

WLAN-ankermobiliteit op Catalyst 9800 configureren

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Configureren](#)
- [Buitenlands/ankerscenario tussen 9800 WLC's](#)
- [Netwerkdigram: twee Catalyst 9800 WLC's](#)
- [Een 9800 Foreign configureren met een 9800 anker](#)
- [Foreign 9800 WLC - anker AireOS](#)
- [Catalyst 9800 buitenlands netwerkdigram - AireOS anker](#)
- [Configureer 9800 Foreign met AireOS-anker](#)
- [Foreign AireOS - anker 9800 WLC](#)
- [AireOS Foreign met 9800 ankernetwerkdigram](#)
- [Een 9800 Foreign configureren met een AireOS-anker](#)
- [Verificatie](#)
- [Controleer de 9800 WLC](#)
- [Controleer de AireOS WLC](#)
- [Problemen oplossen](#)
- [Voorwaardelijke debuging en radio actieve tracement](#)
- [Controleer de AireOS WLC](#)

Inleiding

Dit document beschrijft hoe u een Wireless Local Area Network (WLAN) kunt configureren op een buitenlands/ankerscenario met Catalyst 9800 draadloze controllers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de draadloze controllers via Command Line Interface (CLI) of Graphic User Interface (GUI)
- Mobility Express op Cisco draadloze LAN-controllers (WLC's)
- 9800 draadloze controllers
- Aire OS WLC's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AireOS WLC versie 8.8 MR2 (u kunt ook gebruik maken van Inter Release Controller Mobility (IRCM) speciale 8.5 beelden)

- 9800 WLC v16.10 of hoger
- 9800 WLC-configuratiemodel

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

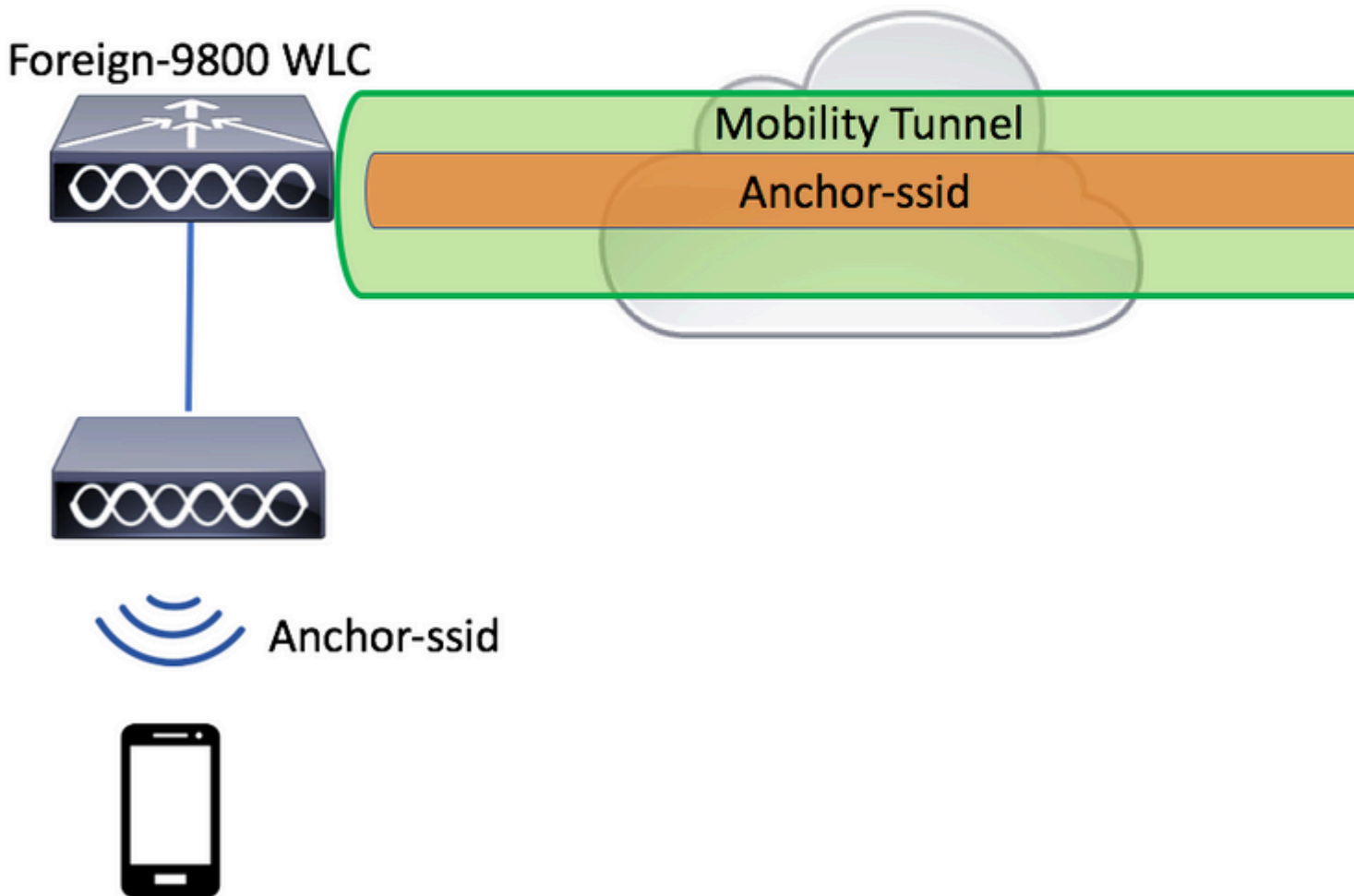
Configureren

Dit is een functie die normaal wordt gebruikt voor de toegangsscenario's van de gast, om al het verkeer van klanten naar een enkel L3-uitgangspunt te beëindigen, zelfs als de klanten van verschillende controllers en fysieke locaties komen. De mobiliteitstunnel biedt een mechanisme om het verkeer geïsoleerd te houden, aangezien het het netwerk doorkruist.

Buitenlands/ankerscenario tussen 9800 WLC's

Dit scenario toont de twee gebruikte Catalyst 9800s.

Netwerkdigram: twee Catalyst 9800 WLC's



Voor mobiliteitsgastenscenario's, zijn er twee belangrijke controllerrollen:

- Buitenlandse controller: deze WLC bezit Layer 2 of de draadloze kant. Het heeft toegangspunten die erop zijn aangesloten. Al cliëntverkeer voor verankerde WLAN's is ingekapseld in de mobiliteitstunnel die naar het anker moet worden verzonden. Dit gebeurt niet lokaal.
- Ankerbesturing: Dit is het afsluitpunt voor Layer 3. Het ontvangt de mobiliteitstunnels van de buitenlandse controllers en decapsuleert of beëindigt het clientverkeer naar het exit point (VLAN). Dit is het punt waar de cliënten in het netwerk, dus de ankernaam worden gezien.

Access points op de externe WLC broadcast de WLAN-SSID's en hebben een beleidstag toegewezen die het WLAN-profiel koppelt aan het juiste beleidsprofiel. Wanneer een draadloze client verbinding maakt met deze SSID, stuurt de buitenlandse controller beide, de SSID-naam en het beleidsprofiel als onderdeel van de clientinformatie naar het anker WLC. Na ontvangst, controleert het anker WLC zijn eigen configuratie om de SSID naam evenals de naam van het Profiel van het Beleid aan te passen. Zodra het anker WLC een overeenkomst vindt, past het de configuratie toe die aan het en een uitgangspunt aan de draadloze cliënt beantwoordt. Daarom is het verplicht dat WLAN- en beleidsprofielnamen en -configuraties overeenkomen

op zowel buitenlandse 9800 WLC als anker 9800 WLC met uitzondering van VLAN onder het beleidsprofiel.

Opmerking: WLAN-profiel en beleidsprofielnamen kunnen overeenkomen op zowel 9800 anker als 9800 Foreign WLC.

Een 9800 Foreign configureren met een 9800 anker

Stap 1. Bouw een mobiliteitstunnel tussen de Foreign 9800 WLC en Anchor 9800 WLC.

U kunt naar dit document verwijzen: [Mobility-topologieën configureren op Catalyst 9800](#)

Stap 2. Maak de gewenste SSID op beide 9800 WLC's.

Ondersteunde beveiligingsmethoden:

- Open (Openstaand)
- MAC-filter
- PSK
- Dot1x
- Lokale/externe webverificatie (LWA)
- Centrale webverificatie (CWA)

Opmerking: beide 9800 WLC's moeten dezelfde configuratie hebben, anders werkt anker niet.

Stap 3. Log in op de buitenlandse 9800 WLC en definieer anker 9800 WLC IP-adres onder het beleidsprofiel.

Naar navigeren [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

Op de Mobility Kies op het tabblad het IP-adres van het anker 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)


Anchor IP

 172.16.0.5	→
---	---

Selected (1)

Anchor IP

Anchor Priority

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

Cancel

Save &

Stap 4. Koppel het beleidsprofiel met het WLAN binnen de beleidstag die is toegewezen aan de AP's die zijn gekoppeld aan de buitenlandse controller die dit WLAN afhandelt.

Naar navigeren [Configuration > Tags & Profiles > Tags](#) en maak een nieuwe of gebruik de bestaande.

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*

Zorg ervoor dat u kiest **Update & Apply to Device** om de wijzigingen in de beleidstag toe te passen.

Edit Policy Tag

Name*

Description

+ Add

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

Stap 5 (facultatief). Wijs de beleidsmarkering toe aan een toegangspunt of controleer of het toegangspunt deze reeds heeft.

Naar navigeren [Configuration](#) > [Wireless](#) > [Access Points](#) > [AP name](#) > [General](#).

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	karlcisn-AP-30
Location*	default-location
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	PT1
Site	ST1
RF	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)	11.11.0.39
Netmask	255.255.0.0
Gateway (IPv4/IPv6)	11.11.0.1
DNS IP Address (IPv4/IPv6)	0.0.0.0
Domain Name	Cisco

Time Statistics

Up Time	3 days 0 mins 26
---------	------------------

Cancel

Update &

Opmerking: Houd er rekening mee dat als u een wijziging in de AP-tag uitvoert nadat u hebt gekozen `Update & Apply to Device` Maar de AP herstart zijn tunnel CAPWAP, dus het verliest associatie met de 9800 WLC en dan herstelt het.

Van de 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
```

Stap 6. Log in om 9800 WLC te verankeren en maak het ankerbeleidsprofiel. Zorg ervoor dat het exact dezelfde naam heeft die u hebt gebruikt op de buitenlandse 9800 WLC's.

Naar navigeren [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	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"/>	

Naar navigeren Mobility tabblad en inschakelen Export Anchor. Dit instrueert de 9800 WLC dat het anker 9800 WLC is voor elk WLAN dat dat beleidsprofiel gebruikt. Wanneer de buitenlandse 9800 WLC de clients naar anker 9800 WLC stuurt, informeert het over het WLAN en het beleidsprofiel waaraan de client is toegewezen, zodat het anker 9800 WLC weet welk lokaal beleidsprofiel moet worden gebruikt.

Opmerking: u mag geen mobiliteitspers configureren en ankers tegelijkertijd exporteren. Dat is een ongeldig configuratiescenario.

Opmerking: u mag de instelling Anker exporteren niet gebruiken voor een beleidsprofiel dat is gekoppeld aan een WLAN-profiel op een controller met toegangspunten. Dit verhindert dat de SSID wordt uitgezonden, dus dit beleid moet uitsluitend worden gebruikt voor ankerfunctionaliteit.

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 →		

Van de CLI:

```
Anchor 9800 WLC

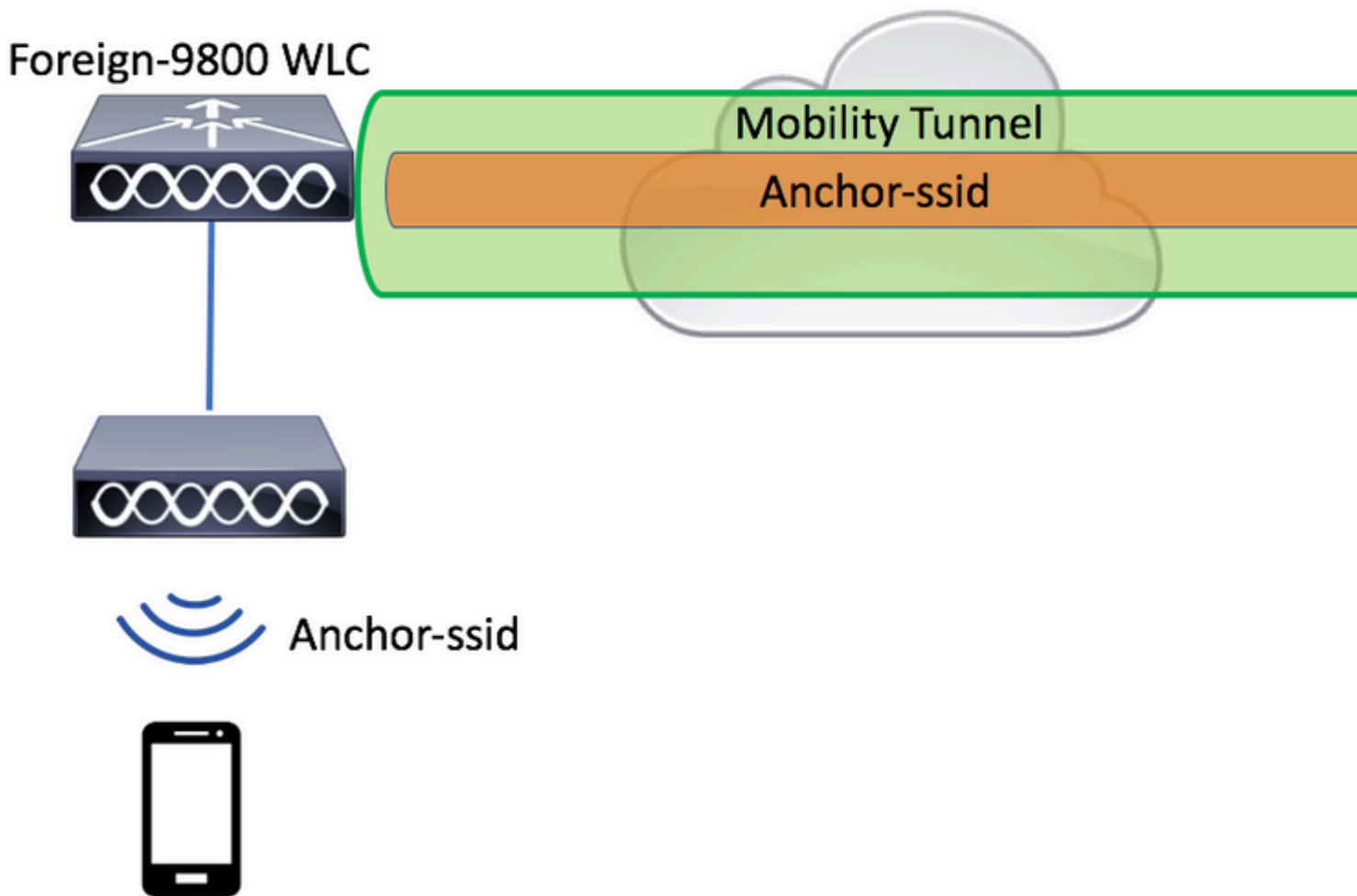
# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Foreign 9800 WLC - anker AireOS

Deze opstelling schildert het scenario af waar een Catalyst 9800 WLC als Foreign wordt gebruikt met een

AireOS Unified WLC die als anker wordt gebruikt.

Catalyst 9800 buitenlands netwerkdiagram - AireOS anker



Configureer 9800 Foreign met AireOS-anker

Stap 1. Bouw een mobiliteitstunnel tussen de Foreign 9800 WLC en Anchor AireOS WLC.

Raadpleeg dit document: [Mobility topologieën configureren op Catalyst 9800](#)

Stap 2. Maak de gewenste WLAN's op beide WLC's.

Ondersteunde beveiligingsmethoden:

- Open (Openstaand)

- MAC-filter
- PSK
- Dot1x
- Lokale/externe webverificatie (LWA)
- Centrale webverificatie (CWA)

Opmerking: zowel AireOS WLC als 9800 WLC moeten dezelfde configuratie hebben, anders werkt anker niet.

Stap 3. Log in op de 9800 WLC (dat als buitenlands) en maak het ankerbeleidsprofiel.

Naar navigeren 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

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 &

Naar navigeren Mobility en kies het anker AireOS WLC. De 9800 WLC stuurt het verkeer van de SSID gekoppeld aan dit beleidsprofiel naar het gekozen anker.

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 ... </div>

Stap 4. Koppel het beleidsprofiel met het WLAN binnen de beleidstag die is toegewezen aan de AP's die zijn gekoppeld aan de buitenlandse controller die dit WLAN afhandelt.

Naar navigeren Configuration > Tags & Profiles > Tags en maak een nieuwe of gebruik de bestaande.

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*

Zorg ervoor dat u kiest **Update & Apply to Device** om de wijzigingen in de beleidstag toe te passen.

Edit Policy Tag

Name*

Description

+ Add

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

Stap 5 (facultatief). Wijs de Site toe aan een AP of controleer of deze de Site reeds heeft.

Naar navigeren [Configuration](#) > [Wireless](#) > [Access Points](#) > [AP name](#) > [General](#).

Edit AP

General

Interfaces

High Availability

Inventory

Advanced

AP Name*	karlcisn-AP-30
Location*	default-location
Base Radio MAC	000a.ad00.1f00
Ethernet MAC	000a.ad00.1ff0
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	PT1
Site	ST1
RF	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)	11.11.0.39
Netmask	255.255.0.0
Gateway (IPv4/IPv6)	11.11.0.1
DNS IP Address (IPv4/IPv6)	0.0.0.0
Domain Name	Cisco

Time Statistics

Up Time	3 days 0 mins 26
---------	------------------

Cancel

Update &

Opmerking: houd er rekening mee dat als u een wijziging in de AP-tag uitvoert nadat u hebt gekozen Update & Apply to Device Maar de AP herstart zijn tunnel CAPWAP, dus het verliest associatie met de 9800 WLC en dan herstelt het.

Van de CLI:

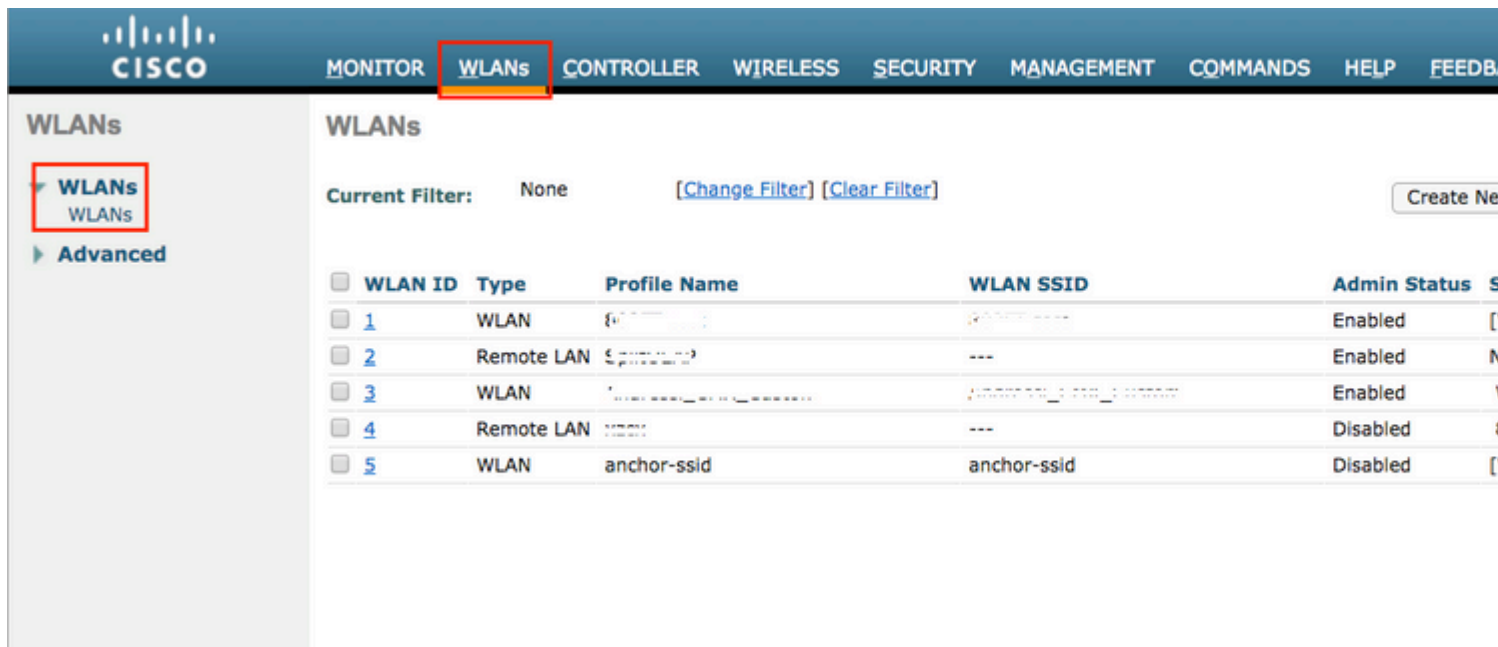
```
# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

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

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

Stap 6. Configureer de AireOS WLC als anker.

Log in op AireOS en navigeer naar WLANs > WLANs. Kies de pijl naar de rechterkant van de WLAN-rij om naar het vervolgkeuzemenu te navigeren en kies 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

Stel dit in als het lokale anker.

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority ¹

3

Foot Notes

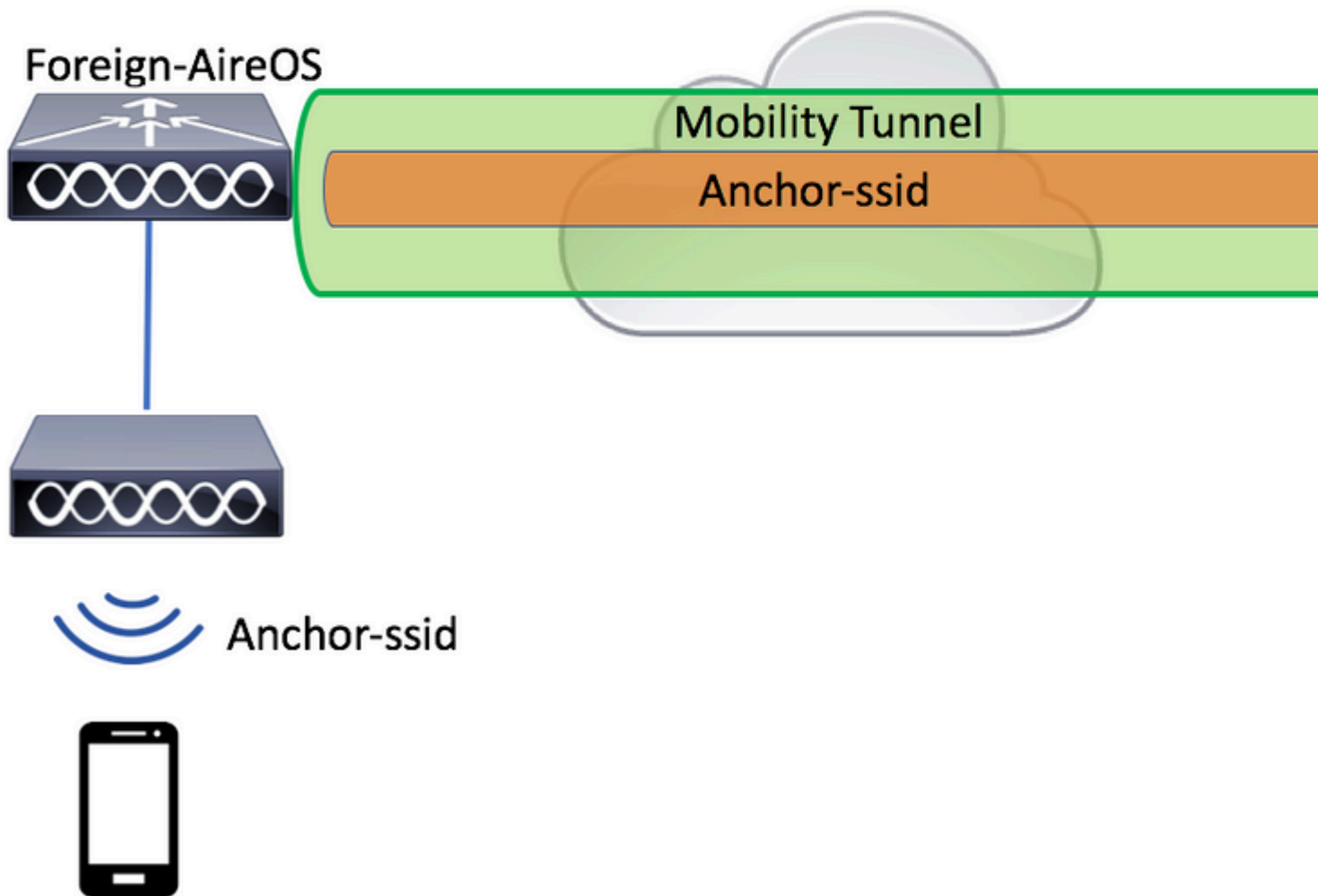
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

Van de 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 - anker 9800 WLC

AireOS Foreign met 9800 ankernetwerkdigram



Een 9800 Foreign configureren met een AireOS-anker

Stap 1. Bouw een mobiliteitstunnel tussen de Foreign 9800 WLC en Anchor AireOS WLC.

U kunt naar dit document verwijzen: [Mobility-topologieën configureren op Catalyst 9800](#)

Stap 2. Maak de gewenste SSID op beide WLC's.

Ondersteunde beveiligingsmethoden:

- Open (Openstaand)
- MAC-filter
- PSK
- Dot1x
- Lokale/externe webverificatie (LWA)

- Centrale webverificatie (CWA)

Opmerking: zowel AireOS WLC als 9800 WLC moeten dezelfde configuratie hebben, anders werkt anker niet.

Stap 3. Log in op de 9800 WLC (dat fungeert als anker) en maak het ankerbeleidsprofiel.

Naar navigeren [Configuration](#) > [Tags & Profiles](#) > [Policy](#) > + Add. Zorg ervoor dat de naam van het beleidsprofiel op 9800 exact dezelfde is als de profielnaam op de AireOS WLC, anders werkt het niet.

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 & Cancel

Naar navigeren [Mobility](#) tabblad en inschakelen [Export Anchor](#). Dit instrueert de 9800 WLC dat het anker 9800 WLC is voor elk WLAN dat dat beleidsprofiel gebruikt. Wanneer de buitenlandse AireOS WLC de clients naar anker 9800 WLC stuurt, informeert het over de WLAN-naam waaraan de client is toegewezen, zodat de anker 9800 WLC weet welke lokale WLAN-configuratie moet worden gebruikt en het gebruikt ook deze naam om te weten welk lokaal beleidsprofiel moet worden gebruikt.

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 &

Opmerking: Zorg ervoor dat u dit beleidsprofiel uitsluitend gebruikt om verkeer van buitenlandse luchtverkeersleiders te ontvangen.

Van de CLI:

Anchor 9800 WLC

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

Stap 4. Configureer de AireOS WLC als vreemd.

Log in op AireOS en navigeer naar WLANs > WLANs. Navigeer naar de pijl van de pijl onder de versmalling aan het einde van de WLAN-rij en kies Mobility Anchor.

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

Stel de 9800 WLC in als anker voor deze SSID.

WLAN SSID anchor-ssid

Switch IP Address (Anchor) 10.88.173.105

Priority 3

Foot Notes

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

Van de CLI:


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

Verificatie

U kunt deze opdrachten gebruiken om de configuratie en de status van de draadloze clients te verifiëren met behulp van een buitenlandse/anker-SSID.

Controleer de 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>
```

Controleer de AireOS WLC

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

Problemen oplossen

WLC 9800 biedt altijd-on traceermogelijkheden. Dit zorgt ervoor dat alle client-connectiviteit gerelateerde fouten, waarschuwingen en meldingen voortdurend worden vastgelegd en u kunt gebeurtenissen bekijken voor een incident of storing nadat het is opgetreden.

Opmerking: afhankelijk van het volume van de gegenereerde logbestanden, kunt u een paar uur teruggaan naar meerdere dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en naar deze stappen verwijzen. (Zorg ervoor dat u de sessie in een tekstbestand logt)

Stap 1. Controleer de huidige tijd van de controller, zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

```
# show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals de systeemconfiguratie dicteert. Dit geeft een snel overzicht van de systeemstatus en eventuele fouten.

```
# show logging
```

Stap 3. Verzamel de altijd-op berichtniveau sporen voor het specifieke mac of IP adres. Remote mobility peer kan dit filteren als je een mobiliteitstunnel probleem vermoedt, of door het draadloze client mac adres.

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

Stap 4. U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

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

Voorwaardelijke debugging en radio actieve tracering

Als de altijd-op sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-sporen opnemen, die debug-level sporen biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Raadpleeg deze stappen om voorwaardelijke debugging in te schakelen.

Stap 5. Zorg ervoor dat geen debug voorwaarden zijn ingeschakeld.

```
# clear platform condition all
```

Stap 6. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdrachten wordt het opgegeven MAC-adres 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

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

Opmerking: als u meer dan één client tegelijk wilt bewaken, voert u de opdracht `debug wireless mac <aaaa.bbbb.ccc>` per mac-adres uit.

Opmerking: U ziet de output van de client activiteit niet op de terminal sessie, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 7. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 8. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

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

Zodra de monitortijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Stap 9. Verzamel het bestand van de mac-adresactiviteit. U kunt het RA-spoor kopiëren `.log` naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Controleer de naam van het RA traces bestand:

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

Kopieert het bestand naar een externe server:

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

Geef de inhoud weer:

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

Stap 10. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer uitgebreide mening van debug-niveau logboeken zijn. U hoeft de client niet opnieuw te debuggen, aangezien de logbestanden al in het geheugen van de controller zijn geschreven en u alleen een uitgebreidere weergave van deze logbestanden hoeft te vullen.

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

Opmerking: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem Cisco TAC in om te helpen bij het doorlopen van deze sporen.

U kunt de ra-internal-FILENAME.txt naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Kopieert het bestand naar een externe server:

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

Geef de inhoud weer:

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

Stap 11. Verwijder de debug-voorwaarden.

```
# clear platform condition all
```

Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossing sessie.

Controleer de AireOS WLC

U kunt deze opdracht uitvoeren om de activiteit van een draadloze client op een AireOS WLC te bewaken.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.