

Configurar o recurso de mobilidade de âncora de WLAN no Catalyst 9800

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Componentes Utilizados](#)
- [Configurar](#)
- [Cenário externo/âncora entre 9800 WLCs](#)
- [Diagrama de rede: duas WLCs Catalyst 9800](#)
- [Configurar um 9800 externo com uma âncora 9800](#)
- [WLC 9800 estrangeira - AireOS âncora](#)
- [Catalyst 9800 Externo - Diagrama de Rede de Âncora AireOS](#)
- [Configure 9800 Foreign com âncora AireOS](#)
- [Foreign AireOS - WLC Anchor 9800](#)
- [AireOS Foreign com diagrama de rede de âncora 9800](#)
- [Configure um 9800 Foreign com uma âncora AireOS](#)
- [Verificação](#)
- [Verifique na WLC 9800](#)
- [Verificar no AireOS WLC](#)
- [Troubleshoot](#)
- [Depuração condicional e rastreamento radioativo](#)
- [Verificar o AireOS WLC](#)

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) em um cenário externo/âncora com controladores sem fio Catalyst 9800.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) ou à interface gráfica de usuário (GUI) dos controladores sem fio
- Mobilidade nas controladoras Cisco Wireless LAN (WLCs)
- Controladores sem fio 9800
- WLCs AireOS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AireOS WLC versão 8.8 MR2 (você também pode usar as imagens especiais 8.5 do Inter Release Controller Mobility (IRCM))

- 9800 WLC v16.10 ou posterior
- Modelo de configuração da WLC 9800

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

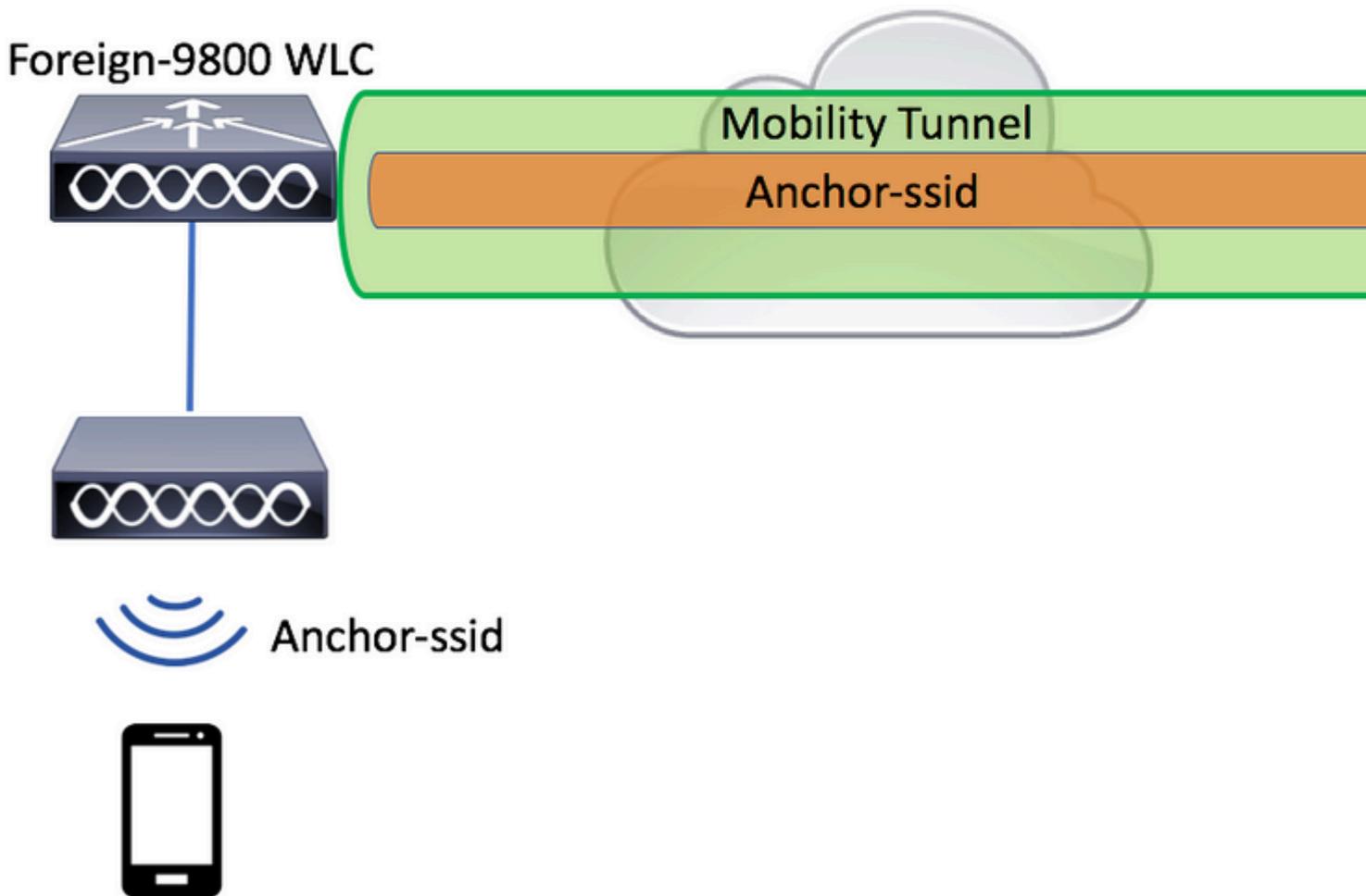
Configurar

Esse é um recurso normalmente usado para cenários de acesso de convidado, para encerrar todo o tráfego dos clientes em um único ponto de saída L3, mesmo que os clientes venham de diferentes controladores e locais físicos. O túnel de mobilidade fornece um mecanismo para manter o tráfego isolado, à medida que atravessa a rede.

Cenário externo/âncora entre 9800 WLCs

Este cenário descreve os dois Catalyst 9800s usados.

Diagrama de rede: duas WLCs Catalyst 9800



Para cenários de convidados de mobilidade, há duas funções principais de controlador:

- Controlador externo: este WLC possui a camada 2 ou o lado sem fio. Ele tem pontos de acesso conectados a ele. Todo o tráfego do cliente para as WLANs ancoradas é encapsulado no túnel de mobilidade a ser enviado à âncora. Ele não existe localmente.
- Controlador de âncora: este é o ponto de saída da camada 3. Ele recebe os túneis de mobilidade dos controladores externos e desencapsula ou encerra o tráfego do cliente no ponto de saída (VLAN). Esse é o ponto onde os clientes são vistos na rede, portanto, o nome da âncora.

Os pontos de acesso na WLC externa transmitem os SSIDs da WLAN e têm uma marca de política atribuída que vincula o perfil da WLAN ao perfil de política apropriado. Quando um cliente sem fio se conecta a esse SSID, o controlador externo envia o nome do SSID e o perfil de política como parte das informações do cliente para o WLC âncora. Após o recebimento, a WLC âncora verifica sua própria configuração para corresponder ao nome SSID, bem como ao nome do Perfil de política. Uma vez que a WLC âncora encontra uma correspondência, ela aplica a configuração que corresponde a ela e um ponto de saída para o cliente sem fio. Portanto, é obrigatório que os nomes e as configurações da WLAN e do perfil de política

correspondam tanto na WLC 9800 externa quanto na WLC 9800 âncora, com exceção da VLAN no perfil de política.

Observação: os nomes do Perfil de WLAN e do Perfil de Política podem ser correspondentes em ambas as WLCs 9800 Anchor e 9800 Foreign.

Configurar um 9800 externo com uma âncora 9800

Etapa 1. Construa um túnel de mobilidade entre a WLC 9800 externa e a WLC 9800 âncora.

Você pode consultar este documento: [Configurando topologias de mobilidade no Catalyst 9800](#)

Etapa 2. Crie o SSID desejado em ambas as 9800 WLCs.

Métodos de segurança suportados:

- Abrir
- filtro MAC
- PSK
- Ponto1x
- Autenticação da Web Local/Externa (LWA)
- Autenticação da Web Central (CWA)

Observação: ambas as WLCs 9800 devem ter o mesmo tipo de configuração, caso contrário, a âncora não funciona.

Etapa 3. Faça login na WLC 9800 externa e defina o endereço IP da WLC 9800 âncora no perfil de política.

Navegue até 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*

anchor-policy-profile

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

Na guia Mobility selecione o endereço IP da WLC âncora 9800.

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)

Anchor IP

 172.16.0.5	→
---	---

Selected (1)

Anchor IP

Anchor Priority

 10.88.173.49	Tertiary ...
---	--------------

Cancel

Save &

Etapa 4. Vincule o Policy Profile com a WLAN dentro da Policy Tag atribuída aos APs associados ao controlador externo que serve esta WLAN.

Navegue até Configuration > Tags & Profiles > Tags e criar um novo ou usar o existente.

Edit Policy Tag

Name*

Description

+ Add

WLAN Profile Policy Profile

◀ 0 ▶ 10 items per page No items to display

Map WLAN and Policy

WLAN Profile* Policy Profile*

Certifique-se de escolher **Update & Apply to Device** para aplicar as alterações à tag de política.

Edit Policy Tag

Name*

Description

+ Add

WLAN Profile Policy Profile

anchor-ssid anchor-policy

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

Etapa 5 (opcional). Atribua a etiqueta de política a um AP ou verifique se ele já a tem.

Navegue até [Configuration](#) > [Wireless](#) > [Access Points](#) > [AP name](#) > [General](#).

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>
Location*	<input type="text" value="default-location"/>
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	<input type="text" value="Enabled"/>
AP Mode	<input type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled

Tags

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

Primary Software Version	8.5.97.110
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	8.5.97.110
IOS Version	
Mini IOS Version	0.51.0.3

IP Config

CAPWAP Preferred Mode	Not Configured
Static IPv4 Address	<input type="text" value="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 mins 26
---------	------------------

 Cancel

 Update &

Note: Lembre-se de que, se você realizar uma alteração na tag AP após escolher `Update & Apply to Device`, o AP reinicia seu CAPWAP de túnel, de modo que ele perde a associação com a WLC 9800 e, em seguida, a recupera.

Na 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
```

Etapa 6. Faça login na WLC âncora 9800 e crie o perfil de política âncora. Certifique-se de que ele tenha exatamente o mesmo nome que você usou nas WLCs 9800 estrangeiras.

Navegue até `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 type="checkbox" value="ENABLED"/>	Central Authentication <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox" value="DISABLED"/>	Central DHCP <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox" value="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"/>	

Navegue até **Mobility** e ativar **Export Anchor**. Isso instrui a WLC 9800 de que ela é a WLC âncora 9800 de qualquer WLAN que use esse Perfil de política. Quando a WLC 9800 externa envia os clientes para a WLC 9800 âncora, ela informa sobre a WLAN e o perfil de política ao qual o cliente está atribuído, para que a WLC 9800 âncora saiba qual perfil de política local usar.

Observação: você não deve configurar pares de mobilidade e exportar âncora ao mesmo tempo. Esse é um cenário de configuração inválido.

Observação: você não deve usar a configuração **Export Anchor** para nenhum perfil de política vinculado a um perfil de WLAN em uma controladora com pontos de acesso. Isso impede que o SSID seja transmitido, portanto, essa política deve ser usada exclusivamente para a funcionalidade **Âncora**.

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 →		

Na CLI:

```
Anchor 9800 WLC

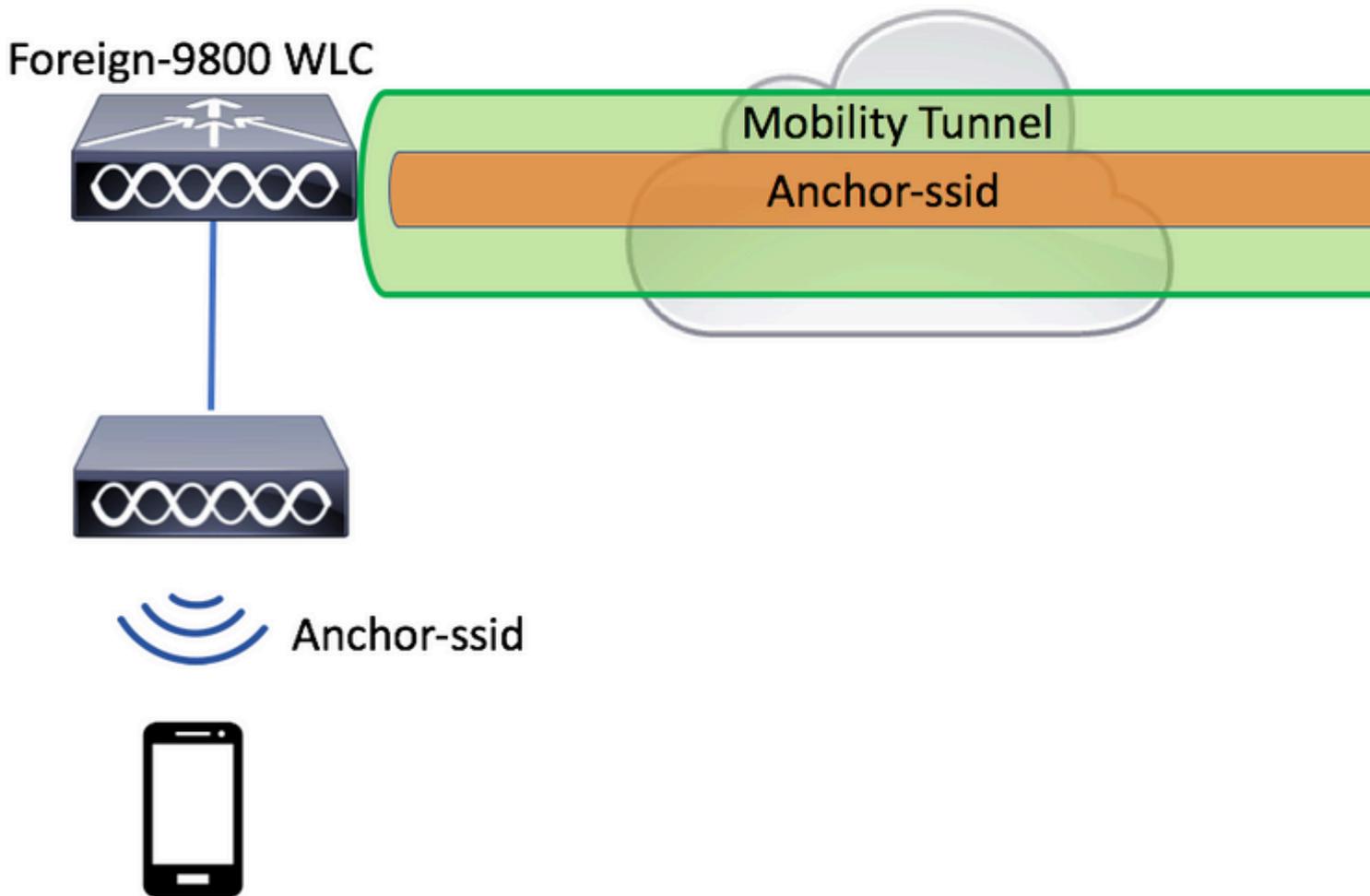
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

WLC 9800 estrangeira - AireOS âncora

Esta configuração descreve o cenário em que uma WLC Catalyst 9800 é usada como estrangeira com uma

WLC AireOS Unified usada como âncora.

Catalyst 9800 Externo - Diagrama de Rede de Âncora AireOS



Configure 9800 Foreign com âncora AireOS

Etapa 1. Construa um túnel de mobilidade entre a WLC 9800 estrangeira e a WLC AireOS âncora.

Consulte este documento: [Configurando topologias de mobilidade no Catalyst 9800](#)

Etapa 2. Crie as WLANs desejadas em ambas as WLCs.

Métodos de segurança suportados:

- Abrir

- filtro MAC
- PSK
- Ponto1x
- Autenticação da Web Local/Externa (LWA)
- Autenticação da Web Central (CWA)

Observação: tanto a WLC AireOS quanto a WLC 9800 devem ter o mesmo tipo de configuração, caso contrário, a âncora não funciona.

Etapa 3. Faça login na WLC 9800 (que atua como externa) e crie o perfil de política âncora.

Navegue até 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 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"/>	

Navegue até Mobility e escolha a âncora AireOS WLC. A WLC 9800 encaminha o tráfego do SSID associado a esse perfil de política para a âncora escolhida.

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)				
<p>Anchor IP</p> <div>No anchors available</div>	<table><thead><tr><th>Anchor IP</th><th>Anchor Priority</th></tr></thead><tbody><tr><td> 10.88.173.105</td><td>Tertiary ... ▼</td></tr></tbody></table>	Anchor IP	Anchor Priority	 10.88.173.105	Tertiary ... ▼
Anchor IP	Anchor Priority				
 10.88.173.105	Tertiary ... ▼				

Etapa 4. Vincule o Policy Profile com a WLAN dentro da Policy Tag atribuída aos APs associados ao controlador externo que serve esta WLAN.

Navegue até Configuration > Tags & Profiles > Tags e criar um novo ou usar o existente.

Edit Policy Tag

Name*

Description

+ Add

WLAN Profile	Policy Profile
<input type="button" value="x"/> <input type="button" value="✓"/>	

Map WLAN and Policy

WLAN Profile* Policy Profile*

Certifique-se de escolher **Update & Apply to Device** para aplicar as alterações à tag de política.

Edit Policy Tag

Name*

Description

+ Add

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

Update & Apply to Device

Etapa 5 (opcional). Atribua o site a um AP ou verifique se ele já o tem.

Navegue até [Configuration](#) > [Wireless](#) > [Access Points](#) > [AP name](#) > [General](#).

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	<input type="text" value="karlcisn-AP-30"/>
Location*	<input type="text" value="default-location"/>
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	<input type="text" value="Enabled"/>
AP Mode	<input type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled

Tags

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

Primary Software Version	8.5.97.110
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	8.5.97.110
IOS Version	
Mini IOS Version	0.51.0.3

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
mins 26

 Cancel

 Update &

Observação: lembre-se de que, se você realizar uma alteração na tag AP depois de escolher `Update & Apply to Device`, o AP reinicia seu CAPWAP de túnel, de modo que ele perde a associação com a WLC 9800 e, em seguida, a recupera.

Na CLI:

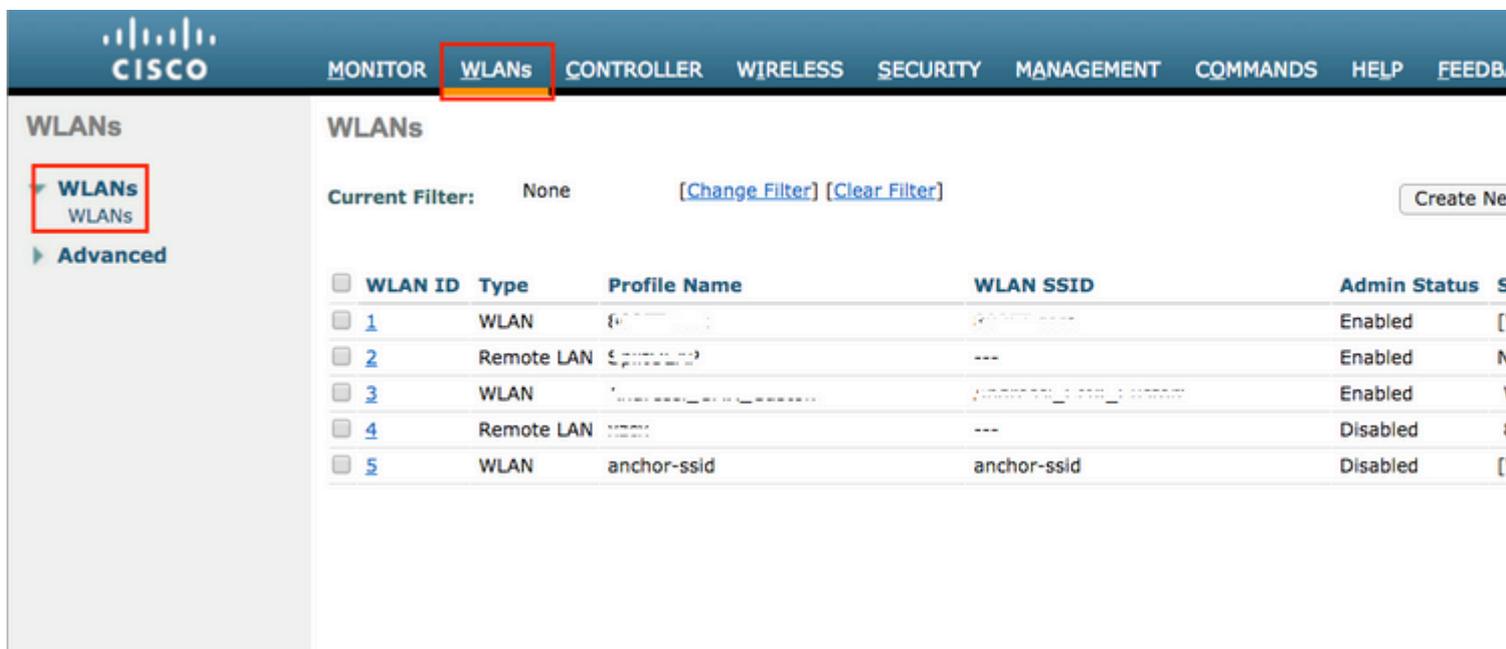
```
# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

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

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

Etapa 6. Configure o AireOS WLC como a âncora.

Inicie sessão no AireOS e navegue até `WLANs > WLANs`. Escolha a seta à direita da linha WLAN para navegar até o menu suspenso e escolha `Mobility Anchors`.



The screenshot displays the Cisco AireOS WLC GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu item is highlighted with a red box. The left sidebar shows 'WLANs' and 'Advanced' options, with 'WLANs' also highlighted. The main content area is titled 'WLANs' and shows a table of WLAN configurations. The table has columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', and 'Admin Status'. The current filter is 'None'. There are links for '[Change Filter]' and '[Clear Filter]'. A 'Create New' button is visible in the top right corner. The table contains five rows of WLAN configurations:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN	Enabled
2	Remote LAN	...	---	Enabled
3	WLAN	Enabled
4	Remote LAN	...	---	Disabled
5	WLAN	anchor-ssid	anchor-ssid	Disabled

Defina-o como a âncora local.

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority ¹

3

Foot Notes

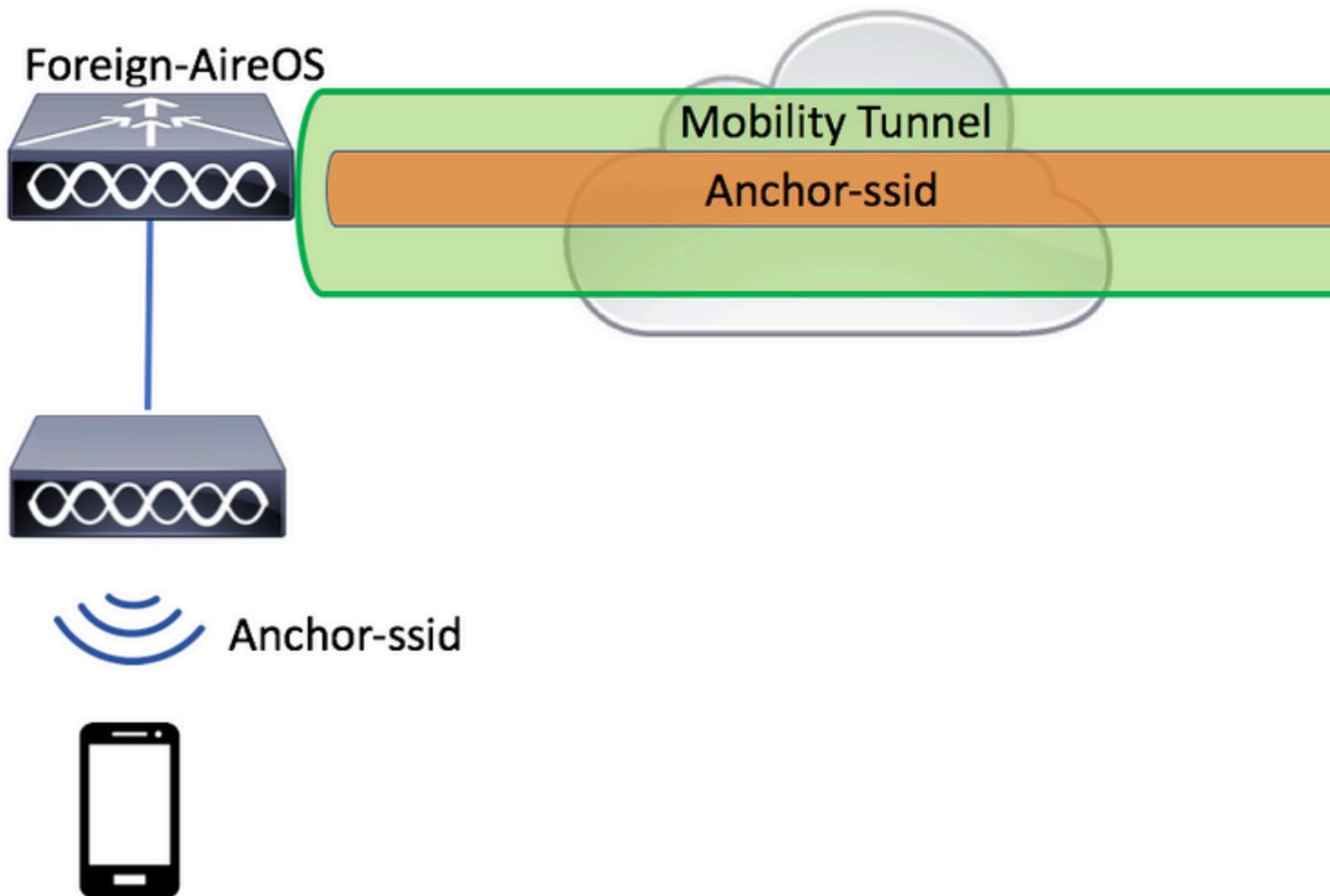
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Na 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 - WLC Anchor 9800

AireOS Foreign com diagrama de rede de âncora 9800



Configure um 9800 Foreign com uma âncora AireOS

Etapa 1. Construa um túnel de mobilidade entre a WLC 9800 estrangeira e a WLC AireOS âncora.

Você pode consultar este documento: [Configurando topologias de mobilidade no Catalyst 9800](#)

Etapa 2. Crie o SSID desejado em ambas as WLCs.

Métodos de segurança suportados:

- Abrir
- filtro MAC
- PSK
- Ponto1x
- Autenticação da Web Local/Externa (LWA)

- Autenticação da Web Central (CWA)

Observação: tanto a WLC AireOS quanto a WLC 9800 devem ter o mesmo tipo de configuração, caso contrário, a âncora não funciona.

Etapa 3. Faça login na WLC 9800 (que atua como uma âncora) e crie o perfil de política de âncora.

Navegue até [Configuration > Tags & Profiles > Policy > + Add](#) Certifique-se de que o nome do Perfil de política no 9800 seja exatamente o mesmo nome do Nome do perfil no AireOS WLC, caso contrário, ele não funcionará.

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 &

Navegue até [Mobility](#) e ativar [Export Anchor](#). Isso instrui a WLC 9800 de que ela é a WLC âncora 9800 de qualquer WLAN que use esse Perfil de política. Quando a WLC AireOS externa envia os clientes para a WLC âncora 9800, ela informa sobre o nome da WLAN ao qual o cliente está atribuído, para que a WLC âncora 9800 saiba qual configuração de WLAN local usar e também usa esse nome para saber qual Perfil de política local usar.

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



10.88.173.49



Anchors not assigned

Cancel



Save &

Observação: use este perfil de política exclusivamente para receber tráfego de controladores externos.

Na CLI:

Anchor 9800 WLC

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

Etapa 4. Configure o AireOS WLC como externo.

Inicie sessão no AireOS e navegue até WLANs > WLANs. Navegue até a seta abaixo ao final da linha WLAN e escolha Mobility AnchorS .

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
1	WLAN			Enabled
2	Remote LAN		---	Enabled
3	WLAN			Enabled
4	Remote LAN		---	Disabled
5	WLAN	anchor-ssid	anchor-ssid	Disabled

Defina a WLC 9800 como uma âncora para este SSID.

WLAN SSID anchor-ssid

Switch IP Address (Anchor) 10.88.173.105

Priority 3

Mobility Anchor Create

Foot Notes

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

Na CLI:

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

Verificação

Você pode usar esses comandos para verificar a configuração e o estado dos clientes sem fio com o uso de um SSID estrangeiro/âncora.

Verifique na 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>
```

Verificar no AireOS WLC

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

Troubleshoot

O WLC 9800 fornece recursos de rastreamento sempre conectados. Isso garante que todos os erros, avisos e mensagens de nível de aviso relacionados à conectividade do cliente sejam registrados constantemente e que você possa exibir eventos de uma condição de incidente ou falha após sua ocorrência.

Observação: Dependendo do volume de logs gerados, você pode voltar de algumas horas a vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e consultar essas etapas. (Certifique-se de registrar a sessão em um arquivo de texto)

Etapa 1. Verifique a hora atual do controlador para que você possa controlar os registros no tempo de volta para quando o problema ocorreu.

```
# show clock
```

Etapa 2. Colete syslogs do buffer do controlador ou do syslog externo conforme a configuração do sistema. Isso fornece uma visão rápida da integridade do sistema e dos erros, se houver.

```
# show logging
```

Etapa 3. Colete os rastreamentos de nível de aviso sempre ativo para o endereço MAC ou IP específico. O peer de mobilidade remota pode filtrar isso, se você suspeitar de um problema no túnel de mobilidade, ou pelo endereço mac do cliente sem fio.

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

Etapa 4. Você pode exibir o conteúdo da sessão ou copiar o arquivo para um 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>
```

Depuração condicional e rastreamento radioativo

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar rastreamentos de Radio Ative (RA), que fornecem rastreamentos em nível de depuração para todos os processos que interagem com a condição especificada (endereço MAC do cliente, neste caso). Para habilitar a depuração condicional, consulte estas etapas.

Etapa 5. Verifique se não há condições de depuração habilitadas.

```
# clear platform condition all
```

Etapa 6. Ative a condição de depuração para o endereço MAC do cliente sem fio que você deseja monitorar.

Estes comandos começam a monitorar o endereço MAC fornecido por 30 minutos (1.800 segundos). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 segundos.

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

Observação: para monitorar mais de um cliente de cada vez, execute o comando `debug wireless mac<aaaa.bbbb.cccc>` por endereço MAC.

Observação: você não vê a saída da atividade do cliente na sessão do terminal, pois tudo é armazenado em buffer internamente para ser visualizado posteriormente.

Passo 7. Reproduza o problema ou comportamento que você deseja monitorar.

Etapa 8. Interrompa as depurações se o problema for reproduzido antes que o tempo de monitoramento padrão ou configurado acabe.

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

Quando o tempo do monitor tiver decorrido ou a depuração sem fio tiver sido interrompida, a WLC 9800 gerará um arquivo local com o nome: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Etapa 9. Colete o arquivo da atividade do endereço MAC. Você pode copiar o rastreamento do RA `.log` a um servidor externo ou exibir a saída diretamente na tela.

Verifique o nome do arquivo de rastreamentos de RA:

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

Copie o arquivo para um servidor externo:

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

Mostre o conteúdo:

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

Etapa 10. Se a causa raiz ainda não for óbvia, colete os logs internos, que são uma visualização mais detalhada dos logs de depuração. Não é necessário depurar o cliente novamente, pois os logs já foram gravados na memória do controlador e você só precisa preencher uma exibição mais detalhada deles.

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

Observação: a saída desse comando retorna rastros para todos os níveis de registro de todos os processos e é bastante volumosa. Envolve o Cisco TAC para ajudar a analisar esses rastreamentos.

Você pode copiar o ra-internal-FILENAME.txt a um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

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

Mostre o conteúdo:

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

Etapa 11. Remova as condições de depuração.

```
# clear platform condition all
```

Observação: certifique-se de sempre remover as condições de depuração após uma sessão de

Verificar o AireOS WLC

Você pode executar este comando para monitorar a atividade de um cliente sem fio em uma WLC AireOS.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.