

Configure WLAN Anchor Mobility Feature on Catalyst 9800

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Foreign/Anchor Scenario Between 9800 WLCs](#)

[Network Diagram: Two Catalyst 9800 WLCs](#)

[Configure a 9800 Foreign with a 9800 Anchor](#)

[Foreign 9800 WLC - Anchor AireOS](#)

[Catalyst 9800 Foreign - AireOS Anchor Network Diagram](#)

[Configure 9800 Foreign with AireOS Anchor](#)

[Foreign AireOS - Anchor 9800 WLC](#)

[AireOS Foreign with 9800 Anchor Network Diagram](#)

[Configure a 9800 Foreign with an AireOS Anchor](#)

[Verification](#)

[Verify on the 9800 WLC](#)

[Verify on the AireOS WLC](#)

[Troubleshoot](#)

[Conditional Debugging and Radio Active Tracing](#)

[Verify the AireOS WLC](#)

Introduction

This document describes how to configure a Wireless Local Area Network (WLAN) on a foreign/anchor scenario with Catalyst 9800 Wireless Controllers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Command Line Interface (CLI) or Graphic User Interface (GUI) access to the wireless controllers
- Mobility on Cisco Wireless LAN Controllers (WLCs)
- 9800 Wireless Controllers
- AireOS WLCs

Components Used

The information in this document is based on these software and hardware versions:

- AireOS WLC version 8.8 MR2 (you can also use Inter Release Controller Mobility (IRCM) special 8.5 images)
- 9800 WLC v16.10 or later
- 9800 WLC Configuration Model

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. If your network is live, ensure that you understand the potential impact of any command.

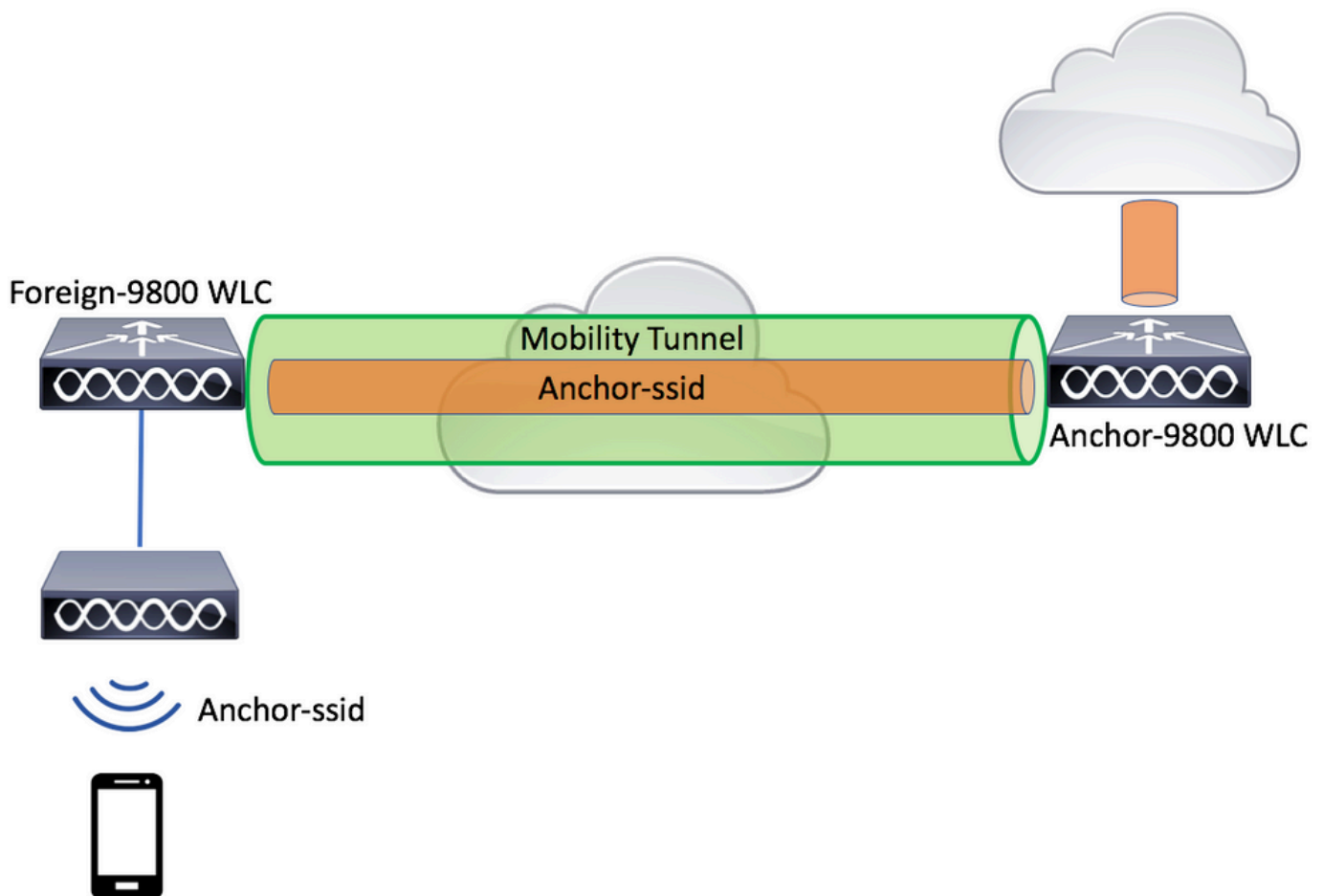
Configure

This is a feature normally used for Guest access scenarios, to terminate all traffic from clients into a single L3 exit point, even if the clients come from different controllers and physical locations. The mobility tunnel provides a mechanism to keep the traffic isolated, as it transverse the network.

Foreign/Anchor Scenario Between 9800 WLCs

This scenario depicts the two Catalyst 9800s used.

Network Diagram: Two Catalyst 9800 WLCs




For mobility guest scenarios, there are two main controller roles:

- Foreign controller: This WLC owns layer 2 or the wireless side. It has access points connected to it. All client traffic for the anchored WLANs is encapsulated into the mobility tunnel to be sent to the anchor. It does not exit locally.

- **Anchor controller:** This is the layer 3 exit point. It receives the mobility tunnels from the foreign controllers and decapsulates or terminates the client traffic into the exit point (VLAN). This is the point where the clients are seen in the network, thus the anchor name.

Access points on the foreign WLC broadcast the WLAN SSIDs and have a policy tag assigned that links the WLAN profile with the appropriate policy profile. When a wireless client connects to this SSID, the foreign controller sends both, the SSID name and Policy Profile as part of the client information to the anchor WLC. Upon receipt, the anchor WLC checks its own configuration to match the SSID name as well as the Policy Profile name. Once anchor WLC finds a match, it applies the configuration that corresponds to it and an exit point to the wireless client. Therefore, it is mandatory that WLAN and Policy Profile names and configurations match on both foreign 9800 WLC and anchor 9800 WLC with the exception of VLAN under the Policy Profile.

 **Note:** WLAN Profile and Policy Profile names can match on both 9800 Anchor and 9800 Foreign WLC.

Configure a 9800 Foreign with a 9800 Anchor


Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor 9800 WLC.

You can refer to this document: [Configuring Mobility topologies on Catalyst 9800](#)

Step 2. Create the desired SSID on both 9800 WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

 **Note:** Both 9800 WLCs must have the same kind of configuration, otherwise anchor does not work.

Step 3. Log in to the foreign 9800 WLC and define anchor 9800 WLC IP address under the policy profile.

Navigate to 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"/> | |

On the **Mobility** tab, choose the IP address of the anchor 9800 WLC.

Add Policy Profile

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

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

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

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

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

Cancel Save & Apply to Device

Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated with the foreign controller that services this WLAN.

Navigate to Configuration > Tags & Profiles > Tags and either create a new one or use the one that exists.

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 ✓

Ensure you choose **Update & Apply to Device** to apply the changes to the Policy Tag.

Edit Policy Tag ✕

Name*

Description

+ Add

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

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

Step 5 (optional). Assign the Policy Tag to an AP or verify that it already has it.

Navigate to **Configuration > Wireless > Access Points > AP name > General**.

Edit AP
✕

General
Interfaces
High Availability
Inventory
Advanced

| | | | |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------|------------------------------------------|
| AP Name* | <input type="text" value="karlcisn-AP-30"/> | Primary Software Version | 8.5.97.110 |
| Location* | <input type="text" value="default-location"/> | Predownloaded Status | N/A |
| Base Radio MAC | 000a.ad00.1f00 | Predownloaded Version | N/A |
| Ethernet MAC | 000a.ad00.1ff0 | Next Retry Time | N/A |
| Admin Status | <input style="border: none; background-color: #eee; padding: 2px 5px; border-radius: 3px; width: 100%;" type="button" value="Enabled"/> | Boot Version | 8.5.97.110 |
| AP Mode | <input style="border: none; background-color: #eee; padding: 2px 5px; border-radius: 3px; width: 100%;" type="button" value="Local"/> | IOS Version | |
| Operation Status | Registered | Mini IOS Version | 0.51.0.3 |
| Fabric Status | Disabled | IP Config | |
| Tags | | CAPWAP Preferred Mode | Not Configured |
| Policy | <input style="border: none; background-color: #eee; padding: 2px 5px; border-radius: 3px; width: 100%;" type="button" value="PT1"/> | Static IPv4 Address | 11.11.0.39 |
| Site | <input style="border: none; background-color: #eee; padding: 2px 5px; border-radius: 3px; width: 100%;" type="button" value="ST1"/> | Static IP (IPv4/IPv6) | <input checked="" type="checkbox"/> |
| RF | <input style="border: none; background-color: #eee; padding: 2px 5px; border-radius: 3px; width: 100%;" type="button" value="RT1"/> | 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

Note: Be aware that if you perform a change in the AP tag after you choose Update & Apply to Device, the AP restarts its tunnel CAPWAP, so it loses association with the 9800 WLC and then recovers it.

From the 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

```

Step 6. Log in to anchor 9800 WLC and create the anchor policy profile. Ensure it has the exact same name that you used on the foreign 9800 WLCs.

Navigate to Configuration > Tags & Profiles > Policy > + Add.

Add Policy Profile

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

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

Name*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching


Central Authentication


Central DHCP

Central Association

Flex NAT/PAT

Navigate to Mobility tab and enable Export Anchor. This instructs the 9800 WLC that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign 9800 WLC sends the clients to the anchor 9800 WLC, it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 WLC knows which local Policy Profile to use.

 **Note:** You must not configure mobility peers and export anchor at the same time. That is an invalid configuration scenario.

 **Note:** You must not use the Export Anchor setting, for any policy profile tied to a WLAN profile on a controller with access points. This prevents the SSID to be broadcasted, so this policy must be used exclusively for Anchor functionality.

Add Policy Profile ✕

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







Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

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

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

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

From the CLI:

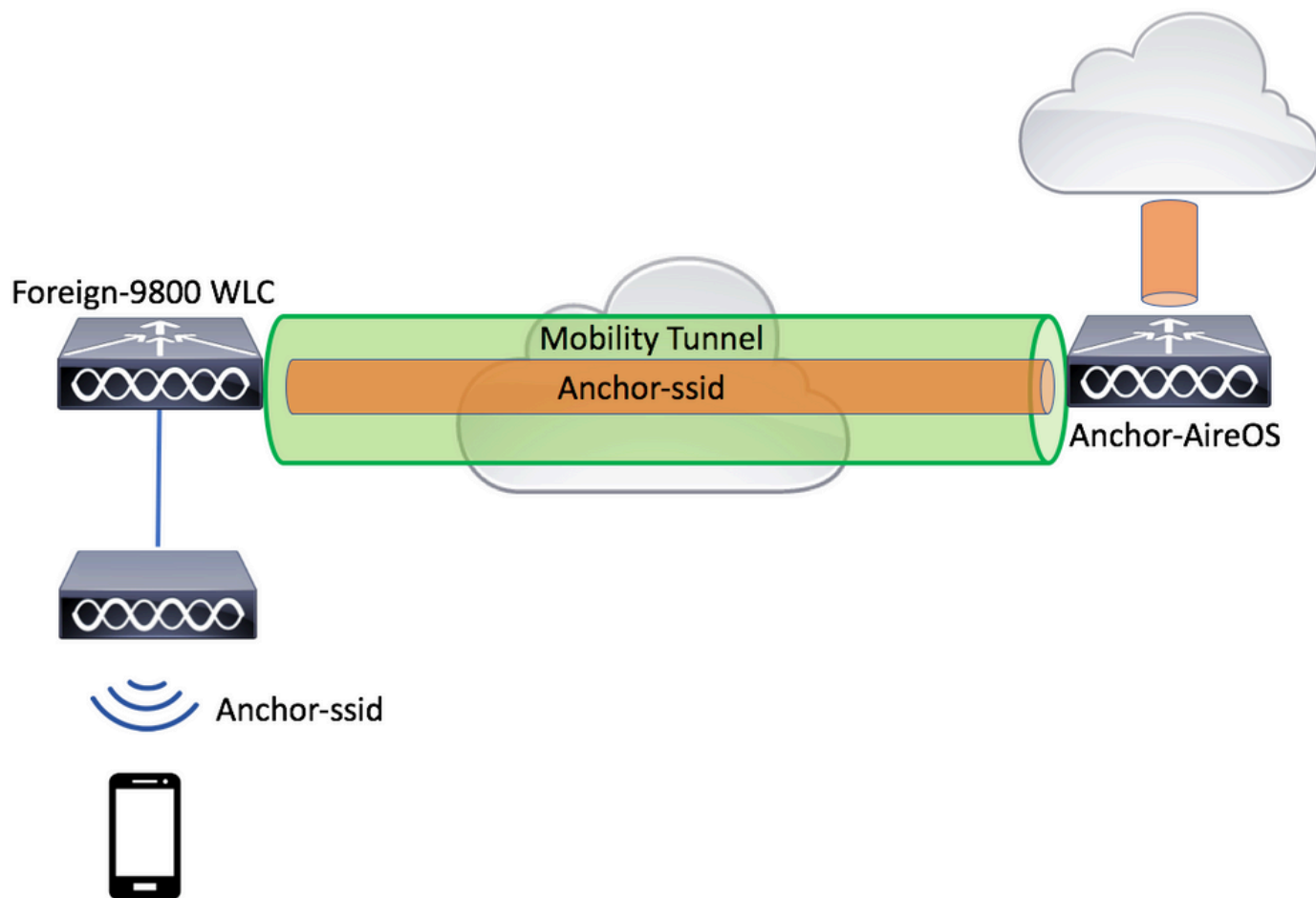
Anchor 9800 WLC

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

Foreign 9800 WLC - Anchor AireOS

This setup depicts the scenario where a Catalyst 9800 WLC is used as Foreign with an AireOS Unified WLC used as the anchor.

Catalyst 9800 Foreign - AireOS Anchor Network Diagram



Configure 9800 Foreign with AireOS Anchor


Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor AireOS WLC.

Refer to this document: [Configuring Mobility topologies on Catalyst 9800](#)

Step 2. Create the desired WLANs on both WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

 **Note:** Both AireOS WLC and 9800 WLC must have the same kind of configuration, otherwise anchor does not work.

Step 3. Log in to the 9800 WLC (that acts as foreign) and create the anchor policy profile.

Navigate to 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 | WLAN Switching Policy | |
| Description | 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 | 2-65519 | | |

Navigate to Mobility tab and choose the anchor AireOS WLC. The 9800 WLC forwards the traffic of the SSID associated with this Policy Profile to the chosen anchor.

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> |

Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated with the foreign controller that services this WLAN.

Navigate to Configuration > Tags & Profiles > Tags and either create a new one or use the one that exists.

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*

Ensure you choose **Update & Apply to Device** to apply the changes to the Policy Tag.

Edit Policy Tag ✕

Name*

Description

+ Add

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

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

Step 5 (optional). Assign the Site to an AP or verify that it already has it.

Navigate to **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 | IP Config | |
| Tags | | CAPWAP Preferred Mode | Not Configured |
| Policy | <input type="text" value="PT1"/> | Static IPv4 Address | 11.11.0.39 |
| Site | <input type="text" value="ST1"/> | Static IP (IPv4/IPv6) | <input checked="" type="checkbox"/> |
| RF | <input type="text" value="RT1"/> | 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

Note: Be aware that if you perform a change in the AP tag after you choose Update & Apply to Device, the AP restarts its tunnel CAPWAP, so it loses association with the 9800 WLC and then recovers it.

From the 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

```

Step 6. Configure the AireOS WLC as the anchor.

Log in to AireOS and navigate to WLANs > WLANs. Choose the arrow to the right end of the WLAN row in order to navigate to the drop-down menu and choose Mobility Anchors.

The screenshot shows the Cisco AireOS configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' section is active, showing a table of WLAN configurations. The table has columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. The fifth row (ID 5) is selected, and a dropdown menu is open, showing options like 'Remove', 'Mobility Anchors', '802.11u', 'Foreign Maps', 'Service Advertisements', and 'Hotspot 2.0'. The 'Mobility Anchors' option is highlighted.

| 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)] |

Set it as the local anchor.

Mobility Anchors

WLAN SSID anchor-ssid

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

local

Priority 1

3

Foot Notes

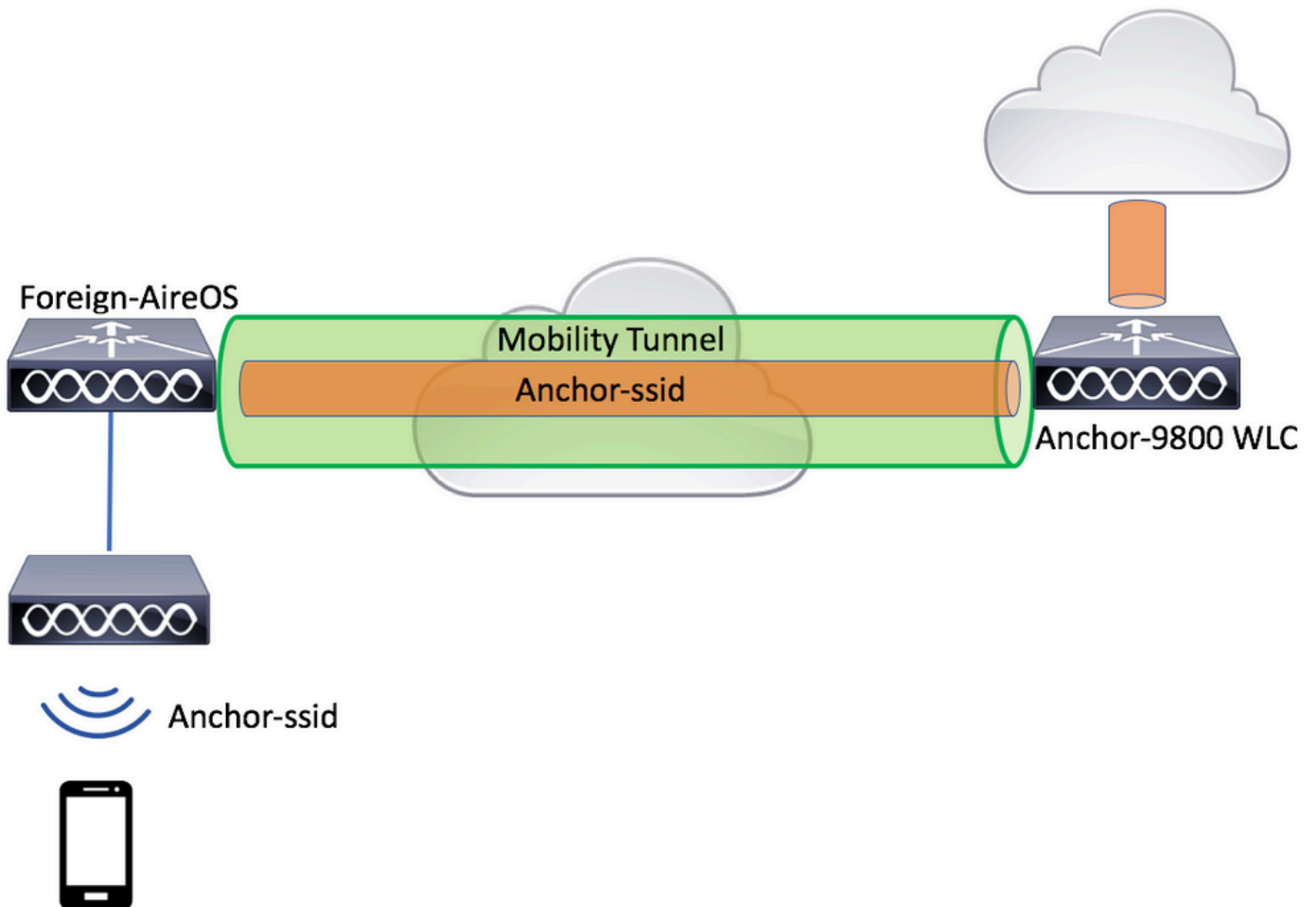
1. Priority number, 1=Highest priority and 3=Lowest priority(default).

From the 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

AireOS Foreign with 9800 Anchor Network Diagram



Configure a 9800 Foreign with an AireOS Anchor


Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor AireOS WLC.

You can refer to this document: [Configuring Mobility topologies on Catalyst 9800](#)

Step 2. Create the desired SSID on both WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

 **Note:** Both AireOS WLC and 9800 WLC must have the same kind of configuration, otherwise anchor does not work.

Step 3. Log in to the 9800 WLC (that acts as an anchor) and create the anchor policy profile.

Navigate to Configuration > Tags & Profiles > Policy > + Add. Ensure that the name of the Policy Profile on 9800 is the exact same name as the Profile name on the AireOS WLC, otherwise, it does not work.

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

Navigate to **Mobility** tab and enable **Export Anchor**. This instructs the 9800 WLC that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign AireOS WLC sends the clients to the anchor 9800 WLC, it informs about the WLAN name that the client is assigned to, so the anchor 9800 WLC knows which local WLAN configuration to use and it also uses this name to know which local Policy Profile to use.

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 |
| <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 172.16.0.5 → </div> <div style="border: 1px solid #ccc; padding: 5px;"> 10.88.173.49 → </div> | Anchors not assigned | |

Note: Ensure you use this policy profile exclusively to receive traffic from foreign controllers.

From the CLI:

Anchor 9800 WLC

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

Step 4. Configure the AireOS WLC as foreign.

Log in to AireOS and navigate to WLANs > WLANs. Navigate to the blow arrow at the end of the WLAN row and choose 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

Set the 9800 WLC as an anchor for this SSID.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Mobility Anchors

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).

From the CLI:

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

Verification

You can use these commands to verify the configuration and the state of the wireless clients with the use of a foreign/anchor SSID.

Verify on the 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>
```

Verify on the AireOS WLC

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

Troubleshoot

WLC 9800 provides always-on tracing capabilities. This ensures all client connectivity-related errors, warnings, and notice-level messages are constantly logged and you can view events for an incident or failure condition after it has occurred.



Note: Depending on the volume of logs generated, you can go back a few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and refer to these steps. (Ensure you log the session to a text file)

Step 1. Check the current time of the controller so you can track the logs in the time back to when the issue happened.

```
# show clock
```

Step 2. Collect syslogs from the controller buffer or the external syslog as the system configuration dictates. This provides a quick view into the system health and errors if any.

```
# show logging
```

Step 3. Collect the always-on notice level traces for the specific mac or IP address. Remote mobility peer can filter this, if you suspect a mobility tunnel issue, or by wireless client mac address.

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

Step 4. You can either display the content on the session or you can copy the file to an external 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>
```

Conditional Debugging and Radio Active Tracing

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) traces, which provides debug-level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, refer to these steps.


Step 5. Ensure there are no debug conditions enabled.


```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client mac address that you want to monitor.

These commands start to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

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

 **Note:** In order to monitor more than one client at a time, run `debug wireless mac <aaaa.bbbb.cccc>` command per mac address.

 **Note:** You do not see the output of the client activity on the terminal session, as everything is buffered internally to be viewed later.

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

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

Once the monitor time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name: `ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log`

Step 9. Collect the file of the mac address activity. You can either copy the RA trace `.log` to an external server or display the output directly on the screen.

Check the name of the RA traces file:

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

Copy the file to an external server:


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

Display the content:

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

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug-level logs. You do not need to debug the client again as the logs were already written in the controller memory and you only need to populate a more verbose view of them.

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

 **Note:** This command output returns traces for all logging levels for all processes and is quite voluminous. Engage Cisco TAC to help parse through these traces.

You can either copy the `ra-internal-FILENAME.txt` to an external server or display the output directly on the screen.

Copy the file to an external server:

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

Display the content:

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

Step 11. Remove the debug conditions.

```
# clear platform condition all
```

 **Note:** Ensure that you always remove the debug conditions after a troubleshooting session.

Verify the AireOS WLC

You can run this command to monitor the activity of a wireless client on an AireOS WLC.


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