la asociación con el WLC 9800 y luego lo recupera.

Desde la 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
```

Paso 6. Configure el WLC de AireOS como el ancla.

Inicie sesión en AireOS y navegue hasta WLANs > WLANs. Elija la flecha al extremo derecho de la fila WLAN para navegar al menú desplegable y elegir Mobility Anchors.

cisco		<u>W</u> LANs Q	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDB
WLANs	WLANs								
WLANS WLANS	Current Filte	None	(Cha	ange Filter) (Cle	ear Filter]				Create Ne
Advanced		Type	Profile Nat	me	w	AN SSTD		Admin	Status (
		WLAN	6					Enabled	[] [
	2	Remote LA	N 5200000			-		Enabled	1
	3	WLAN	·		10			Enabled	
	<b>4</b>	Remote LA	N 20200			-		Disabled	t
	<u>5</u>	WLAN	anchor-ssid		ar	nchor-ssid		Disabled	1 [

Ajústelo como delimitador local.

MONITOR	<u>W</u> LANs	CONTROLLER	W <u>I</u> RELESS	SECURITY	M <u>A</u> NAG
Mobility A	nchors				
WLAN SSI	and and	chor-ssid			
Switch IP /	Address (/	Anchor)			
Mobility A	nchor Cre	ate			-
Switch IP	Address	(Anchor)	local	\$	
Priority <sup>1</sup>			3 🖨		
Foot Note	s				
1. Priority nu	mber, 1=H	lighest priority and	1 3=Lowest prio	rity(default).	

Desde la CLI:

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

## Foreign AireOS - Anchor 9800 WLC

Diagrama de red de anclaje AireOS Foreign con 9800



#### Configuración de un Foreign 9800 con un Anchor AireOS

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor AireOS.

Puede consultar este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree el SSID deseado en ambos WLC.

Métodos de seguridad admitidos:

- Abierto
- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)

• Autenticación web central (CWA)

**Nota**: Tanto el WLC de AireOS como el WLC de 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 (que actúa como anclaje) y cree el perfil de política de anclaje.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.Asegúrese de que el nombre del perfil de política en 9800 sea exactamente el mismo nombre que el nombre del perfil en el WLC de AireOS; de lo contrario, no funcionará.

Ad	d Policy Profile				
_	General A	Access Policies	QOS and AV	C Mobility	Advanced
	4	Configuring in enable	ed state will result in lo	ss of connectivity for clier	nts associated with this pro
	Name*	ancho	r-ssid	WLAN Swit	ching Policy
	Description	Enter	Description	Central Swit	ching 🗹
	Status	ENABLE	D	Central Auth	entication 🖌
	Passive Client		ABLED	Central DHC	P 🗹
	Encrypted Traffic Ar	nalytics DIS	ABLED	Central Asso	ciation 🖌
	CTS Policy			Flex NAT/PA	T 🗌
	Inline Tagging				
	SGACL Enforcemen	nt 🗌			
	Default SGT	2-655	;19		
	<b>D</b> Cancel				Save 8

Desplácese hasta Mobility y activar Export Anchor. Esto indica al WLC 9800 que es el WLC 9800 de anclaje para cualquier WLAN que utilice ese perfil de política. Cuando el WLC de AireOS externo envía los clientes al WLC de anclaje 9800, informa sobre el nombre WLAN al que está asignado el cliente, de modo que el WLC de anclaje 9800 sabe qué configuración WLAN local debe utilizar y también utiliza este nombre para saber qué perfil de política local debe utilizar.

Add Policy Profile	•					
General	Access Policies	QOS and AVC	Mobil	ity	Advanced	
Mobility Anchors						
Export Anchor						
Static IP Mobility	DISABLED					
Adding Mobility Ancho disable and may result	ors will cause the enabled t in loss of connectivity for	NLANs to momentarily some clients.				
Drag and Drop/doubl	le click/click on the arrov	v to add/remove Ancho	ors			
Available (2)		Selected (0)				
Anchor IP		Anchor IP	Anchor	Priority		
172.16.0.5	÷					
10.88.173.4	9 <b>&gt;</b>	Anchors not assigned				
Cancel					📄 Save 8	

**Nota**: Asegúrese de utilizar este perfil de política exclusivamente para recibir tráfico de controladores externos.

Desde la CLI:

Anchor 9800 WLC
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id\_VLAN-name>
# no shutdown
# exit

Paso 4. Configure el WLC de AireOS como externo.

uluili. cisco		<u>W</u> LANs <u>C</u> C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDB
WLANs	WLANs								
WLANS WLANS	Current Filte	r: None	[Cha	ange Filter) (Cle	ear Filter]				Create Ne
Advanced	WLAN ID	Туре	Profile Nar	ne	w	LAN SSID		Admin	Status \$
		WLAN	6 <sup></sup> :		19	· · · · · · · · ·		Enabled	
	□ <u>2</u>	Remote LAN	4 Sporter 200			-		Enabled	. P
	<u>3</u>	WLAN	·		15			Enabled	(
	<u>4</u>	Remote LAN	4 202200			-		Disabled	đ
	<u>5</u>	WLAN	anchor-ssid		a	nchor-ssid		Disabled	d [

Establezca el WLC 9800 como un ancla para este SSID.

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	M <u>A</u> NAGEM					
Mobility Anchors										
WLAN SSI	D and	chor-ssid								
Switch IP	Address (/	Anchor)								
Mobility A	Mobility Anchor Create									
Switch IP	Address	(Anchor)	10.88.17	73.105 🗘						
Priority <sup>1</sup>			3 \$							
Foot Note	S									

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

Desde la CLI:

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

## Verificación

Puede utilizar estos comandos para verificar la configuración y el estado de los clientes inalámbricos con el uso de un SSID externo/de anclaje.

#### Verifique en el 9800 WLC

# 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>

#### Verificar en el WLC de AireOS

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

## Troubleshoot

El WLC 9800 ofrece capacidades de seguimiento SIEMPRE ACTIVAS. Esto garantiza que todos los errores, advertencias y mensajes de nivel de notificación relacionados con la conectividad del cliente se registren constantemente y que pueda ver los eventos de una condición de incidente o error después de que se haya producido.

Nota: Dependiendo del volumen de registros generados, puede retroceder unas horas a varios días.

Para ver los seguimientos que 9800 WLC recolectó por defecto, puede conectarse vía SSH/Telnet al 9800 WLC y consultar estos pasos. (Asegúrese de registrar la sesión en un archivo de texto)

Paso 1. Compruebe la hora actual del controlador para poder realizar un seguimiento de los registros en el tiempo hasta el momento en que ocurrió el problema.

# show clock

Paso 2. Recopile los syslogs del buffer del controlador o del syslog externo según lo dicte la configuración del sistema. Esto proporciona una vista rápida del estado del sistema y de los errores, si los hubiera.

# show logging

Paso 3. Recopile los seguimientos del nivel de aviso siempre activo para la dirección MAC o IP específica. El par de movilidad remota puede filtrar esto, si sospecha un problema de túnel de movilidad, o por dirección MAC del cliente inalámbrico.

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

Paso 4. Puede mostrar el contenido de la sesión o copiar el archivo en un servidor TFTP externo.

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

#### Depuración condicional y seguimiento activo por radio

Si los seguimientos siempre activos no proporcionan suficiente información para determinar el desencadenador del problema que se está investigando, puede habilitar la depuración condicional y capturar seguimientos de Radio Active (RA), que proporciona seguimientos de nivel de depuración para todos los procesos que interactúan con la condición especificada (dirección MAC del cliente en este caso). Para habilitar la depuración condicional, consulte estos pasos.

Paso 5. Asegúrese de que no hay condiciones de depuración habilitadas.

Paso 6. Habilite la condición de depuración para la dirección MAC del cliente inalámbrico que desea monitorear.

Estos comandos comienzan a monitorear la dirección MAC proporcionada durante 30 minutos (1800 segundos). Opcionalmente, puede aumentar este tiempo hasta 2 085 978 494 segundos.

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

**Nota**: Para monitorear más de un cliente a la vez, ejecute el comando debug wireless mac<aaaa.bbbb.cccc> por dirección MAC.

**Nota**: Usted no ve el resultado de la actividad del cliente en la sesión de terminal, ya que todo se almacena en buffer internamente para ser visto más tarde.

Paso 7. Reproduzca el problema o el comportamiento que desea monitorear.

Paso 8. Detenga las depuraciones si el problema se reproduce antes de que se agote el tiempo de monitoreo predeterminado o configurado.

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

Una vez que ha transcurrido el tiempo del monitor o se ha detenido el debug wireless, el WLC 9800 genera un archivo local con el nombre: ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log

Paso 9. Recopile el archivo de la actividad de la dirección MAC. Puede copiar el seguimiento de RA .log a un servidor externo o muestre el resultado directamente en la pantalla.

Verifique el nombre del archivo de seguimiento activo por radio:

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

Copie el archivo en un servidor externo:

# copy bootflash:ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log tftp://a.b.c.d

Muestre el contenido:

# more bootflash:ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log

Paso 10. Si la causa raíz aún no es obvia, recopile los registros internos que son una vista más detallada de los registros de nivel de depuración. No es necesario depurar el cliente de nuevo, ya que los registros ya se escribieron en la memoria del controlador y sólo es necesario rellenar una vista más detallada de ellos.

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

**Nota**: Esta salida de comando devuelve seguimientos para todos los niveles de registro para todos los procesos y es bastante voluminosa. Póngase en contacto con el TAC de Cisco para analizar estos seguimientos.

Puede copiar el archivo ra-internal-FILENAME.txt a un servidor externo o muestre el resultado directamente en la pantalla.

Copie el archivo en un servidor externo:

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

Muestre el contenido:

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

Paso 11. Elimine las condiciones de depuración.

**Nota**: Asegúrese de eliminar siempre las condiciones de depuración después de una sesión de troubleshooting.

## Verifique el WLC de AireOS

Puede ejecutar este comando para monitorear la actividad de un cliente inalámbrico en un WLC de AireOS.

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

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).