

Implement Software-Defined Access for Wireless with DNAC

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[SD-Access](#)
[SD-Access Wireless Architecture](#)
[Overview](#)
[SDA Roles & Terminology](#)
[Underlay and Overlay Networks](#)
[Basic Workflows](#)
[AP join](#)
[Client Onboard](#)
[Client Roams](#)
[Configure](#)
[Network Diagram](#)
[WLC Discovery & Provision in DNA Center](#)
[Add WLC](#)
[Add Access Points](#)
[Create SSID](#)
[Provision WLC](#)
[Provision Access Points](#)
[Create Fabric Site](#)
[Add WLC to Fabric](#)
[AP Join](#)
[Client Onboard](#)
[Verify](#)
[Verify fabric configuration on WLC and DNAC](#)
[Troubleshoot](#)
[Client does not get IP address](#)
[SSID is not broadcasted](#)
[Related Information](#)

Introduction

This document describes how to implement SDA for wireless technology related to fabric enabled WLC and access LAP on DNAC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 Wireless LAN Controllers (WLC) configuration

- Lightweight Access Points (LAPs)
- DNA Center (DNAC)

Components Used

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

- 9800-CL WLC Cisco IOS® XE, Version 17.9.3
- Cisco Access Points: 9130AXE, 3802E, 1832I
- DNA Center (DNAC) version 2.3.3.7

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.

SD-Access

Software-Defined Access establishes and automatically enforces security policies across the network, with dynamic rules and automated segmentation, and allows the end user to control and configure how the users connect to their network. SD-Access establishes an initial level of trust with each endpoint that is connected, and continuously monitors it to re-verify its level of trust. If an endpoint behaves not normally or a threat is detected, the end user can immediately contain it and take action, before breach takes place, reduces business risk, and protects its resources. Fully integrated solution and easy to deploy and configure on both new and deployed networks.

SD-Access is a Cisco technology that is an evolution of the traditional campus network that delivers intent-based networking (IBN) and central policy control with the use of Software-Defined Networking (SDN) components.

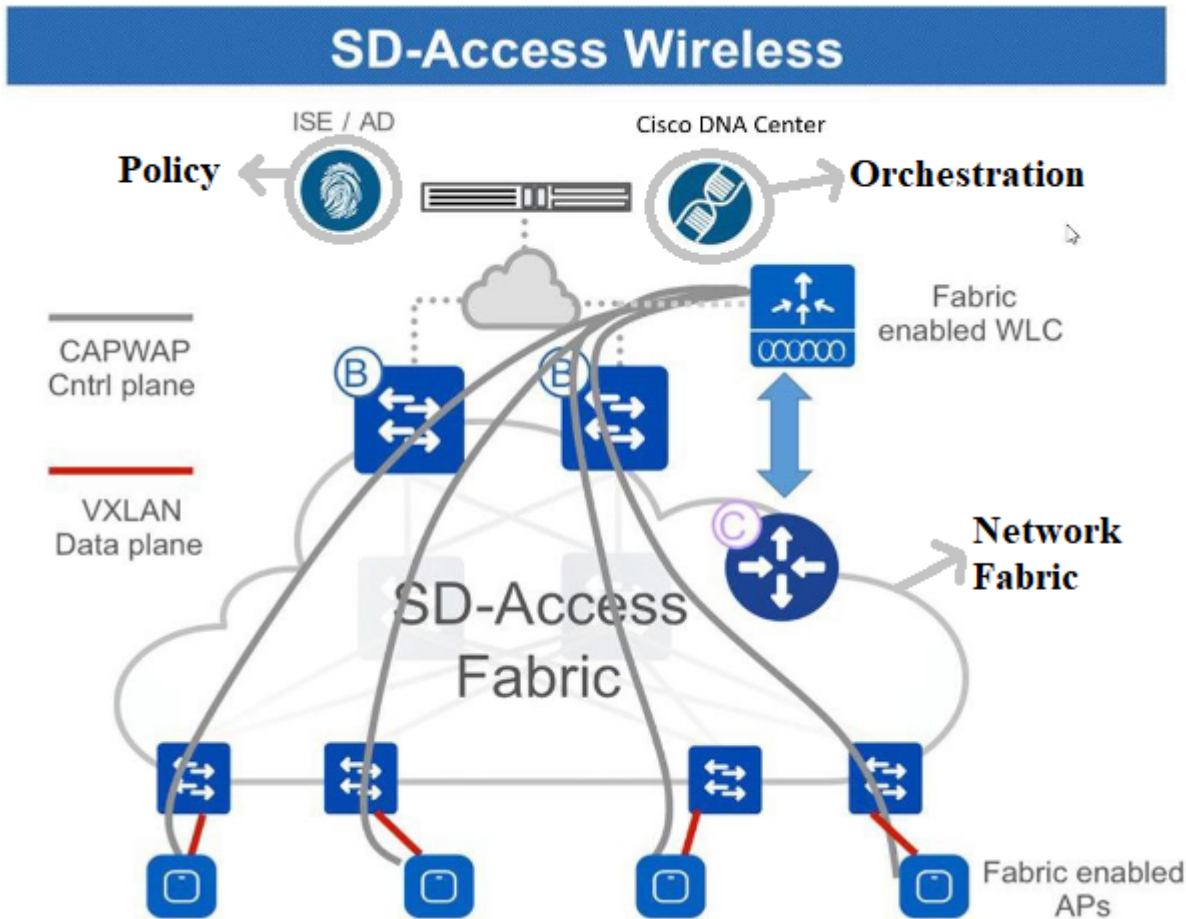
Three network-centric pillars of SD-Access:

1. **A network fabric:** It is an abstraction of the network itself that supports programmable overlays and virtualization. The network fabric supports both wired and wireless access, allows it to host multiple logical networks that are segmented from one other and are defined by business intent.
2. **Orchestration:** DNA Center is the orchestrator engine of SDA. DNA Center functions like an SDN controller. It implements policies and configuration changes in the fabric. Also incorporates a tool that supports network design and supports real-time network telemetry operations and performance analytics through DNA Assurance. The role of DNA Center is to orchestrate the network fabric to deliver policy changes and network intent for security, quality of service (QoS), and microsegmentation.
3. **Policy:** Identity Services Engine (ISE) is the tool that defines network policy. ISE organizes how the devices and nodes are segmented into virtual networks. ISE also defines scalable group tags (SGTs) that are used by access devices to segment user traffic as it enters the fabric. SGTs are responsible to enforce the microsegmentation policy defined by ISE.

SDA is built on centralized orchestration. The combinations of DNA Center as the programmable orchestration engine, ISE as the policy engine, and a new generation of programmable switches makes it a much more flexible and manageable fabric system than anything that has come before.

Note: This document deals specifically with SD-Access Wireless.

The network fabric is composed of these elements:

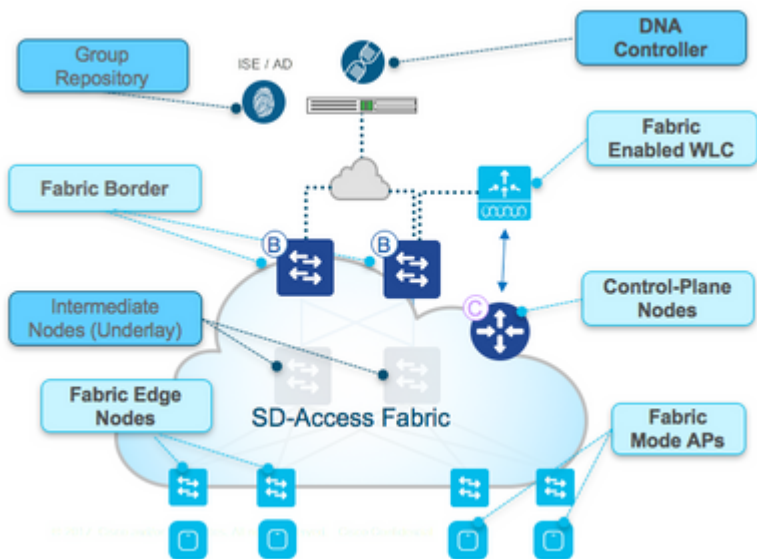


Elements of Network Fabric

The wireless integration to fabric leads to several advantages for the wireless network for example: addressing simplification, mobility with stretched subnets across physical locations; and microsegmentation with centralized policy that is consistent across both of the wired and wireless domains. It also enables the controller to shed data plane to forward duties while it continues to function as the centralized services and control plane for the wireless network. Thus wireless controller scalability is actually increased because it no longer needs to process data plane traffic, similar to the FlexConnect model.

SD-Access Wireless Architecture

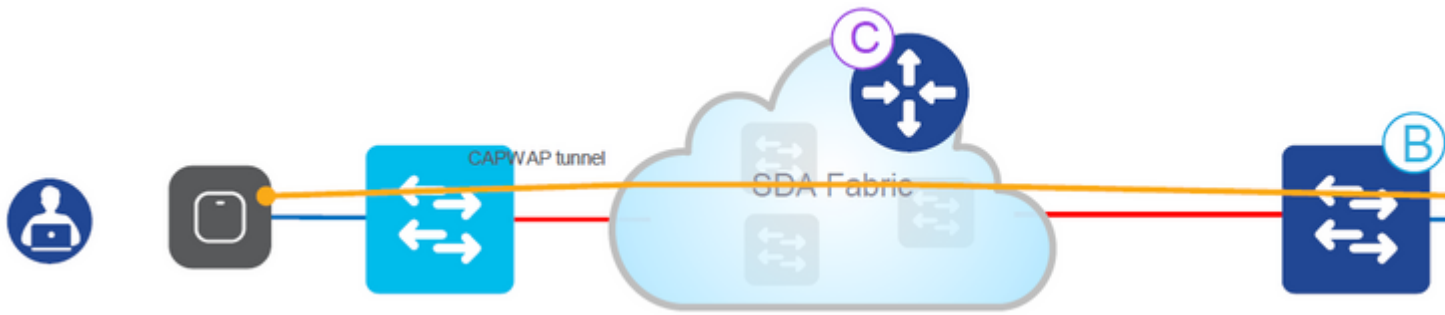
Overview



SDA Overview

There are two primary SDA supported wireless deployment models:

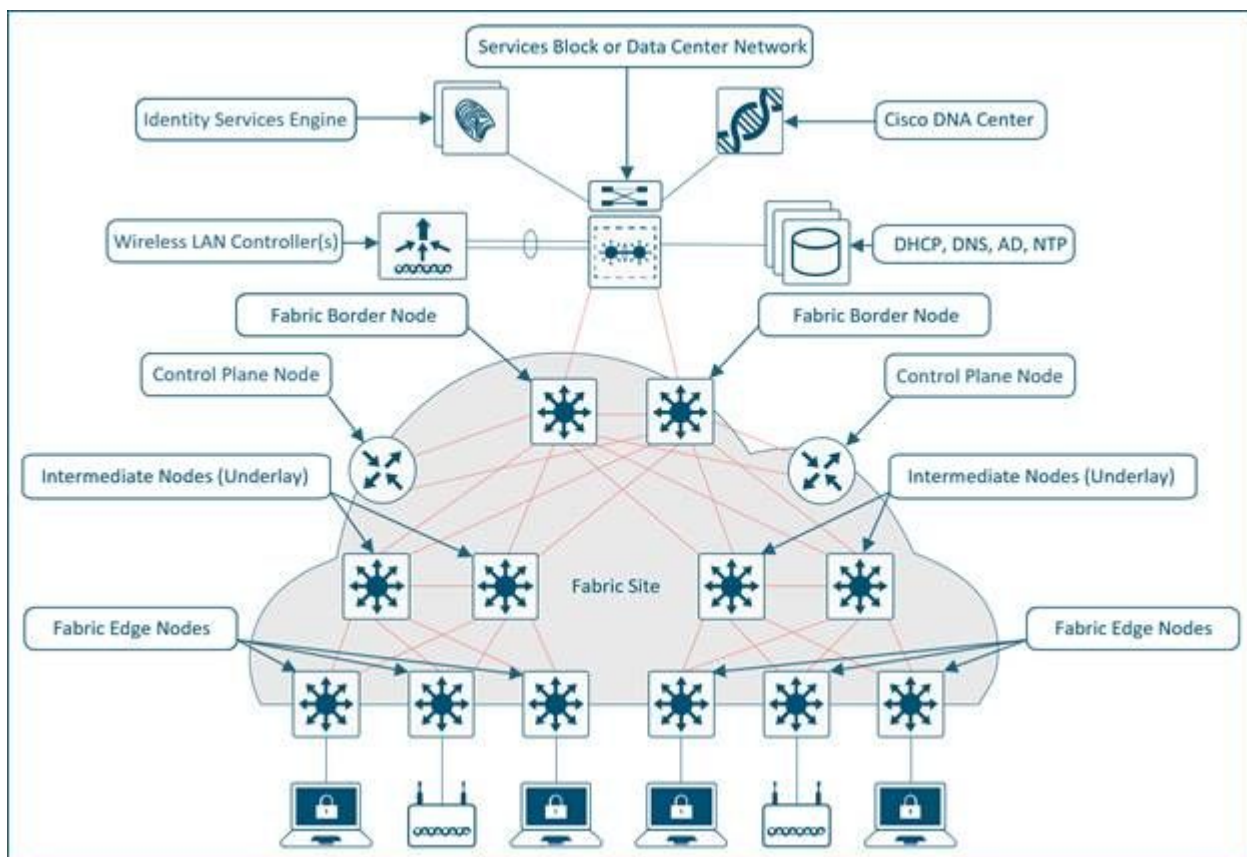
One is an over-the-top (OTT) method, a traditional CAPWAP deployment connected on top of a fabric wired network. The SDA fabric transports the CAPWAP control and data plane traffic to the wireless controller:



Over-The-Top Method

In this deployment model, the SDA fabric is a transport network for wireless traffic (a model often deployed in migrations). The AP works very similarly to classic Local mode: both CAPWAP control and data planes terminate on the controller, that means the controller does not directly participate in the fabric. This model is often used when wired switches are first migrated to the SDA fabric but the wireless network is not yet ready for full fabric overlay integration.

The other deployment models the fully integrated SDA model. The wireless network is fully integrated to the fabric and participates in overlays, it allows different WLANs to be part of different virtual networks (VNs). The wireless controller only manages the CAPWAP control plane (to manage APs), and the CAPWAP data plane does not come to the controller:



Fully Integrated SDA Model

The wireless data plane is handled similarly to wired switches - each AP encapsulates data in VXLAN and sends it to a fabric edge node where it is then sent across the fabric to another edge node. The wireless controllers must be configured as fabric controllers, which is a modification from their normal operation.

Fabric enabled controllers communicate with the fabric control plane, it registers Layer 2 client MAC

addresses, and Layer 2 Virtual Network Identifier (VNI) information. The APs are responsible for communication with wireless endpoints, and assist the VXLAN data plane by encapsulation and de-encapsulation traffic.

SDA Roles & Terminology

The network fabric is composed of these elements:

- **Control-Plane Node:** This is the location mapping system (host database) that is part of the Location Separator Protocol (LISP) control plane, that manages endpoint identity (EID) to location relationships (or device relationships). Either the control plane can be a dedicated router that provided control plane functions or it can coexist with other fabric network elements.
- **Fabric Border Nodes:** Typically a router that functions at the border between external networks and the SDA fabric, that provides routing services to the virtual networks in the fabric. It connects external Layer 3 network(s) to the SDA fabric.
- **Fabric Edge Nodes:** Device within the fabric that connects non-fabric devices, such as switches, APs, and routers to the SDA fabric. These are the nodes that create the virtual overlays tunnels and VNs with Virtual eXtensible LAN (VXLAN) and impose the SGTs on fabric-bound traffic. The networks on both sides of the fabric edge are inside the SDA network. They connect wired endpoints to the SD-Access fabric.
- **Intermediate Nodes:** These nodes are inside the core of the SDA fabric and connect to either edge or border nodes. The intermediate nodes simply forward SDA traffic as IP packets, unaware that there are multiple virtual networks involved.
- **Fabric WLC:** Wireless controller that is fabric enabled and participates in the SDA control plane but does not process the CAPWAP data plane.
- **Fabric mode APs:** Access points that are fabric enabled. Wireless traffic is VXLAN-encapsulated at the AP, which allows it to be sent into the fabric through an edge node.
- **DNA Center (DNAC):** The Enterprise SDN controller for the Software Defined Access (SDA) fabric overlay network, and is responsible for both automation and assurance tasks. It can also be utilized for some automation and related tasks for the network devices that form the underlay (that is non-SDA related) as well.
- **ISE:** The Identity Services Engine (ISE) is an enhanced policy platform that can serve a variety of roles and functions, not the least of which is that of the Authentication, Authorization and Accounting (AAA) server. ISE typically interacts with Active Directory (AD), but users can be configured locally as well on ISE itself for smaller deployments.

Note: The control plane is a critical infrastructure piece of the SDA architecture, so it is recommended to be deployed in a resilient way.

Underlay and Overlay Networks

The SDA architecture utilizes fabric technology that supports programmable virtual networks (overlay networks) that run on a physical network (an underlay network).

A fabric is an Overlay.

An Overlay network is a logical topology used to virtually connect devices, built over an arbitrary physical Underlay topology. It uses alternate forward attributes to provide additional services that are not provided by the Underlay. It is created on top of the underlay to create one or more virtualized and segmented networks. Due to the software-defined nature of overlays, it is possible to connect them in very flexible ways without

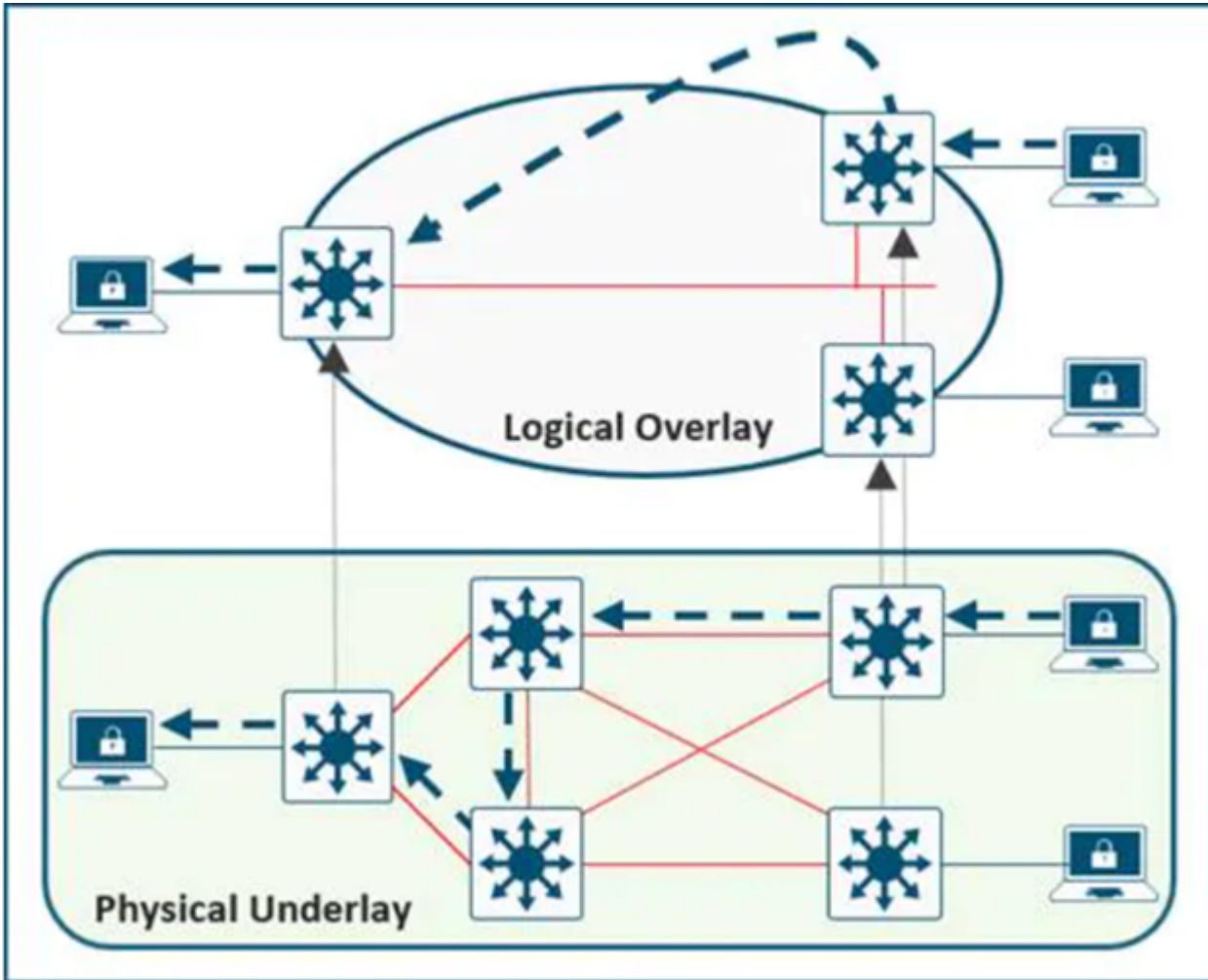
the constraints of physical connectivity. It is an easy way to enforce security policies, since the overlay can be programmable to have a single physical exit point (the fabric border node), and one firewall can be used to protect the networks behind it (whether they can be located). Overlay encapsulates traffic with the use of VXLAN. VXLAN encapsulates complete Layer 2 frames for transport across the underlay with each overlay network identified by a VXLAN network identifier (VNI). Overlay fabrics tend to be complex and require a significant amount of administrator overhead on new virtual networks deployed, or to implement security policies.

Examples of network overlays:

- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

An Underlay network is defined by the physical nodes such as switches, routers, and wireless APs that are used to deploy the SDA network. All network elements of the underlay must establish IP connectivity via the use of a routing protocol. While the underlay network is not likely to use the traditional access, distribution, core model, it must use a well-designed Layer 3 foundation that delivers robust performance, scalability, and high availability.

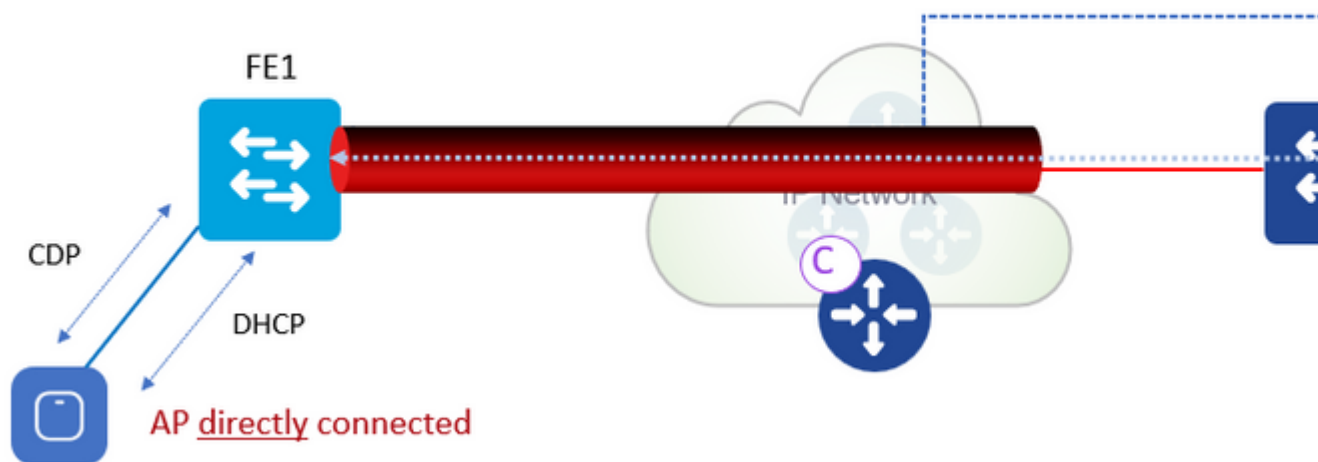
Note: SDA supports IPv4 in the underlay network and IPv4 and/or IPv6 in overlay networks.



Underlay and Overlay Networks

Basic Workflows

AP join



AP Join Workflow

AP Join Workflow:

1. Admin configures AP pool in DNAC in INFRA_VN. Cisco DNA Center pre-provision a configuration on all the Fabric Edge Node to automatically onboard APs.
2. AP is plugged in and powers up. Fabric Edge discovers it™s an AP via CDP and applies the macro to assign (or the interface template) the switch port the the right VLAN.
3. AP gets an IP address via DHCP in the overlay.
4. Fabric Edge registers APs IP address and MAC (EID) and updates the Control Plane (CP).
5. AP learns WLCs IP with traditional methods. Fabric AP joins as a Local mode AP.
6. WLC checks if it is fabric-capable (Wave 2 or Wave 1 APs).
7. If AP is supported for Fabric, WLC queries the CP to know if AP is connected to Fabric.
8. Control Plane (CP) replies to WLC with RLOC. This means AP is attached to Fabric and is shown as "Fabric enabled".
9. WLC does a L2 LISP registration for AP in CP (that is AP "special" secure client registration). This is used to pass important metadata information from WLC to the Fabric Edge.
10. In response to this proxy registration, Control Plane (CP) notifies Fabric Edge and pass the metadata received from WLC (flag that says it is an AP and the AP IP address).
11. Fabric Edge processes the information, it learns it is an AP and creates a VXLAN tunnel interface to the specified IP (optimization: switch side is ready for clients to join).

The debug/show commands can be used to verify and validate the AP join workflow.

Control Plane

```
debug lisp control-plane all
```

```
show lisp instance-id <L3 instance id> ipv4 server (must show the AP IP address registered by edge switch
```

```
show lisp instance-id <L2 instance id> ethernet server (must show the AP radio as well as ethernet mac-addr
```

◆roam-to◆ switch) to add the client MAC to the forward table that points to VXLAN tunnel.

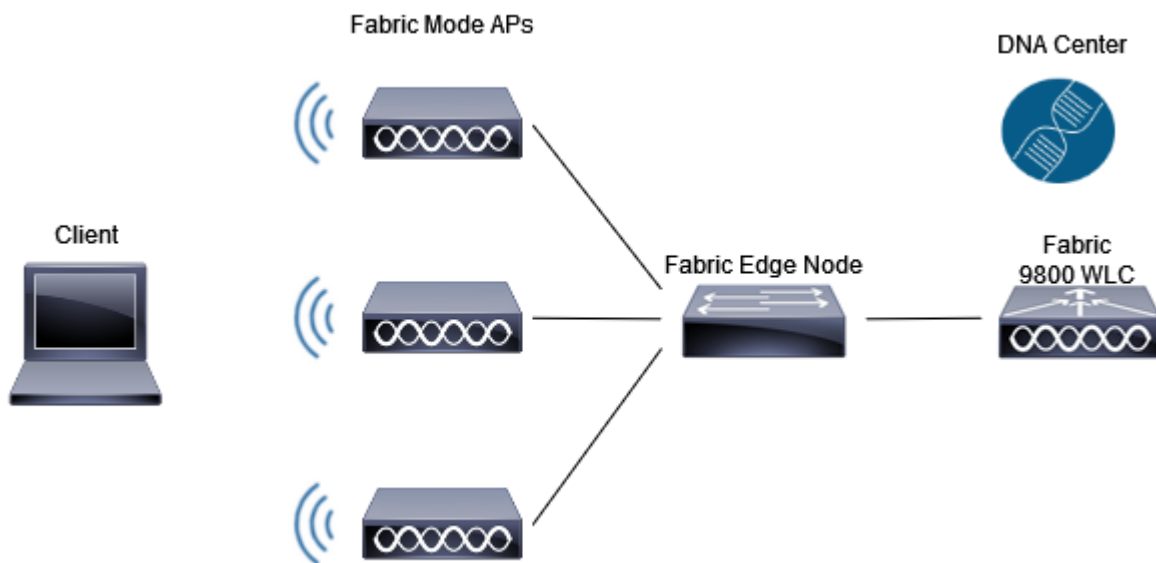
- Fabric Edge FE1 (◆roam-from◆ switch) to do clean up for the wireless client.

5. Fabric Edge update the L3 entry (IP) in CP data base upon it receives traffic.

6. Roam is Layer 2 as Fabric Edge 2 has the same VLAN interface (Anycast GW).

Configure

Network Diagram



Network Diagram

WLC Discovery & Provision in DNA Center

Add WLC

Step 1. Navigate to the location where you want to add the WLC. You can add a new building/floor.

Navigate to **Design > Network Hierarchy** and enter the building/floor, or you can create a new floor, as shown in the image:

and verify the string configured. You need to add the correct SNMP community string when you add the WLC on DNAC, and ensure that netconf-yang is enabled on the 9800 WLC with 'show netconf-yang status' commands. At the end click Add:

SNMP Mode

ENABLED

General

SNMP Views

Community Strings

V3 User Groups

V3 Users

Hosts

Wireless

+ Add

× Delete

	Community Name	Access Mode
<input type="checkbox"/>	private	Read/Write
<input type="checkbox"/>	public	Read Only

1 / 10

SNMP Configuration

Step 5. Add the WLC IP address, CLI credentials (the credentials DNAC uses to log in to the WLC and these must be configured on the WLC before add it to DNAC), the SNMP string and verify if the NETCONF port is configured on port 830:

Add Device

Device Controllability is **Enabled**. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. [Firepower Management more](#) | [Disable](#)

Type ⓘ

Network Device

Device IP / DNS Name*

10.48.39.186

Credentials

[Validate](#)

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

^ CLI*

Select global credential Add device specific credential

Username*

admin

Password*

Enable Password

WARNING: Do not use 'admin' as the username for your device CLI credentials, if you are using Cisco ISE as your AAA server. If you do, this can result in you not being able to login to

^ SNMP*

Select global credential Add device specific credential

Version*

V2C

Credential*

private | Write

: Do not forget to configure and associate AAA server for the SSID. The default method list is mapped if no AAA server are configured.

When you click next you can see advanced settings for your SSID:

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: Demo (Guest)

Fast Transition (802.11r)

Adaptive Enable Disable

Over the DS

11k

Neighbor List

Session Timeout

in (secs)*

1800

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout

Client User Idle Timeout(Default: 300 secs)*

300

Radius Client Profiling

NAS-ID

NAS-ID Opt 1

MFP Client Protection

Optional Required Disabled

Client Exclusion

Directed Multicast Service

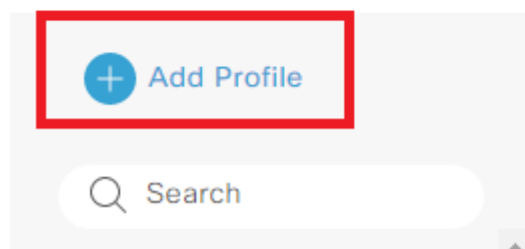
SSID Advanced Settings


Step 3. After the creation of the SSID, you need to associate it to a profile. Click Add Profile:

Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile:

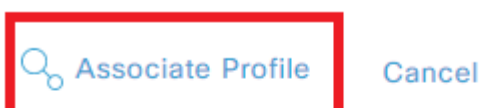
SSID Name: Demo (Guest)



 0 profile(s) associated.

Add Profile

Step 4. Give a name to the profile, select Fabric and at the end click on Associate Profile:



: When provision the APs, which are already part of the configured floor for the selected RF profile is be processed and rebooted.

The APs are now provisioned.

Step 6. On the WLC side, navigate to **Configuration > Wireless > Access Points**. Verify that the AP tags were pushed from the DNAC:

▼ All Access Points

Total APs : 3

Misconfigured APs
Tag : 0 Country Code : 0 LSC

Country Code Misconfigured	LSC Fallback Misconfigured	Policy Tag	Site Tag	RF Tag
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile
No	No	PT_Lisbo_Lisbo_Flor1_45ce7	ST_Lisbo_Lisbon_3e5f5_0	DemoRFProfile

Navigation: 1 / 10

Tags on APs

Step 7. Navigate to **Configuration > Tags & Profiles > WLANs** and verify that the SSID was pushed from DNAC:

+ Add × Delete Clone Enable WLAN Disable WLAN

Selected WLANs : 0

Status	Name	ID	SSID
	Demo_Global_NF_986e8d08	17	Demo

Navigation: 1 / 10

WLAN

Create Fabric Site

Step 1. Navigate to **Provision > Fabric Sites**. Create a fabric site:

Cisco DNA Center

Virtual Networks	Fabric Sites	Transits
------------------	---------------------	----------

. Select one AP from the list. Verify that the Fabric Status is Enabled, the IP address of the control plane and the control plane name:

Edit AP

Configuration ▾

▼ All Access Points

Total APs : 3

AP Name	AP Mode	Operation Status	Fabric Status	CleanAir NSI Key	RLOC IP	Control Plane Name	Primary Software Version	Predownloaded Status	Predownloaded Version	Next Retry Time	Boot Version	IOS Version	Mini IOS Version
AP0C75-BDB...	Local	Registered	Enabled		10.XX.XX.XX	default-control-plane							
3800E-I													

Verify AP Fabric Status

Client Onboard

Step 1. Add the pool to Virtual Network and verify that Layer-2 Extension toggle is ON to enable L2 LISP and Layer 2 subnet extension on the client Pool/subnet. In DNA Center 1.3.x you cannot disable it.

Layer 2 Only ⓘ Layer 3 Only ⓘ

IP Address Pool
S1_CLIENT-IP (10.0.0.0/24) ▾

VLAN
39

VLAN Name
VLAN0039 Auto generate VLAN name

Security Group ▾ Traffic **Data** ▾ IP-directed broadcast ⓘ

Layer-2 Flooding ⓘ Critical Pool ⓘ **Wireless Pool**

Bridge-Network Virtual Machine ⚠

Add IP Address Pool

Step 2. Verify if the Layer-2 Extension and Wireless Pool are enabled.

Edit Virtual Network: S1_CORP_VN