Cisco Catalyst 9800 Wireless Controller N+1 High Availability White Paper

Table of Contents

Introduction

This guide provides information on the theory of operation and configuration for the Cisco Catalyst 9800 Wireless Controller as it pertains to N+1 mode of High Availability allowing a single WLC to be used as a backup controller for 'N' primary controllers. This solution allows for High availability to be configured for controllers that are geographically on separate L3 network or across the WAN link.

N+1 High Availability Overview

- The N+1 High Availability architecture provides redundancy for controllers across geographically apart data centers with low cost of deployment.

- A single backup controller can be used in order to provide backup for multiple primary WLCs, considering appropriate compatibility in terms of AP mode.

- These WLCs are independent of each other and do not share configuration or IP addresses on any of their interfaces. Each of the WLCs needs to be managed separately and can run a different hardware and a different software version. Note that if the software version is different between the Primary and secondary controllers, the AP will download the software upon joining the secondary controller and result in higher failover time will.

- These WLCs can be deployed in different datacenters across the WAN link.

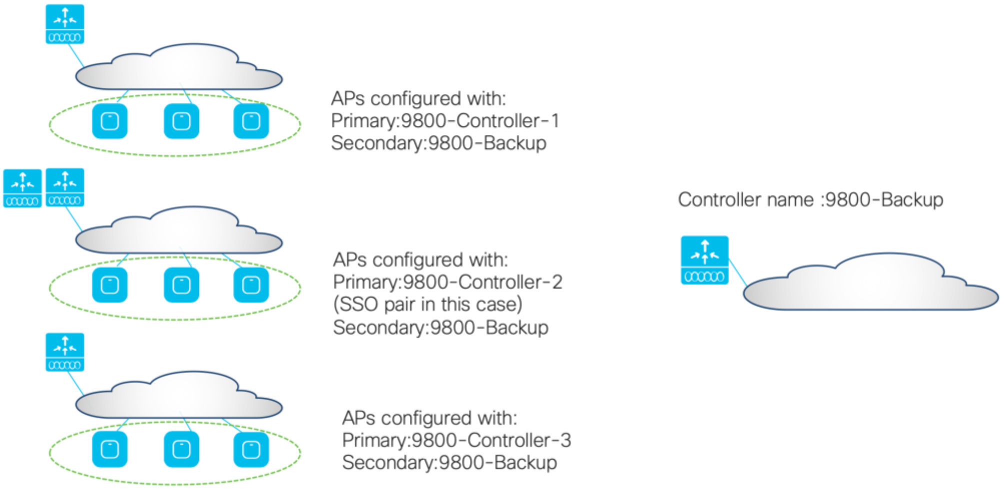
- N+1 HA is not stateful, meaning that no state information about APs and clients is shared between controllers and thus the AP's CAPWAP state machine will be restarted when the primary controller fails.

- When a primary WLC resumes operation, the APs fall back from the backup WLC to the primary WLC automatically if the AP fallback option is enabled.

- APs with high priority on the Primary always connect first to the Backup controller even if they have to push out low priority APs.

- The N+1 HA can be configured in combination with AP SSO where the Primary and/or secondary controllers are their own SSO pair.

- It is recommended to have the same configuration in terms of WLANs, profiles, mobility group, policy, RF and site tags as well as AP-to-tag mappings on the primary, secondary and tertiary controllers to avoid AP flaps and service disruptions when failing over.



Components Used

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

- Catalyst Wireless Controllers 9800-L, 9800-40, 9800-80, 9800-CL, Embedded wireless controller on switch and Embedded Wireless Controller(EWC) on AP9100s.
- 802.11ax, Wave 2 and Wave 1 802.11ac Access points.
- IOS XE Release 16.10 and higher.

Difference Between SSO (Stateful Switchover) and N+1 High availability

Functionality	SSO	N+1
Failover time	Order of sub seconds for box failover and up to 8 seconds for Network GW failure	In the order of 45-60 seconds for the re-discovery and join to secondary controller
Config Sync	Full Configuration and AP/Client State sync	No Sync of config or AP/Client run time data
Detection mechanism	Keep alive timer between Active and Standby units can be configured between 100-1000 msec and retry count between 5-10	Based on various timers, including heartbeat timers and discovery request timers.
L2/L3 topology	Only L2 supported between controllers	L3 is also supported between controller

Software/hardware	Has to be the same between controllers	Can be different
AP/Client Impact	APs and Clients do not disconnect.	APs will rejoin and client need to re-associate and re-authenticate in case of local mode APs and centrally switched, centrally associated SSIDs on Flex APs

Moving APs between controllers and preserving tags

The following should be considered when moving APs between two C9800 wireless controllers for N+1 HA (C9800-1 and C9800-2):

- If the AP on C9800-1 doesn't hold any tag information (the command ap name <AP name> write tag-config was not used)and there is no mapping configured for that AP on C9800-2, the AP will be assigned default tags when moved to C9800-2.
- The AP will retain the tag information when moving between the controllers, if both have the same mapping of AP to tags. This can be done via static configuration, by assigning the AP to a location, or via filters.
- The AP will also retain its tag when moved between the two controllers if the tags are saved to the AP (with the write tag-config command) and the tags are defined on both controllers.
- If the AP has a saved tag assigned via the write tag-config command and joins a controller where those tags are not present, it will be assigned to the default tags (assuming no other mapping is configured on the controller that the AP is joining).
- In all cases, if the AP retains its tag name assignment but the settings within the tag are different on the two controllers, the AP will be configured based on the settings present on the currently joined controller.

When moving an AP from an AireOS controller to a C9800 controller, since the AP doesn't carry any tag information from AireOS, it will be mapped to the default tags; this is true unless a static or dynamic tag pre-assignment has been done on the C9800 controller, as explained above.

When configuring N+1 HA,

- make sure that the controller has the tags and AP-to-tag mapping defined using static mapping or regular expression mapping based on AP name/location.

OR

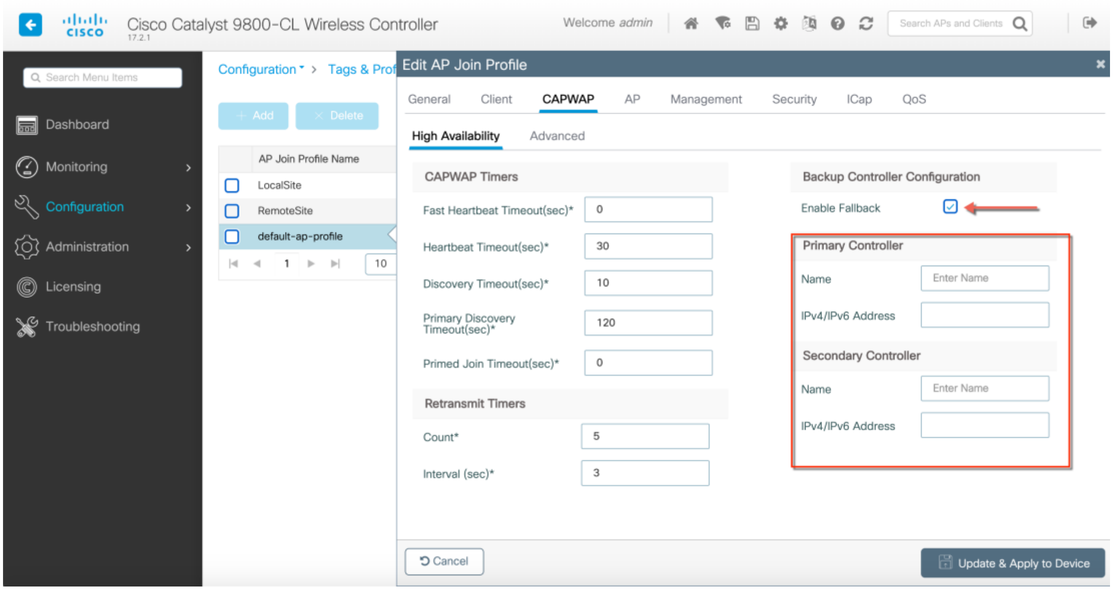
- Use the write tag-config command to save the tags on the AP and define the tags on the secondary controller.

N+1 High Availability Configuration using WebUI

There are two ways to configure N+1 High Availability on the Catalyst 9800: Using the AP join Profiles or High Availability configuration individually on the Access point.

Configuration on AP Join Profile

Under **Configuration > Tags & Profiles > AP Join**, configure the Primary Controller Name and IP and Secondary Controller Name and IP. The **Enable Fallback** option determines if the APs fall back from the backup WLC to the primary WLC automatically if the Primary becomes available. This is enabled by default. CAPWAP Timers and Retransmit timers are used to customize heartbeat and discovery timeouts as well as the retransmit count and interval to track the AP's connection to the controller.



CAPWAP Timers

Fast Heartbeat Timeout(sec)*	0
Heartbeat Timeout(sec)*	30
Discovery Timeout(sec)*	10
Primary Discovery Timeout(sec)*	120
Primed Join Timeout(sec)*	0

Retransmit Timers

Count*	5
Interval (sec)*	3

Backup Controller Configuration

Enable Fallback ☑

Primary Controller

Name	Enter Name
IPv4/IPv6 Address	

Secondary Controller

Name	Enter Name
IPv4/IPv6 Address	

CAPWAP Timers

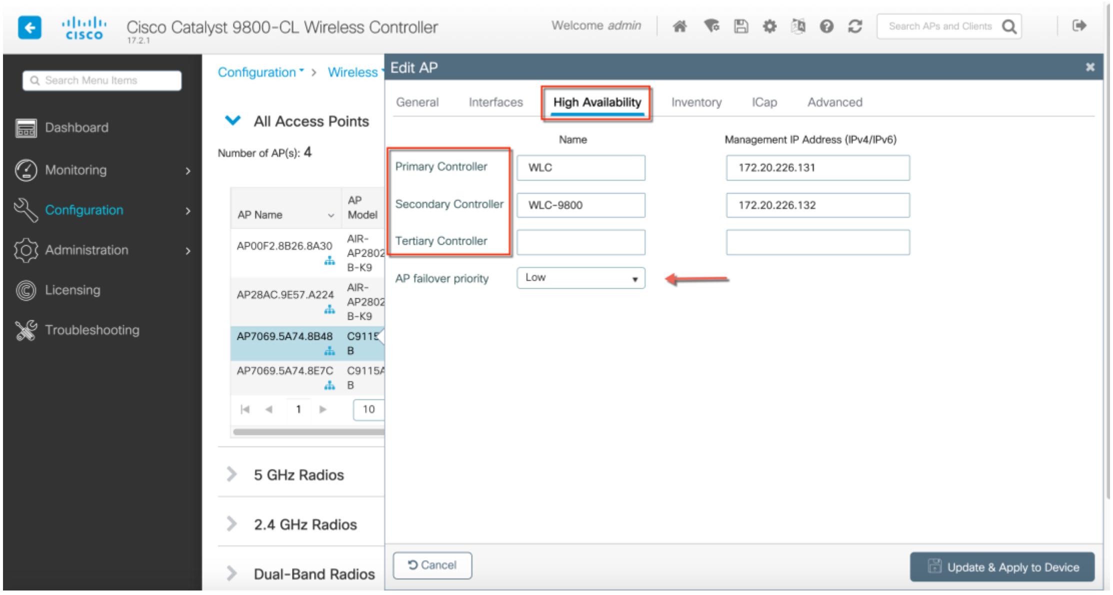
- In the Heartbeat Timeout field, enter the time (in seconds) to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
- In the Discovery Timeout field, enter a value between 1 and 10 seconds (inclusive) to configure the AP discovery request timer.
- In the Primary Discovery Timeout field, enter a value between 30 and 3000 seconds (inclusive) to configure the access point primary discovery request timer.
- In the Primed Join Timeout field, enter a value between 120 and 43200 seconds (inclusive) to configure the access point primed join timeout.
- In the Retransmit Timers Count field, enter the number of times that you want the AP to retransmit the request to the device and vice-versa. Valid range is between 3 and 8.
- In the Retransmit Timers Interval field, enter the time duration between retransmission of requests. Valid range is between 2 and 5.

CLI Commands:

```
WLC(config-ap-profile)#capwap backup ?
  primary    Configures primary Controller
  secondary  Configures secondary Controller

WLC(config-ap-profile)#capwap fallback

CLIs for CAPWAP Timers:

WLC(config-ap-profile)#capwap retransmit ?
  count     Configures AP CAPWAP control packet retransmit count
  interval  Configures AP CAPWAP control packet retransmit interval

WLC(config-ap-profile)#capwap timer
WLC(config-ap-profile)#capwap timers ?
  discovery-timeout          Configures AP Discovery Timeout
  fast-heartbeat-timeout     Configures fast heartbeat timeout
  heartbeat-timeout          Configures heartbeat timeout
  primary-discovery-timeout  Configures primary discovery timeout
  primed-join-timeout        Configures primed join timeout
```

Configuration on Access Points

Under **Configuration > Wireless > Access Points,** click on the AP. Under the High Availability tab configure **Primary, Secondary, Tertiary Controller**. **AP failover priority** determines priority on the access points that connecting to the Primary controller.



Number of AP(s): 4

AP Name	AP Model
AP00F2.8B26.8A30	AIR-AP2802 B-K9
AP28AC.9E57.A224	AIR-AP2802 B-K9
AP7069.5A74.8B48	C911 B
AP7069.5A74.8E7C	C9115A B

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	WLC	172.20.226.131
Secondary Controller	WLC-9800	172.20.226.132
Tertiary Controller		

AP failover priority: Low

CLI Commands:

```
WLC#ap name 00f2.8b26.8a30 controller ?
  primary    Configure primary controller
  secondary  Configure secondary controller
  tertiary   Configure tertiary controller

WLC#ap name 00f2.8b26.8a30 priority ?
  <1-4>  Enter priority number
```

Image Upgrade with N+1 deployment

Zero downtime network upgrade is a challenge for Wireless Networks. The reason is that these networks are made up of a set of interlocked devices, WLCs and a set of APs, which all need to be up to keep the network operational.

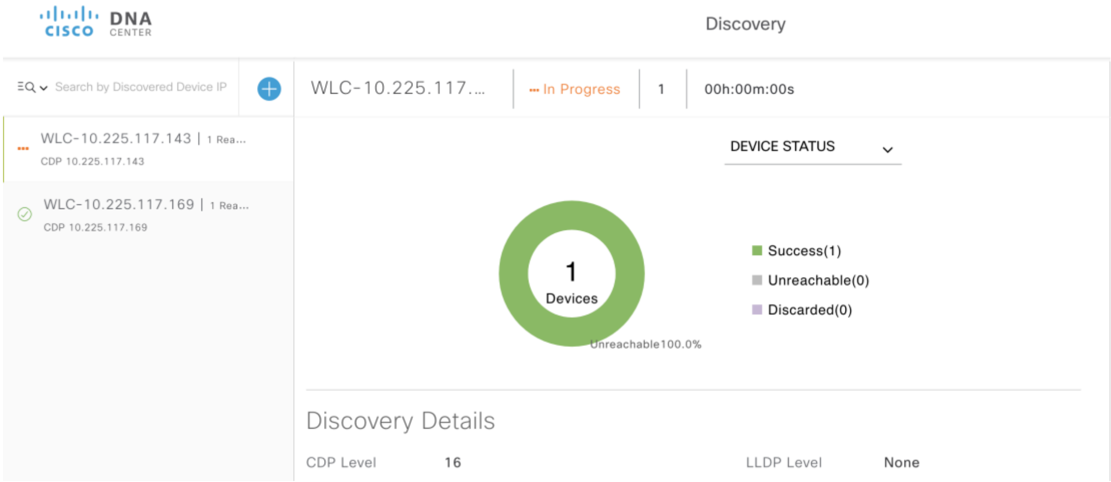
The advent of Rolling AP Upgrade opens up new possibilities for upgrading the controller code in a network without bringing the network down using an N+1 controller. This can effectively achieve a Zero Downtime network upgrade in a N+1 deployment.
The idea here is to upgrade access points in a wireless network in a staggered manner, using the same Rolling AP update infrastructure as described earlier in this document, such that an appropriate number of APs are always up and running in the network and providing RF coverage to clients. For N+1 Rolling AP Upgrade to work seamlessly it is essential that the WLCs be part of the same mobility group and have the same WLAN configuration.

This is explained in detail in the Patching guide here:
https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-ha-rau-apsp-apdp-issu-rel-17-1.pdf

Cisco DNA Center Configuration for N+1 High Availability

Cisco DNA Center supports Primary and Secondary configurations for N+1 HA. The below sequence outlines the workflow to configure N+1 High Availability using Cisco DNA Center

Step 1: Discover both the primary and secondary WLC devices.
Check for network connectivity between these devices



WLC-10.225.117.... ··· In Progress | 1 | 00h:00m:00s

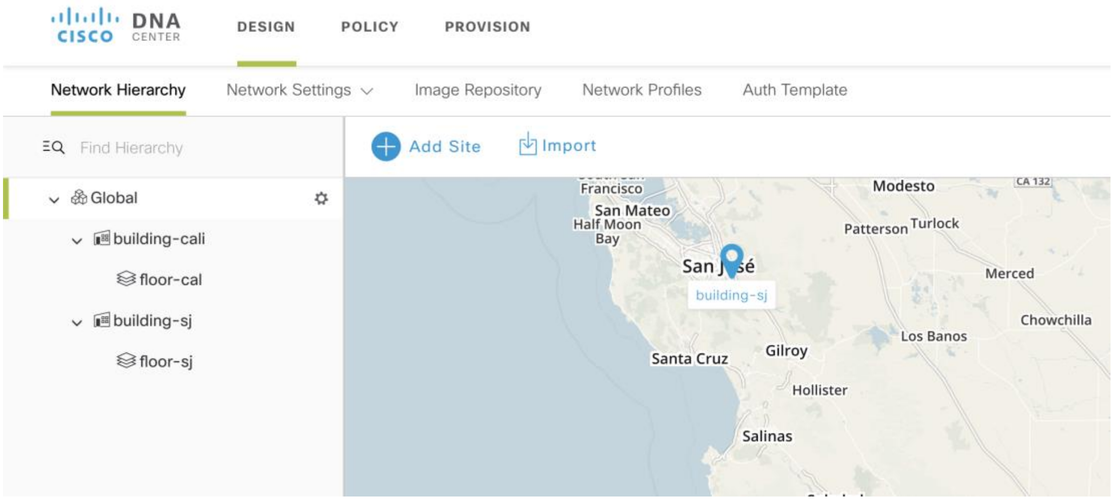
WLC-10.225.117.143 | 1 Rea...
CDP 10.225.117.143

WLC-10.225.117.169 | 1 Rea...
CDP 10.225.117.169

Discovery Details

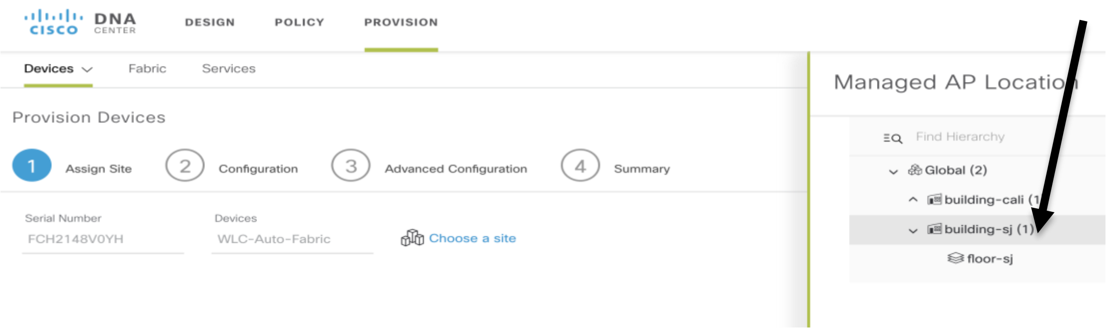
CDP Level	16	LLDP Level	None

Step 2: Create buildings where the access points will be connecting to the primary and secondary controllers. In the example below the two buildings, building-sj and building-cali are created where building-sj will be a Primary managed location for WLC-1 and same will be a Secondary managed location for WLC-2.
Building-cali is configured as only a primary managed location for WLC-2.



Step3: Provision the Primary device WLC-1. APs in building-sj are provisioned to be managed by WLC-1

Select the building-sj primary managed location



DNA CENTER | DESIGN | POLICY | PROVISION

Devices | Fabric | Services

Provision Devices

1 Assign Site | 2 Configuration | 3 Advanced Configuration | 4 Summary

Serial Number	Devices	
FCH2148V0YH	WLC-Auto-Fabric	Choose a site

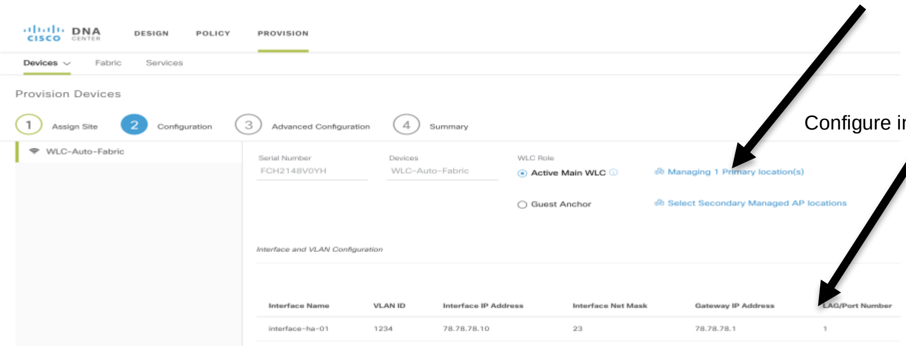
Managed AP Location

Find Hierarchy

- Global (2)
  - building-cali (1)
  - building-sj (1)
    - floor-sj

Primary device has 1 managed primary

Configure interface and



DNA CENTER | DESIGN | POLICY | PROVISION

Devices | Fabric | Services

Provision Devices

1 Assign Site | 2 Configuration | 3 Advanced Configuration | 4 Summary

WLC-Auto-Fabric

Serial Number: FCH2148V0YH

Devices: WLC-Auto-Fabric

WLC Role

● Active Main WLC — Managing 1 Primary location(s)

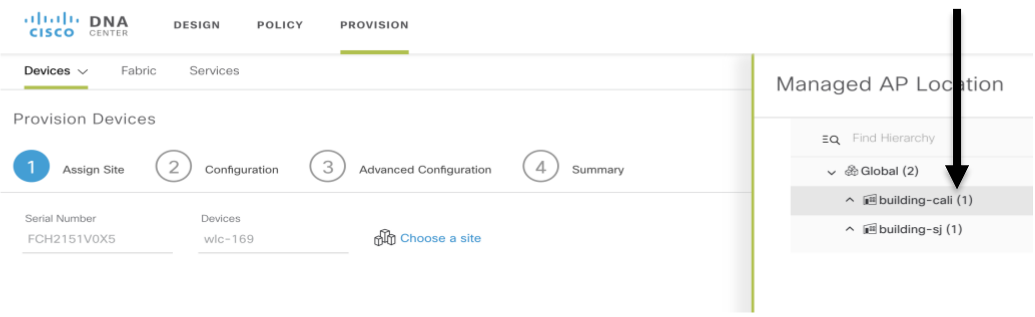
○ Guest Anchor — Select Secondary Managed AP locations

Interface and VLAN Configuration

Interface Name	VLAN ID	Interface IP Address	Interface Net Mask	Gateway IP Address	LAG/Port Number
interface-ha-01	1234	78.78.78.10	23	78.78.78.1	1

Step 4: Provision the Secondary device WLC-2. In this example, WLC-2 is the primary device for building-cali and secondary device for building-sj. So, building-sj APs have Primary as WLC-1 and secondary N+1 as WLC-2

Secondary device has 1 managed primary location as building-cali
And one secondary managed location as building-sj



DNA CENTER | DESIGN | POLICY | PROVISION

Devices | Fabric | Services

Provision Devices

1 Assign Site | 2 Configuration | 3 Advanced Configuration | 4 Summary

Serial Number	Devices	
FCH2151V0X5	wlc-169	Choose a site

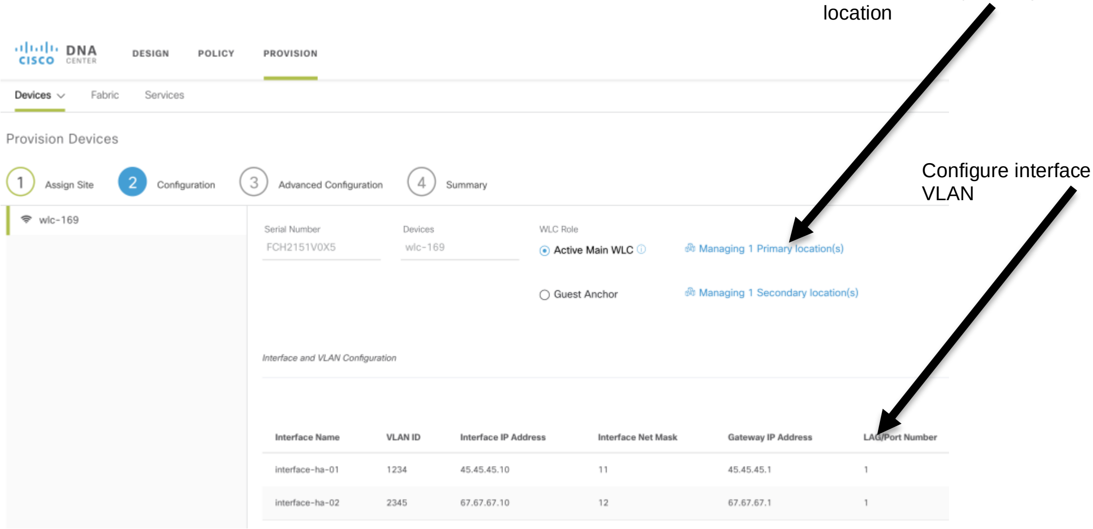
Managed AP Location

Find Hierarchy

- Global (2)
  - building-cali (1)
  - building-sj (1)

Secondary device has 1 managed primary location and 1 secondary Managed location

Configure interface and VLAN



Provision Devices

1 Assign Site · 2 Configuration · 3 Advanced Configuration · 4 Summary

wlc-169

Serial Number: FCH2151V0X5

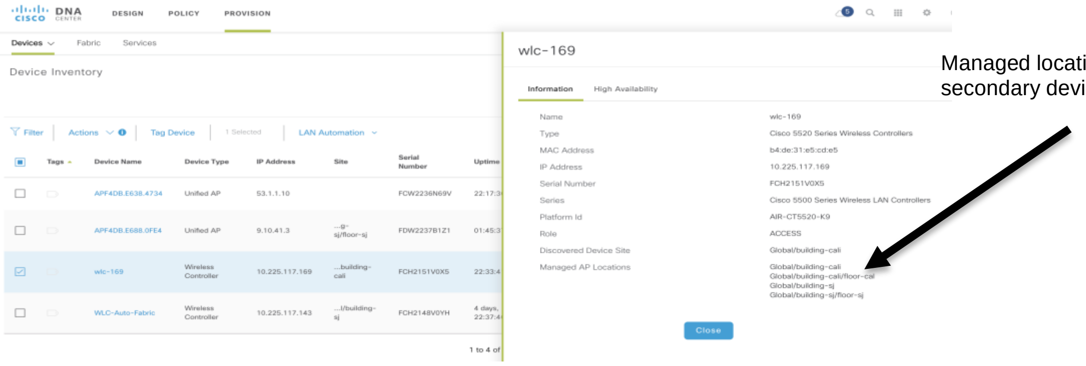
Devices: wlc-169

WLC Role:
● Active Main WLC — Managing 1 Primary location(s)
○ Guest Anchor — Managing 1 Secondary location(s)

Interface and VLAN Configuration

Interface Name	VLAN ID	Interface IP Address	Interface Net Mask	Gateway IP Address	LAG/Port Number
interface-ha-01	1234	45.45.45.10	11	45.45.45.1	1
interface-ha-02	2345	67.67.67.10	12	67.67.67.1	1

Managed locations of secondary device



Device Inventory

	Tags	Device Name	Device Type	IP Address	Site	Serial Number	Uptime
□		APF4DB.E638.4734	Unified AP	53.1.1.10		FCW2236N69V	22:17:3
□		APF4DB.E688.0FE4	Unified AP	9.10.41.3	...g-sj/floor-sj	FDW2237B1Z1	01:45:3
☑		wlc-169	Wireless Controller	10.225.117.169	...building-cali	FCH2151V0X5	22:33:4
□		WLC-Auto-Fabric	Wireless Controller	10.225.117.143	...l/building-sj	FCH2148V0YH	4 days, 22:37:4

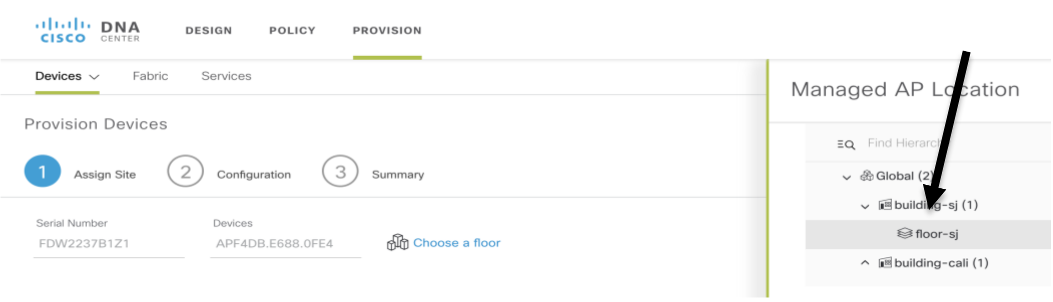
1 to 4 of

wlc-169

Name	wlc-169
Type	Cisco 5520 Series Wireless Controllers
MAC Address	b4:de:31:e5:cd:e5
IP Address	10.225.117.169
Serial Number	FCH2151V0X5
Series	Cisco 5500 Series Wireless LAN Controllers
Platform Id	AIR-CT5520-K9
Role	ACCESS
Discovered Device Site	Global/building-cali
Managed AP Locations	Global/building-cali Global/building-cali/floor-cal Global/building-sj Global/building-sj/floor-sj

Step 5: Verify AP Provisioning Summary

Selecting the floor from primary



Provision Devices

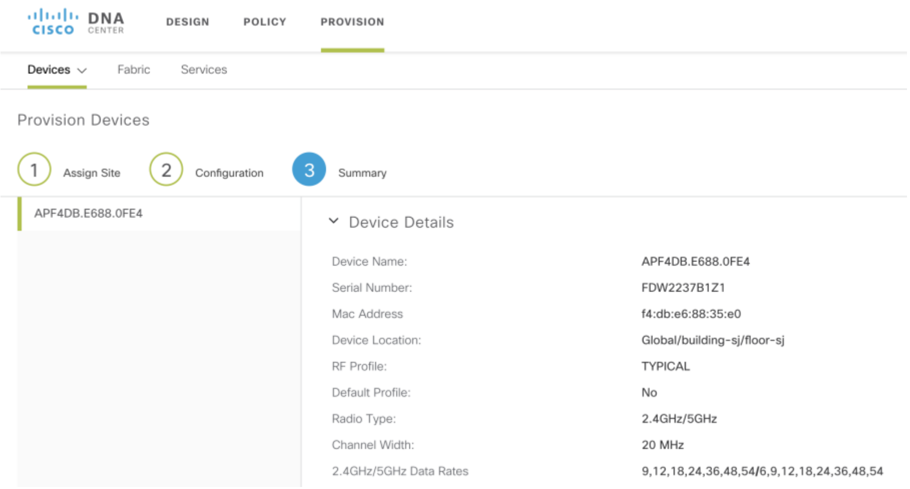
1 Assign Site · 2 Configuration · 3 Summary

Serial Number: FDW2237B1Z1

Devices: APF4DB.E688.0FE4

Choose a floor

Managed AP Location



Device Name:	APF4DB.E688.0FE4
Serial Number:	FDW2237B1Z1
Mac Address	f4:db:e6:88:35:e0
Device Location:	Global/building-sj/floor-sj
RF Profile:	TYPICAL
Default Profile:	No
Radio Type:	2.4GHz/5GHz
Channel Width:	20 MHz
2.4GHz/5GHz Data Rates	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

Licensing

- With Catalyst 9800 since Smart Licensing is mandatory, only as many licenses as the total number of APs in the network are required.
- When APs failover from primary to secondary and tertiary controllers, the smart licensing infrastructure seamless handles the failover since the AP MAC is sent in the entitlement request to the CSSM portal.
- N+1 HA is part of DNA Essentials Licensing Tier.
- There is no HA-SKU on the Catalyst 9800 wireless controllers.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN

ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco Copyright