Configure Mobility Anchor on Catalyst 9800 Wireless Controllers

Contents

Introduction
Prerequisites
Requirements
Components Used
Configuration

--
Foreign/Anchor Scenario between 9800 WLCs
Network Diagram
Configurations
Foreign 9800 WLC - Anchor AireOS
Network Diagram
Configurations
Foreign AireOS - Anchor 9800 WLC
Network Diagram
Configurations
Verification
9800 WLC
AireOS WLC
Troubleshoot
AireOS WLC

Introduction

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

**Configuration**

**Foreign/Anchor Scenario between 9800 WLCs**

Network Diagram

AP on the foreign WLC broadcasting SSIDs will have a policy tag assigned that links the SSID and corresponding WLAN profile with the policy profile. When a wireless client connects to this SSID, foreign WLC 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 config to match the SSID name as well as Policy Profile name. Once anchor WLC finds a match, it will apply corresponding configuration to the wireless client. Therefore, it is mandatory that WLAN and Policy Profile names match on both foreign 9800 WLC and anchor 9800 WLC with the exception of
VLAN under the Policy Profile.

Configurations

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

You can follow this document:

Building Mobility Tunnels on 9800 WLCs

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

Supported security methods:

- Open
- MAC filtering
- PSK
- Dot1x
- Local Web Authentication (LWA)
- Central Web Authentication (CWA)

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 (called

Navigate to Configuration > Tags & Profiles > Policy > + Add.)
On the Mobility tab, select the IP address of the anchor 9800 WLC.
Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned (or that will be assigned) to the APs associated to the foreign controller that service this WLAN.

Navigate to Configuration > Tags & Profiles > Tags and either create a new one or use an existing one.
Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

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

**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**

Navigate to **Mobility** tab and enable **Export Anchor**. This instruct this 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:** Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

**CLI:**

Anchor 9800 WLC

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

**Foreign 9800 WLC - Anchor AireOS**

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

You can follow this document:

Building Mobility Tunnels on 9800 WLCs

Step 2. Create the desired SSID on both WLCs.

Supported security methods:

- Open
- MAC filtering
- PSK
- Dot1x
- Local Web Authentication (LWA)
- Central Web Authentication (CWA)

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 (acting as foreign) and create the anchor policy profile.
Navigate to **Configuration > Tags & Profiles > Policy > + Add**

Navigate to **Mobility** tab and select the anchor AireOS WLC. The 9800 WLC forwards the traffic of the SSID associated to this Policy Profile to the selected anchor.
Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned (or that will be assigned) to the APs associated to the foreign controller that service this WLAN.

Navigate to **Configuration > Tags & Profiles > Tags** and either create a new one or use an existing one.

**Add Policy Profile**

**Mobility Anchors**

- **Export Anchor**: unchecked
- **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)**

<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>

**Save & Apply to Device**

**Edit Policy Tag**

- **Name**: PT1
- **Description**: Enter Description

**Add**

**Map WLAN and Policy**

- **WLAN Profile**: anchor-ssid
- **Policy Profile**: anchor-policy
Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

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

**CLI:**

```sh
# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit
```
Step 6. Configure the AireOS WLC as anchor

Log in to the AireOS and navigate to WLANs > WLANs. Navigate to the drop down menu by clicking on the arrow to the right end of the WLAN's row and select Mobility anchor.

Set it as local anchor.

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

You can follow this document:

Building Mobility Tunnels on 9800 WLCs

Step 2. Create the desired SSID on both WLCs.

Supported security methods:

- Open
- MAC filtering
PSK
• Dot1x
• Local Web Authentication (LWA)
• Central Web Authentication (CWA)

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 (acting as anchor) and create the anchor policy profile.

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

Navigate to **Mobility** tab and enable **Export Anchor**. This instructs this 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.
Note: Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

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 the AireOS and navigate to WLANs > WLANs. Navigate to the blow arrow at the end of the WLAN's row and select Mobility anchor
Set the 9800 WLC as anchor for this SSID.

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 using a foreign/anchor SSID.
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>

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, warning and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

**Note:** Depending on volume of logs being generated, you can go back 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 follow these steps (Ensure you are logging the session to a text file).

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

```bash
# show clock
```

Step 2. Collect syslogs from the controller's buffer or the external syslog as dictated by the system configuration. This will provide a quick view into the system health and errors, if any.

```bash
# show logging
```

Step 3. Verify if any debug conditions are enabled.

```bash
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:

Packet Infra debugs:
```
### 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) trace, which will provide debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, follow these steps.

**Step 5.** Ensure there are no debug conditions are enabled.

```bash
# clear platform condition all
```

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

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

```bash
# 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 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_aaaabbccccc_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_aaaabbccccc_HHmmSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

Display the content:

```
# more bootflash:ra_trace_MAC_aaaabbccccc_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 we are only taking a further detailed look at debug logs that have been already collected and internally stored.

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

**Note:** This command output returns traces for all logging levels for all processes and is quite voluminous. Please 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.

**AireOS WLC**

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

> debug client <client-mac-add>