



Software-Defined Access Wireless

- [Information about Software-Defined Access Wireless, on page 1](#)
- [Configure SD-access wireless, on page 4](#)
- [Verifying SD-Access Wireless, on page 9](#)

Information about Software-Defined Access Wireless

The Enterprise Fabric provides end-to-end enterprise-wide segmentation, flexible subnet addressing, and controller-based networking with uniform enterprise-wide policy and mobility. It moves the enterprise network from current VLAN-centric architecture to a user group-based enterprise architecture, with flexible Layer 2 extensions within and across sites.

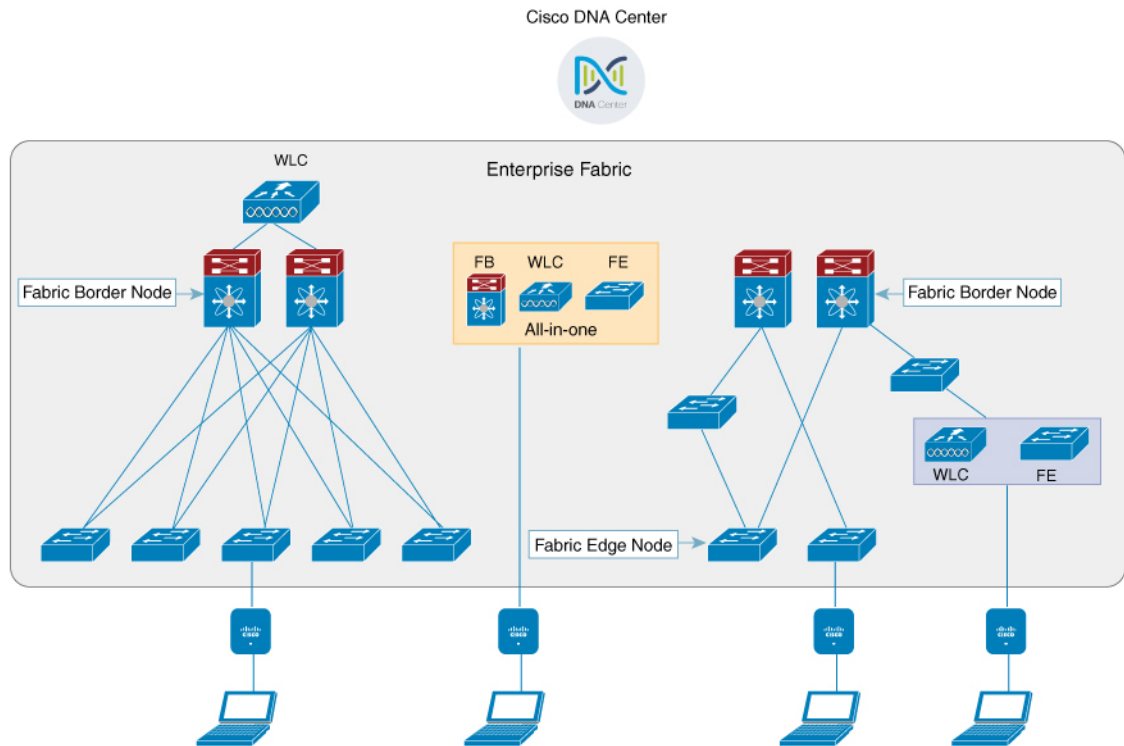
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which makes the network appear as a single virtual entity without using clustering technologies.

The following definitions are used for fabric nodes:

- **Enterprise Fabric:** A network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device.
- **Fabric Domain:** An independent operation part of the network. It is administered independent of other fabric domains.
- **End Points:** Hosts or devices that connect to the fabric edge node are known as end points (EPs). They directly connect to the fabric edge node or through a Layer 2 network.

The following figure shows the components of a typical SD-Access Wireless. It consists of Fabric Border Nodes (BN), Fabric Edge Nodes (EN), Wireless Controller, Cisco Catalyst Center, and Host Tracking Database (HDB).

Figure 1: Software-Defined Access Wireless



The figure covers the following deployment topologies:

- All-in-one Fabric—When we have all Fabric Edge, Fabric Border, Control-Plane and controller functionality enabled on a Cat 9K switch. This topology is depicted in the mid part of the figure.
- Split topology—When we have Fabric Border, or Control Plane, or controller on a Cat 9K switch with separate Fabric Edge. This topology is depicted in the left-most part of the figure.
- Co-located Fabric Edge and Controller—When we have Fabric Edge and controller on a Cat 9K switch. This topology is depicted in the right-most part of the figure.

Cisco Catalyst Center: Is an open, software-driven architecture built on a set of design principles with the objective of configuring and managing Cisco Catalyst 9800 Series Wireless Controllers.

Control Plane: This database allows the network to determine the location of a device or user. When the EP ID of a host is learnt, other end points can query the database about the location of the host. The flexibility of tracking subnets helps in summarization across domains and improves the scalability of the database.

Fabric Border Node (Proxy Egress Tunnel Router [PxTR or PITR/PETR] in LISP): These nodes connect traditional Layer 3 networks or different fabric domains to the enterprise fabric domain. If there are multiple fabric domains, these nodes connect a fabric domain to one or more fabric domains, which could be of the same or different type. These nodes are responsible for translation of context from one fabric domain to another. When the encapsulation is the same across different fabric domains, the translation of fabric context is generally 1:1. The fabric control planes of two domains exchange reachability and policy information through this device.

Fabric Edge Nodes (Egress Tunnel Router [ETR] or Ingress Tunnel Router [ITR] in LISP): These nodes are responsible for admitting, encapsulating or decapsulating, and forwarding of traffic from the EPs. They lie at the perimeter of the fabric and are the first points of attachment of the policy. EPs could be directly or indirectly attached to a fabric edge node using an intermediate Layer 2 network that lies outside the fabric domain. Traditional Layer 2 networks, wireless access points, or end hosts are connected to fabric edge nodes.

Wireless Controller: The controller provides AP image and configuration management, client session management and mobility. Additionally, it registers the mac address of wireless clients in the host tracking database at the time of client join, as well as updates the location at the time of client roam.

Access Points: AP applies all the wireless media specific features. For example, radio and SSID policies, webauth punt, peer-to-peer blocking, and so on. It establishes CAPWAP control and data tunnel to controller. It converts 802.11 data traffic from wireless clients to 802.3 and sends it to the access switch with VXLAN encapsulation.

The SDA allows to simplify:

- Addressing in wireless networks
- Mobility in wireless networks
- Guest access and move towards multi-tenancy
- Leverage Sub-net extension (stretched subnet) in wireless network
- Provide consistent wireless policies



Note Role co-location between wireless controller and fabric edge is supported.

Platform Support

Table 1: Supported Platforms for Software-Defined Access Wireless

Platforms	Support
Catalyst 9300	Yes
Catalyst 9400	Yes
Catalyst 9500H	Yes
Cisco Catalyst 9800 Series Wireless Controller for Cloud	Yes
Cisco Catalyst 9800-40 Series Wireless Controller	Yes
Cisco Catalyst 9800-80 Series Wireless Controller	Yes

Table 2: Multi-Instance Support

Multi-instance	Support
Multiple LISP sessions	Yes

Multi-instance	Support
Emulated database support	Yes
Client roaming between WNCd instances	Yes

Table 3: Feature Support

Feature	Support
Inter-WLC roam for IRCM	Only L2 mobility is supported as VLAN is stretched across the fabric.
DNS-IPv4-ACL	<ul style="list-style-type: none"> • ACLs are enforced at AP. • Controller needs to push the DNS-ACL information to AP.
IPv6 ACL for clients	Yes. Open, 802.11x, WebAuth, PSK WLANs, IPv6 address visibility are also supported.
Location tracking/Hyperlocation	Yes
Multicast Video-Stream (IPv4)	Yes
Smart Licensing	Yes

Table 4: Outdoor Access Points Support

AP	Support
1542	Yes
1560	Yes

Configure SD-access wireless

Enable SD-Access wireless globally, you need to run the **wireless fabric** configuration command. During SD-Access Wireless provisioning, ensure that L2-VNID value is unique.

Configure default map server (GUI)

Set up the default map server. This action enables the wireless fabric network to properly associate controllers and devices with their respective mapping information.

Procedure

Step 1 Click **Configuration > Wireless Plus > Fabric > Fabric Configuration**.

- Step 2** In the **Map Server** section, enter the IP address and preshared key details for Server 1.
- Step 3** (Optional) Specify the IP address and preshared key details to configure Server 2.
- Step 4** Click **Apply**.

The default map server settings are saved, enabling fabric devices to communicate and register with the specified servers.

Configure default map server (CLI)

Configure a default map server to ensure that wireless Fabric components in your Cisco network can register and operate as part of the control plane using commands.

Procedure

- Step 1** Enter the global configuration mode.

Example:

```
Device# configure terminal
```

- Step 2** Configure the default map server.

Example:

```
Device(config)# wireless fabric control-plane map-server-name
```

Here, *map-server-name* defines a pair of map servers.

- Step 3** Configure IP address for the default map server.

Example:

```
Device(config-wireless-cp)# ip address ip-address key user-password reenter-password
```

- Step 4** Return to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example:

```
Device(config-wireless-cp)# end
```

The default map server is configured. Wireless fabric components can now register with the control-plane infrastructure and exchange location and policy information for network operations.

```
Device# configure terminal
Device(config)# wireless fabric control-plane map-server-name
Device(config-wireless-cp)# ip address 200.0.0.0 key user-password user-password
Device(config-wireless-cp)# end
```

Configuring SD-Access Wireless Profile (GUI)

Procedure

- Step 1** Choose **Configuration** > **Wireless** > **Fabric**.
- Step 2** On the **Fabric** page, click the **Profiles** tab and click **Add**.
- Step 3** In the **Add New Profile** window that is displayed, specify the following parameters:
- Profile name
 - Description
 - L2 VNID; valid range is between 0 and 16777215
 - SGT tag; valid range is between 2 and 65519
- Step 4** Click **Save & Apply to Device**.
-

Configure SD-Access wireless profile (CLI)

Configure a wireless profile for SD-Access fabric deployment using commands.

Follow the procedure given below to configure SD-Access wireless profile:

Procedure

- Step 1** Enter the global configuration mode.
- Example:**
- ```
Device# configure terminal
```
- Step 2** Configure the SD-Access wireless profile parameters.
- Example:**
- ```
Device(config)# wireless profile fabric fabric-profile-name
```
- Step 3** Configure SGT tag.
- Example:**
- ```
Device(config-wireless-fabric)# sgt-tag sgt
```
- Here, *sgt* refers to the sgt tag value. The valid range is from 2-65519. The default value is 0.
- Step 4** Configure client L2-VNID.
- Example:**
- ```
Device(config-wireless-fabric)# client-l2-vnid client-l2-vnid
```
- Here, *client-l2-vnid* refers to the client L2-VNID value. The valid range is from 0-16777215.

- Step 5** Return to the privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Example:

```
Device(config-wireless-fabric)# end
```

Configuring Map Server in Site Tag (GUI)

Before you begin

Ensure that you have configured a control plane at the time of configuring Wireless Fabric.

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
- Step 2** On the **Manage Tags** page, click the **Site** tab.
- Step 3** Click the name of the site tag.
- Step 4** In the **Edit Site Tag** window, choose the Fabric control plane name from the **Control Plane Name** drop-down list.
- Step 5** Save the configuration.

Configuring Map Server in Site Tag (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 2	wireless tag site <i>site-tag</i> Example: Device(config)# wireless tag site default-site-tag	Configures site tag. Here, <i>site-tag</i> refers to the site tag name.
Step 3	fabric control-plane <i>map-server-name</i> Example: Device(config-site-tag)# fabric control-plane map-server-name	Configures fabric control plane details. Here, <i>map-server-name</i> refers to the fabric control plane name associated with the site tag.

	Command or Action	Purpose
Step 4	end Example: Device(config-site-tag)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Map Server per L2-VNID (GUI)

Procedure

-
- Step 1** Choose **Configuration > Wireless > Fabric**.
- Step 2** On the **Fabric Configuration** page in the **Fabric VNID Mapping** section, click **Add**.
- Step 3** In the **Add Client and AP VNID** window, specify a name for the Fabric, L2 VNID value (valid range is from 0 to 4294967295), control plane name.
- Step 4** Save the configuration.
-

Configuring Map Server per L2-VNID (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 2	wireless fabric name name l2-vnid l2-vnid-value l3-vnid l3-vnid-value ip network-ip subnet-mask control-plane-name control-plane-name Example: Device(config)# wireless fabric name fabric_name l2-vnid 2 l3-vnid 2 ip 122.220.234.0 255.255.0.0 control-plane-name sample-control-plane	Configures the map server to the VNID map table. <ul style="list-style-type: none"> • <i>name</i> refers to the fabric name. • <i>l2-vnid-value</i> refers to the L2 VNID value. The valid range is from 0 to 16777215. • <i>l3-vnid-value</i> refers to the L3 VNID value. The valid range is from 0 to 16777215. • <i>control-plane-name</i> refers to the control plane name.
Step 3	end Example: Device(config)# end	Returns to privileged EXEC mode.

Verifying SD-Access Wireless

You can verify the SD-Access wireless configurations using the following commands:

Table 5: Commands for Verifying SD-Access Wireless

Commands	Description
show wireless fabric summary	Displays the fabric status.
show wireless fabric vnid mapping	Displays all the VNID mapping details.
show wireless profile fabric detailed <i>fabric_profile_name</i>	Displays the details of a given fabric profile name.
show ap name AP_name config general	Displays the general details of the Cisco AP.
show wireless client mac MAC_addr detail	Displays the detailed information for a client by MAC address.
show wireless tag site detailed <i>site_tag</i>	Displays the detailed parameters for a site tag.

