Configuring Wireless Support in a LISP VXLAN Fabric

A wireless network uses radio waves to connect the end points to the rest of the network. The main components of a wireless network infrastructure are the wireless Access Points (APs) and a Wireless Controller. An AP allows a wireless-capable device to connect to a wired network. A wireless controller controls and manages all the APs in the network. It is responsible for the AP image and configuration management, radio resource management, client session management and roaming, and all the other wireless control plane functions.

This chapter describes only the configurations that are required to support a wireless network in a LISP VXLAN Fabric. Before you proceed, we recommend that you look through the earlier chapters of this document for the functionality and configuration of a LISP VXLAN fabric.

Wireless Support in a LISP VXLAN Fabric

A LISP VXLAN fabric supports the wireless infrastructure in the these modes: Over-the-Top Centralized Wireless and Fabric-Enabled Wireless.

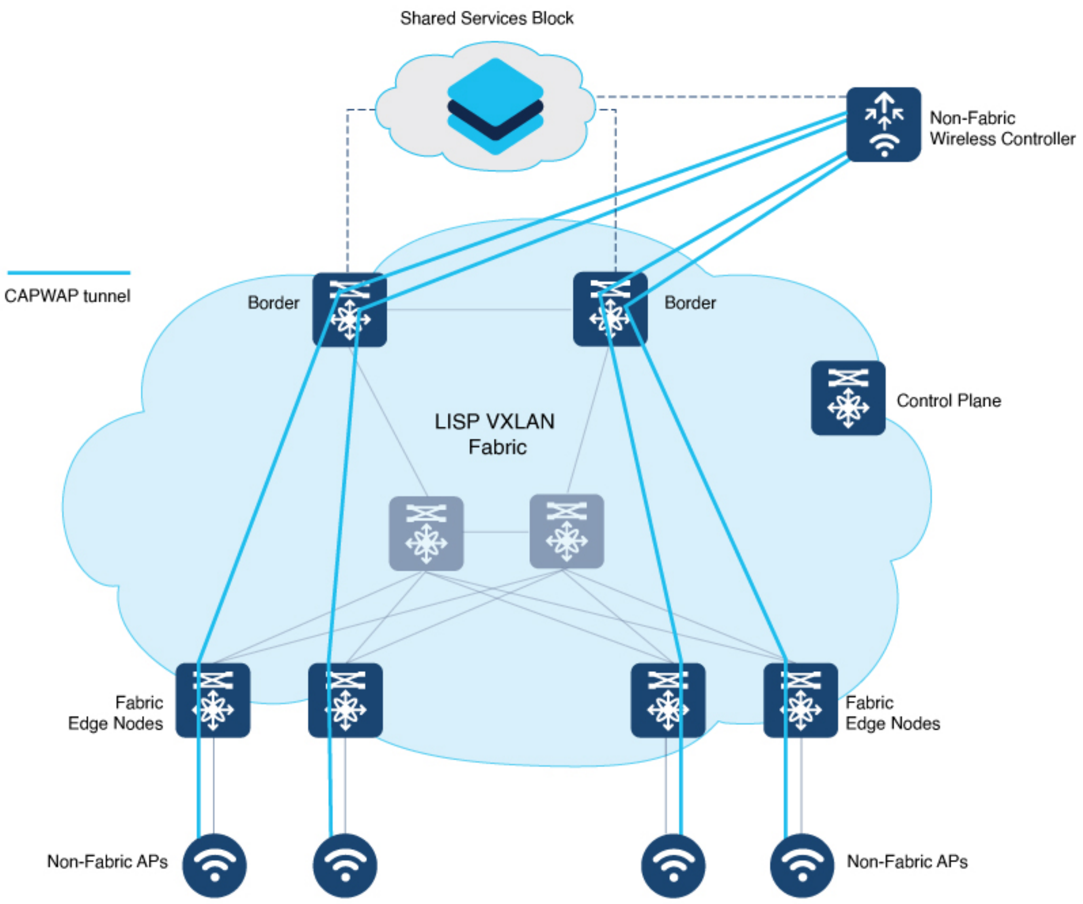
Over-the-Top Centralized Wireless

In an over-the-top (OTT) centralized wireless deployment, traditional wireless client traffic is encapsulated in Control and Provisioning of Wireless Access Points (CAPWAP) at the access point. The CAPWAP data is encapsulated in VXLAN at the fabric edge node, and forwarded to the fabric border node. At the border node, the VXLAN encapsulation is removed and the CAPWAP data traffic is forwarded to the wireless controller.

The CAPWAP tunnel between wireless controller and an AP traverses the campus backbone network, using the wired fabric as a transport medium.

OTT wireless deployment is suitable when you are migrating from a traditional network to a LISP VXLAN fabric network, wherein you might want to first migrate the wired infrastructure and plan wireless integration at a later time.

Figure 1: Over-the-Top Centralized Wireless Topology



Consider the following before you deploy OTT centralized wireless in your LISP VXLAN fabric.

- Wireless controller is located external to the fabric.
- APs are connected to the fabric edge node and are located in the default instance in the fabric overlay. The APs are registered with the control plane node as wired clients.
- After an AP gets an IP address from DHCP, it joins the wireless controller through CAPWAP tunnel. For information on AP connectivity to wireless controller, refer to *Cisco Wireless Controller Configuration Guide*.
- Wireless SSID is mapped to the VLAN or subnet at wireless controller using dynamic interfaces.

- Wireless clients are authenticated and onboarded by the wireless controller.
- A network device that is located upstream of the border advertises the wireless network to the fabric border.
- Communication between a wired host in the fabric and a wireless client outside fabric occurs through the fabric border.

Configuring OTT Centralized Wireless

This task describes only the fabric configurations that are required to enable OTT wireless, assuming that the wireless infrastructure is already functioning in the traditional way.

Before you begin

- Ensure that you have configured the control plane node, border node, and fabric edge node in a LISP VXLAN fabric for wired clients. For configuration information, refer to the earlier chapters in this document.
- Ensure that there is a specific subnet reachability in the underlay (global routing table) for the wireless controller subnet at the access layer. This is required for the access points to connect to the wireless controller.

Procedure

Step 1 On the fabric edge node, configure the switched virtual interface (SVI) for the AP VLAN.

Example:

```
interface Vlan92
 description For APs
 mac-address 0000.0c9f.ff39
 ip address 10.92.1.1 255.255.255.240
 no ip redirects
 no lisp mobility liveness test
 lisp mobility APVlan92-IPV4
end
!
```

The same SVI is present on every fabric edge node, with the same Virtual IP address and MAC address. This makes it a default gateway for all traffic from the APs.

Step 2 Configure Layer 3 VNI and Layer 2 VNI for the AP VLAN.

An AP is placed in the global routing table which has a LISP instance ID (VNI) attached.

In this example, Layer 3 instance ID for the global routing table is 4097 and the corresponding Layer 2 instance id is 8189.

Example:

```
router lisp
  instance-id 4097
   remote-rloc-probe on-route-change
   dynamic-eid APVlan92-IPV4
    database-mapping 10.92.1.0/28 locator-set rloc_set
    exit-dynamic-eid
   !
  exit-instance-id
 !
instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 92
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
exit-router-lisp
!
```

Step 3 On the wireless controller, map the wireless SSID to the wireless client VLAN or subnet.

Example:

```
vlan 2055    //wireless client VLAN
 name Client_VLAN1

//Create wireless Policy Profile
wireless profile policy diy-localOTT-open_profile
 description diy-localOTT-open_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 http-tlv-caching
 service-policy input platinum-up
 service-policy output platinum
 vlan Client_VLAN1
 no shutdown

//Create Wirless SSID
wlan diy-localOTT-open_profile 17 diy-localOTT-open
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown

//Create a Policy Tag to map the WLAN Profile to the Policy Profile
wireless tag policy wireless-policy-tag-open
wlan diy-localOTT-open_profile policy diy-localOTT-open_profile
```

Fabric-Enabled Wireless

A fabric-enabled wireless network integrates the wireless infrastructure with the wired fabric network. In a fabric with integrated wired and wireless, a single infrastructure for wired and wireless connectivity provides a uniform experience by having a common overlay for both the wired and wireless hosts. Wireless users get all the advantages of a fabric such as enhanced security with uniform policy application, data plane optimization, and operational simplicity.

- Wireless controller controls and manages all wireless functions. It interacts with the fabric control plane to notify the control plane node of all the wireless client joins, roams and disconnects.

- Fabric control plane node maintains the endpoint locator database for both the wired and wireless clients. It resolves the lookup requests from the fabric edge nodes to locate the endpoints. The control plane node notifies the fabric edge and border nodes about the wireless client mobility and RLOC information.
- Fabric APs connect directly to the fabric edge nodes. A fabric AP establishes a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel to the fabric wireless controller and connects as local-mode AP. It applies all wireless specific features like SSID policies, AVC, QoS, so on, to the wireless endpoints.
- Fabric edge node onboards an AP into the fabric. It serves as a single Layer 3 default gateway for all the connected endpoints.
- Control plane traffic between the fabric APs and the fabric wireless controller is through the CAPWAP tunnel.
- For the data plane, a fabric AP establishes a VXLAN tunnel to the fabric edge node. Wireless data traffic traverses through this tunnel to reach the fabric edge node. The fabric edge node terminates the AP VXLAN tunnel and the client data traffic is placed on the wired fabric network. The VXLAN tunnel between the fabric AP and the fabric edge node carries the segmentation and policy information to and from the fabric edge node.

Note The rest of the document describes the fabric-enabled wireless mode of operation.

Platforms that Support Wireless Infrastructure in a LISP VXLAN Fabric

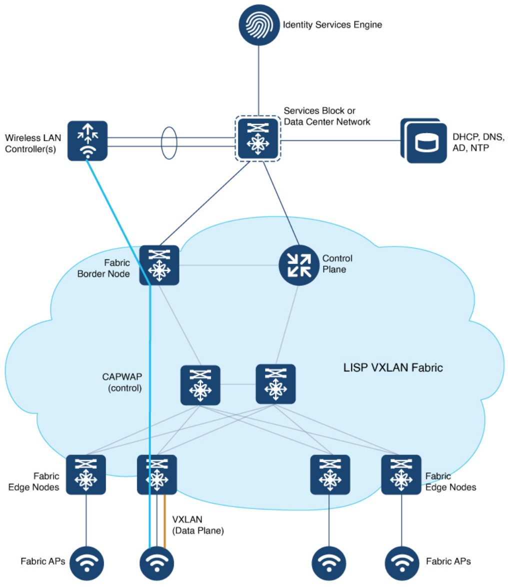
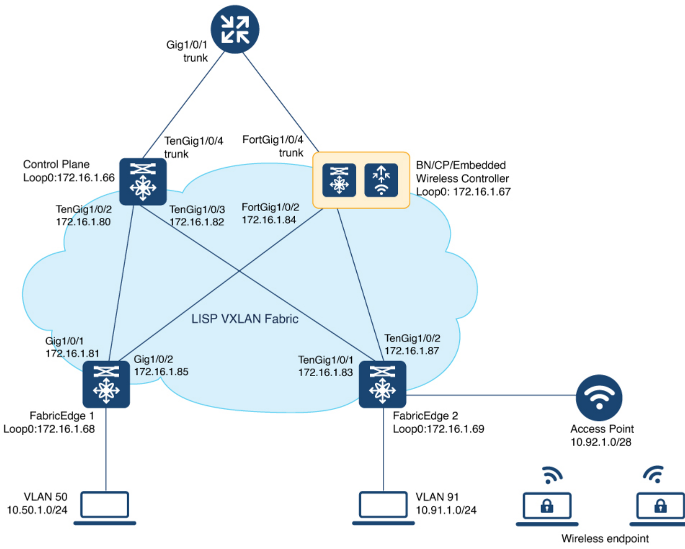
LISP VXLAN Fabric supports the following wireless devices:

- Cisco Catalyst 9800 Series Wireless Controller that is available in multiple form factors such as an Appliance, Cloud-based, or Embedded Wireless for a Switch.
- Wi-Fi 6 Access Points, which are the Cisco Catalyst 9100 Series APs.
- 802.11ac Wave 2 Access Points, which are the AP1540 Series, AP1560 Series, AP1800 Series, AP2800 Series, AP3800 Series, and AP4800 Series.

Wireless Controller

In a LISP VXLAN fabric, a wireless controller can either be hardware device or a software module that runs on a colocated control plane and border node.

The following table describes both these operational modes of a wireless controller.

Wireless Controller - Appliance or Virtual Form for Cloud	Embedded Wireless Controller
The wireless controller is a hardware device that is located external to the fabric. It is physically connected to the fabric border node or is located multiple hops upstream of the fabric border node (such as, in a Data Center). A fabric site can have one or multiple wireless controllers, but a wireless controller cannot be shared by different fabric sites. The wireless controller must have IP reachability with the control plane node of the LISP VXLAN fabric.	The wireless controller functionality is implemented as a software on a fabric node device. This is called an embedded wireless controller, which functions without a separate hardware device. Such an embedded wireless controller can be deployed in distributed branches or small campuses. Cisco Catalyst 9800 Embedded Wireless Controller software can be installed on a switch that functions as a colocated control plane and border node in the fabric. Cisco Catalyst 9300 Series switches, Cisco Catalyst 9400 Series switches, and Cisco Catalyst 9500 Series switches support Cisco Catalyst 9800 Embedded Wireless Controller. **Note** An embedded wireless controller works only in the fabric mode.
Figure 2: Fabric-Enabled Wireless with a Wireless Controller Appliance  Identity Services Engine Services Block or Data Center Network Wireless LAN Controller(s) DHCP, DNS, AD, NTP Fabric Border Node Control Plane CAPWAP (control) LISP VXLAN Fabric Fabric Edge Nodes Fabric Edge Nodes VXLAN (Data Plane) Fabric APs Fabric APs	***Figure 3: Fabric-Enabled Wireless with Embedded Wireless Controller***  Gig1/0/1 trunk TenGig1/0/4 trunk FortGig1/0/4 trunk Control Plane Loop0:172.16.1.66 BN/CP/Embedded Wireless Controller Loop0: 172.16.1.67 TenGig1/0/2 172.16.1.80 TenGig1/0/3 172.16.1.82 FortGig1/0/2 172.16.1.84 LISP VXLAN Fabric Gig1/0/1 172.16.1.81 Gig1/0/2 172.16.1.85 TenGig1/0/1 172.16.1.83 TenGig1/0/2 172.16.1.87 FabricEdge 1 Loop0:172.16.1.68 FabricEdge 2 Loop0:172.16.1.69 Access Point 10.92.1.0/28 VLAN 50 10.50.1.0/24 VLAN 91 10.91.1.0/24 Wireless endpoint

Fabric Access Points

The fabric APs connect directly to the fabric edge nodes and are part of the fabric overlay. AP subnets in the overlay are advertised to the external network and the wireless controller reaches the APs through the overlay. Control plane traffic from a fabric AP to the wireless controller (for the AP join operation) is through the CAPWAP tunnel.

All APs belong to a unique overlay virtual network called the Default Instance, which is mapped to the global routing table. A Default Instance connects network infrastructure elements like Access Points and Layer 2 switches to the fabric access layer. This unique overlay virtual network for all fabric APs simplifies the management of APs by including them within a single subnet.

Before onboarding the fabric APs, ensure that a default instance (instance-id 4097) is already configured on the fabric edge and border nodes. For configuration of a default instance, refer to *Configuring Fabric Edge Node* chapter. Map the AP subnet to the Layer 2 VNI and Layer 3 VNI for the Default Instance. Ensure that the fabric edge device is configured for Dot1x authentication of connected endpoints.

Workflow to Integrate Wireless in a LISP VXLAN Fabric

Before you begin the wireless integration, ensure that you have configured the fabric control plane node, border node, and the fabric edge node for a wired network.

Step	Purpose
Enabling the wireless controller for fabric operations	
Configure the wireless controller with the fabric control plane and virtual networks for the wireless clients and APs.	• Specify the fabric control plane name and its IP address. • Create the Layer 2 and Layer 3 VXLAN network identifiers (VNIDs) for the default instance. (A default instance is where the APs are placed.) • Create the Layer 2 VNID for the overlay virtual networks.
Configure the Wireless Management Interface of the wireless controller with the credentials to establish a secure connection with the fabric control plane node.	The wireless controller communicates with the control plane node on TCP port 4342 on the controller.
Create a **Fabric Profile** for the wireless clients.	• Specify the Layer 2 VNID. • Specify the SGT tag.
Create a **Policy Profile** to define the network policies and switching policies for a wireless client.	• Specify that traffic is local switching. • (Optional) Specify Quality of Service (QoS) – policing and marking policies on SSID and clients. • Specify AAA Override to override the VNID assignment of a client. This allows the AAA server to assign a specific virtual network to a client, based on the client's credentials and the policies configured on the AAA server.
Associate the previously created Fabric Profile with the Policy Profile.	The fabric inherits the associated policies.

Step	Purpose
Create a WLAN Profile to define the wireless characteristics of a WLAN.	• Specify the different types of SSID. For a fabric SSID, enable only Central Authentication. Disable Central Switching, Central DHCP and Flex NAT/PAT. • Specify the Security type for WLAN (PSK, 802.1x, WebAuthentication, and so on). If you define 802.1x or Central Web Authentication as the authentication method, ensure that you have configured AAA. • Specify advanced protocols such as 802.11k.
Create a Policy Tag to associate the SSID (WLAN Profile) with the Policy Profile.	Associating the Policy profile to an SSID applies the switching policies and the networking policies to the SSIDs.
Onboarding an AP	
Before onboarding an AP, ensure that a default instance (to host the AP subnets) is already created in the fabric.	
AP acquires an IP address through DHCP in the overlay.	After an AP connects to a fabric edge and boots up, it acquires an IP address from the DHCP server. The DHCP scope has option 43 configured, which defines the IP address of the wireless controller that the AP should reach out to.
AP registers with the fabric edge node.	The fabric edge node registers the AP's IP address and MAC address as endpoint ID (EID), with the control plane node.
AP registers with the wireless controller.	AP and the wireless controller exchange CAPWAP discovery and response messages. The wireless controller validates the AP and the AP validates the wireless controller to complete the discovery and AP join process. The validation on both the AP & WLC is a mutual authentication mechanism. An AP joins either through inbuilt certificates such as Manufacturer Installed Certificate (MIC) or third-party certificates such as Locally Significant Certificate (LSC).
Fabric edge builds a VXLAN tunnel to the AP. This serves as the data plane for the fabric wireless.	After an AP joins the fabric wireless controller in the local mode through CAPWAP, wireless controller queries the control plane about the AP's connectivity to the fabric infrastructure. After obtaining the RLOC of the AP, the wireless controller registers the AP with the control plane node. The control plane node then notifies the fabric edge about the presence of the AP. The fabric edge creates a VXLAN tunnel interface to the specified IP address of the AP.

Step	Purpose
Assign the previously created Policy Tag to the AP.	A Policy tag identifies the SSIDs and their policies, which are broadcasted by the AP. Site Tag and RF Tags also contain the settings to configure an AP. For information on the tags and their settings, refer to Understand Catalyst 9800 Wireless Controllers Configuration Model.
Onboarding Wireless Clients	
When a wireless client associates with a fabric AP, it is onboarded in the following manner: • Client authenticates with the wireless controller on an SSID that is enabled for fabric. • Wireless controller notifies the fabric AP to use VXLAN encapsulation to the fabric edge node and to populate the appropriate virtual network identifier (VNI) and source group tag (SGT) for that client in a VXLAN packet. • Wireless controller registers the client's MAC address in the fabric control plane node database. • After the client receives an IP address for itself through DHCP, the fabric edge node updates the control plane database with the client IP address. The MAC address and IP address of the client are mapped and correlated. The wireless client can now communicate through the fabric network.	

Wireless Client Roams

Consider a LISP VXLAN Wireless Figure 3: Fabric-Enabled Wireless with Embedded Wireless Controller where there are two fabric edge nodes (Fabric Edge 1 and Fabric Edge 2). Access point AP1 is connected to Fabric Edge 1 and AP2 is connected to Fabric Edge 2. A Catalyst 9800 Series embedded wireless controller runs on the colocated border and control plane node.

When a client that is connected to AP1 roams to AP2 (inter-switch roaming), the following sequence of events occur:

1. AP2 notifies the wireless controller about the client presence.
2. The wireless controller updates the forwarding table of AP2 with the client’s SGT and Layer 2 VNID.
3. The wireless controller updates the control plane node database with the client’s new RLOC (Fabric Edge 2).
4. The control plane notifies Fabric Edge 2 to add the client MAC address to its forwarding table.
5. The control plane then notifies Fabric Edge 1 to clean up the client info.
6. On receiving traffic from the client, Fabric Edge 2 updates the control plane with the client’s IP address.

An anycast gateway that is configured on all the fabric edges facilities seamless client roaming between the fabric edge nodes.

Prerequisites for Configuring Fabric-Enabled Wireless

- Ensure that the underlay network links are configured for routed access connectivity.
- Ensure that you have configured the fabric control plane node, border node, and the fabric edge node for a wired network.
- Ensure that there is a specific subnet reachability in the underlay (global routing table) for the wireless controller subnet at the access layer. This is required for the access points to connect to the wireless controller.
- For an embedded wireless controller:

  A fabric node switch that hosts the embedded controller should operate in Install mode for a wireless package to be installed on it. Install the Cisco Catalyst 9800 Series Wireless Controller as a sub-package on top of the base image on the fabric node switch.

  For information on booting a switch in Install mode and installing a sub-package, refer to Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

  Ensure that the wireless package is the same version as the base image on the switch (Cisco IOS XE). For example, if the switch is operating on Cisco IOS XE 17.10.1, install the 17.10.1 version of the wireless package on the switch.

  To download a wireless package, go to the Software Download page, navigate to the switch family, and select the **IOS XE Wireless Controller Software Package** Software Type.

  After the wireless package is installed, use the **show install summary** command on the switch to verify the version and state of the embedded wireless controller.

How to Configure Fabric-Enabled Wireless

Procedure

Step 1 Connect the wireless controller appliance to the fabric border node and initialize it.

For information on the initial setup of the wireless controller, refer to the Cisco Catalyst 9800 Wireless Controller Configuration Guide for the relevant release.

Step 2 Enable the wireless controller for fabric operations:

a. Configure the name and IP address of the wireless control plane.

b. Configure the wireless client VLAN and the AP VLAN.

c. Configure a fabric profile and associate the Layer 2 VXLAN network identifier (VNID), and optionally SGT, to the fabric profile.

d. Configure a wireless policy profile and map the fabric profile that was created in the previous step.

The following table describes the commands that configure a wireless controller for fabric operations.

Step	Command	Purpose
1	**configure terminal** **Example**: `WC# configure terminal`	Enters global configuration mode.
2	**wireless management interface** *interface-name* **Example**: `WC(config)# wireless management interface Vlan224`	Configure the management interface on the wireless controller.
3	**wireless fabric control-plane** *cp-name* **Example**: `WC(config)# wireless fabric control-plane default-control-plane`	Configures the name of the fabric control plane. You can assign a name of your choice to the control plane.

4	**ip address** *cp-ip address* **key** *authentication-key*
	Example:
	`WC(config-wireless-cp)# ip address 172.16.1.66 key some-key`
	`WC(config-wireless-cp)# end`
		Configures the IP address of the control plane and the authentication key shared with the control plane.

5	**wireless fabric name** *fabric-name* **l2-vnid** *l2-vnid* **control-plane-name** *cp-name*
	Example:
	`WC(config)# wireless fabric name wireless-Campus l2-vnid 8190`
	` control-plane-name default-control-plane`
		Configures the wireless client VLAN.

6	**wireless fabric name** *fabric-name* **l2-vnid** *l2-instance-id* **l3-vnid** *l3-instance-id* **control-plane-name** *cp-name*
	Example:
	`WC(config)# wireless fabric name APVlan92-IPV4 l2-vnid 8189`
	`l3-vnid 4097`
	`ip 10.92.1.1 255.255.255.0 control-plane-name`
	`default-control-plane`
		Configures the AP VLAN.

<table>
<tr><th>Step</th><th>Command</th><th>Purpose</th></tr>
<tr><td>7</td><td>

wlan *wlan-name* *wlan-id* *SSID-name*

Example:

Create the following WLAN profiles:

```
wlan diy-psk_profile 17 diy-psk
 security ft over-the-ds
 security wpa psk set-key ascii 0 Cisco123
 no security wpa akm dot1x
 security wpa akm psk
 no shutdown
!
wlan diy_open_profile 18 diy_open
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
!
wlan diy-dot1x_profile 19 diy-dot1x
 security ft over-the-ds
 security dot1x authentication-list default
 security pmf optional
 no shutdown
```

</td><td>

Configures a WLAN.

This example configures three WLANs with IDs 17, 18, 19 and SSID named diy-psk, diy_open , and diy-dot1x. It also enables the WLAN using the **no shutdown** command.

</td></tr>
<tr><td>8</td><td>

wireless profile fabric *profile-name*

Example:

Create the following fabric profiles:

```
wireless profile fabric diy-psk_profile
 description diy-psk_profile
 client-l2-vnid 8190    //Map to Layer 2 VNID 8190
 sgt-tag 22

wireless profile fabric diy-dot1x_profile
 description diy-dot1x_profile
 client-l2-vnid 8191    //Map to Layer 2 VNID 8191
 sgt-tag 32

wireless profile fabric diy-open_profile
 description diy-open_profile
 client-l2-vnid 8192 //Map to Layer 2 VNID 8192
 sgt-tag 42
```

</td><td>

Configures a fabric profile.

This example configures three fabric profiles (*diy-psk_profile*, *diy_open_profile*, and *diy-dot1x_profile*), each mapped to a different Layer 2 VNI.

</td></tr>
</table>

Step	Command	Purpose

9	**wireless profile policy** *profile-policy*
	Example:
	`wireless profile policy diy-psk_profile`
	`description diy-psk_profile`
	`no central dhcp    //specifies local DHCP mode`
	`no central switching  //configures WLAN for local switching`
	`dhcp-tlv-caching`
	`exclusionlist timeout 180`
	`fabric diy-psk_profile    //maps fabric profile with the policy`
	`profile`
	`http-tlv-caching`
	`service-policy input platinum-up`
	`service-policy output platinum`
	`no shutdown`
	`!`
	`wireless profile policy diy_open_profile`
	`description diy_open_profile`
	`no central dhcp`
	`no central switching`
	`dhcp-tlv-caching`
	`exclusionlist timeout 180`
	`fabric diy_open_profile    //maps fabric profile with the policy`
	`profile`
	`http-tlv-caching`
	`ip nbar protocol-discovery`
	`service-policy input platinum-up`
	`service-policy output platinum`
	`no shutdown`
	`!`
	`wireless profile policy diy-dot1x_profile`
	`description diy-dot1x_profile`
	`no central dhcp`
	`no central switching`
	`dhcp-tlv-caching`
	`exclusionlist timeout 180`
	`fabric diy-dot1x_profile    //maps fabric profile with the policy`
	`profile`
	`http-tlv-caching`
	`service-policy input platinum-up`
	`service-policy output platinum`
	`no shutdown`
		Configures a wireless policy profile for a given SSID and maps the fabric profile with this policy profile.
		This example configures three different wireless policy profiles, (*diy-psk_profile*, *diy_open_profile*, and *diy-dot1x_profile*) and maps the fabric profiles that were created earlier to these policy profiles.
		The wireless profile policy is mapped to a fabric profile using the **fabric** *profile-policy* command.

10	**wireless tag policy** *policy-tag-name* **Example**: `WC(config)# wireless tag policy wireless-policy-tag-psk`	Creates a Policy Tag and enters policy tag configuration mode. This example shows only one policy tag, namely *wireless-policy-tag-psk*. You can create more policy tags.

Step	Command	Purpose
11	**wlan** *wlan-name* **policy** *profile-policy-name* **Example**: `WC(config-policy-tag)# wlan diy-psk_profile policy diy-psk_profile`	Maps a policy profile to a WLAN profile. This example maps the profile policy *diy-psk_profile* that was created in Step 9 to the WLAN profile that was created in Step 7.

12	**end**
	Example:
	`WC(config-policy-tag)# end`
		Returns to privileged EXEC mode.

To see the GUI-based configurations of the wireless controller, click Configuring Wireless Controller for Fabric-Enabled Wireless (GUI).

Step 3 Integrate the wireless controller with the fabric control plane.

a) On the control plane node, define a locator set for the wireless controller.

Example:

```
router lisp
locator-set WLC
192.168.224.4  //IP address of the Wireless Management Interface
exit-locator-set
```

b) On the control plane node, configure open passive TCP sockets to listen for incoming connections. The wireless controller communicates with the control plane node on TCP port 4342.

Example:

```
map-server session passive-open WLC
```

c) On the control plane node, configure the LISP Site to accept EID prefixes.

Example:

```
 site site_uci
  description map-server1
  authentication-key some-key
  eid-record instance-id 4097 10.92.1.0/28 accept-more-specifics //AP subnet
  eid-record instance-id 4099 10.51.1.0/24 accept-more-specifics //New subnet for wireless
 clients
  eid-record instance-id 8189 any-mac
  eid-record instance-id 8190 any-mac
  eid-record instance-id 8191 any-mac
  exit-site
 !
exit-router-lisp
!
```

Step 4 On the border node, update the map cache with the AP subnets.

Example:

```
router lisp
 instance-id 4097  //Layer 3 instance-id for the default instance
```

```
  remote-rloc-probe on-route-change
  service ipv4
   eid-table default
   map-cache 10.92.1.0/28 map-request
   exit-service-ipv4
  !
  exit-instance-id
 !
exit-router-lisp
!
```

Step 5 Configure the fabric edge nodes to onboard the fabric APs. Do the following configurations on the fabric edge node.

a) Configure SVI interface for the wireless client VLAN.

Note

- Ensure that you assign the same MAC address for a given SVI, across all fabric edges within the fabric site. We recommend that you use a MAC address starting from the base range value of 0000.0C9F.F05F.
- IPv6 client address assignment through Stateless Address Auto-Configuration (SLAAC) depends on Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), and Neighbor Discovery (ND) message sequences. A default RA interval of 200 seconds results in a longer duration for IP address resolution. To enable faster address convergence using SLAAC, we recommend that you configure a lower RA interval, such as 1000 milliseconds.

Example:

```
interface Vlan51
 description For Wireless Clients
 mac-address 0000.0c9f.f3b7   //Common MAC address
 vrf forwarding Campus
 ip address 10.51.1.1  255.255.255.0
 ip helper-address 192.168.136.1
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility wireless-Campus-IPV4
 lisp mobility wireless-Campus-IPV6
 ipv6 address 2001:192:168:166::1/96
 ipv6 enable
 ipv6 nd ra-interval msec 1000
 ipv6 nd dad attempts 0
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 dhcp relay destination 2001:192:168:136::1
 ipv6 dhcp relay source-interface Vlan1023
 ipv6 dhcp relay trust
!
```

b) Configure SVI interface for the AP VLAN.

Note Ensure that you assign the same MAC address for a given SVI, across all fabric edges within the fabric site. We recommend that you use a MAC address starting from the base range value of 0000.0C9F.F05F.

Example:

```
interface Vlan92
 description For APs
 mac-address 0000.0c9f.ff39
 ip address 10.92.1.1 255.255.255.240
 no ip redirects
 no lisp mobility liveness test
 lisp mobility APVlan92-IPV4
end
!
```

c) Configure dynamic EID for the AP subnets in the default instance.

Example:

```
router lisp
  instance-id 4097
   remote-rloc-probe on-route-change
   dynamic-eid APVlan92-IPV4
    database-mapping 10.92.1.0/28 locator-set rloc_set
    exit-dynamic-eid
   !
  exit-instance-id
 !
```

d) Configure Layer 3 VNI for the wireless client subnet.

Example:

```
instance-id 4100
  remote-rloc-probe on-route-change
  dynamic-eid wireless-Campus-ipv4
   database-mapping 10.51.1.0/24 locator-set rloc_set
   exit-dynamic-eid
  !
  dynamic-eid wireless-Campus-ipv6
   database-mapping 2001:DB8:2051::/64 locator-set rloc_set
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Campus
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  service ipv6
   eid-table vrf Campus
   map-cache ::/0 map-request
   exit-service-ipv6
  !
  exit-instance-id
 !
```

e) Configure Layer 2 VNI for AP VLAN.

Example:

```
 instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 92
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
```

f) Configure Layer 2 VNI for the wireless client VLAN.

Example:

```
 instance-id 8190
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 51
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
exit-router-lisp
!
```

g) Enable DHCP Snooping on the AP and Client VLANs.

Example:

```
ip dhcp snooping vlan 51,92
```

Configuring Wireless Controller for Fabric-Enabled Wireless (GUI)

Configuring a Fabric and its Control Plane (GUI)

Procedure

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

Step 2 Under the **Control Plane** tab, click **Add**.

Step 3 In the **Add Control Plane** window, enter the name of the control plane and optionally a description. Click **Apply to Device** to save the control plane name.

Step 4 Under the **General** tab, click **Add**.

Step 5 In the **Add Client and AP VNID** window, enter the following values:

- Enter the name of the Fabric.
- Enter the Layer 2 virtual network ID (**L2 VNID**) for the wireless client and AP VLANs.
- Select a control plane node from the **Control Plane Name** drop down list.
- Enter the Layer 3 virtual network ID (**L3 VNID**) for the AP VLAN.
- Enter the **IP Address** and **Netmask** of the fabric control plane node.

Step 6 Click **Apply to Device** to save the configuration.

Configuring a Fabric Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric** page, under the **Profiles** tab, 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
- (Optional) SGT tag; valid range is between 2 and 65519

Step 4 Click **Apply to Device** to save the configuration.

Configuring a Wireless Profile Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, under the **General** tab, enter a name and description for the policy profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces. Do not use spaces because it causes system instability.

Step 4 To enable the policy profile, set **Status** as **Enabled**.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 n the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller or access point understands the source SGT.
- SGACL Enforcement.

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, enable **Central Authentication**. Central Authentication tunnels client data to the controller, as the controller handles client authentication.

Disable **Central Switching**, **Central DHCP**, and **Flex NAT/PAT**.

Step 9 Click **Apply to Device** to save the configuration.

Creating a WLAN Profile (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, click **Add**.

The **Add WLAN** window is displayed.

Step 2 Under the **General** tab, enter the following information: .

a) In the **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces
b) In the SSID field, enter a valid SSID for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.
c) In the WLAN ID field, enter an ID for the WLAN.

Step 3 Enter a valid SSID for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

Step 4 Click **Apply to Device** to save the configuration.

Configuring WLAN Security (GUI)

An authentication method sets the method by which a client can access the WLAN and decides the level of security on the WLAN.

Set up the authentication configurations and filters for the WLAN depending on the method you have chosen. These include the keys, filters, ACLs, and parameter maps as applicable to the selected authentication method.

Procedure

Step 1 If you have selected **PSK** as the authentication method, configure the following:

a) In the **WLAN** > **Pre-Shared Key (PSK)** section, select the PSK format. Choose between ASCII and Hexadecimal formats.
b) From the **PSK type** drop-down list, choose if you want the key to be unencrypted or AES encrypted.
c) In the **Pre-Shared Key** field, enter the pass key for the WLAN.

Step 2 If you have selected **Dot1x** as the authentication method, configure the following:

a) In the **WLAN** > **AAA** tab, configure the AAA server list for the WLAN.
b) Select any of the available AAA servers to add to the WLAN.
c) To add a new AAA server to the list, click on Add New Server and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.

Step 3 If you have selected **Local Web Authentication** as the authentication method, configure the following:

a) In the **WLAN** > **Parameter Map** tab, configure the parameter map for the WLAN. A parameter map sets parameters that can be applied to subscriber sessions during authentication.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure a virtual IP address for redirecting the clients to the login page of the controller.
3. From the Trustpoint drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.

b) In the **WLAN** > **Local Users** tab, enter the username in the local database to establish a username-based authentication system.

1. Enter the user name to be saved.
2. From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
3. In the **Password** field, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters and can contain embedded spaces.
4. Click on the **+** sign to add the credentials to the database. Add as many user credentials as required.

Step 4 If you have selected **External Web Authentication** as the authentication method, configure the following:

a) In the **WLAN** > **Parameter Map** tab, configure the parameter map for the WLAN.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure the virtual IP address of the external web authentication login page to which the guest users are redirected.
3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.
5. To create a new parameter map, enter the parameter-map name.
6. In the **Redirect URL for login** field, enter the URL of the external server that will host the authentication page for login.
7. In the **Portal IPV4 Address** field, enter the IPv4 address of the external server to send redirects. If the external server uses an IPv6 address, in the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects.

b) In the **WLAN > ACL / URL Filter** tab, configure the ACL rules and the URL filter list.

1. In the **Pre Auth ACL** section, enter the name of the ACL.
2. In the **IP address** field, enter the source IP address and the destination IP address. This will configure the ACL to permit packet transfer from and to the specified IP address. You can add as many IP addresses as required.

3. In the **URL Filter** section, enter a name for the URL Filter list that you are creating.
4. Use the slider to set the list action to **Permit** or **Deny** the URLs.
5. Specify the URLs in the **URLs** box. Enter every URL on a new line.

Step 5 If you have selected Central Web Authentication as the authentication method, configure the following:

a) In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
b) In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
c) To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
e) In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

Step 6 Click **Apply to Device** to save the configuration.

Configuring Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **Policy**.

Step 2 Click **Add** to view the **Add Policy Tag** window.

Step 3 Enter a name and description for the policy tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Add** to map WLAN and policy.

Step 5 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

Step 6 Click **Apply to Device** to save the configuration.

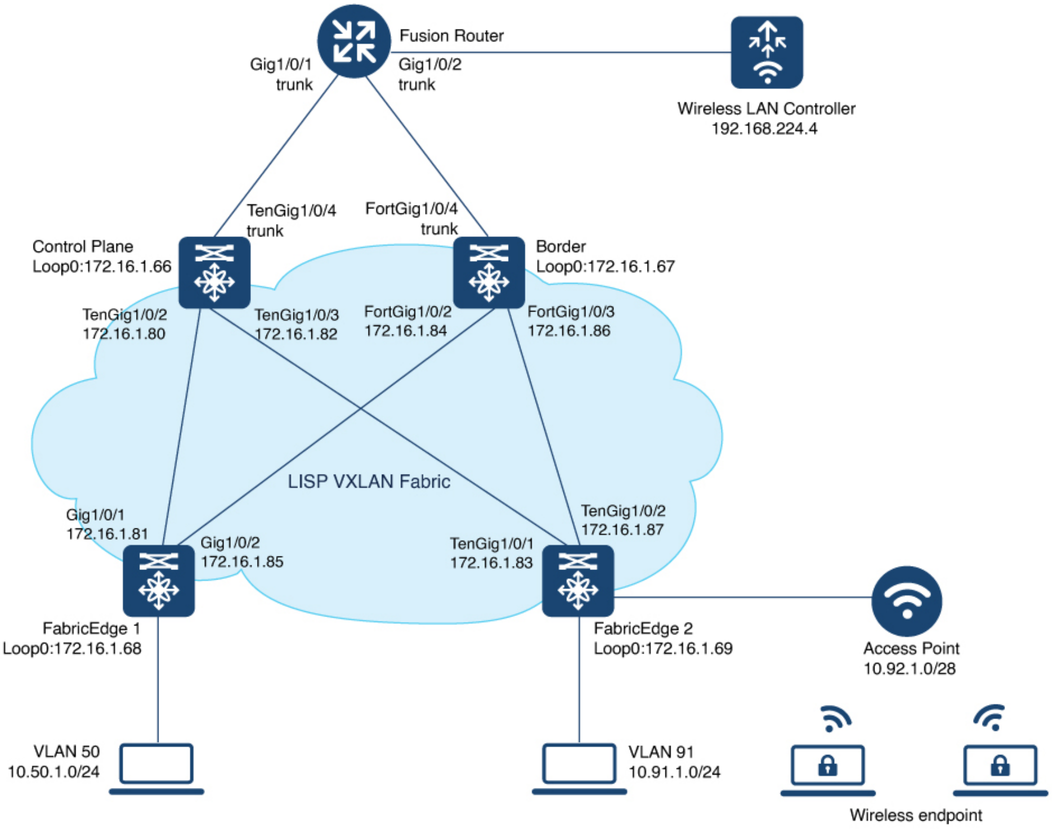
What to do next

Click Step 3 to continue the fabric configurations for integrating wireless.

Configuration Example for Fabric-Enabled Wireless

The example configurations described below are for the control plane node and the fabric edge node of a LISP VXLAN fabric shown in Figure 4: Fabric-enabled Wireless Topology. An upstream router connects the external border and the wireless controller. A fabric-enabled AP (10.92.1.0) is connected to Fabric Edge 2 (172.16.1.69) and is on VLAN 92. The wireless client IP subnets are 10.51.1.0/24 and 2001:DB8:2051::/64.

Figure 4: Fabric-enabled Wireless Topology



The example shows only the LISP configurations on the fabric nodes.

Control Plane Node Configuration	Fabric Edge Node Configuration

Control Plane Node Configuration	Fabric Edge Node Configuration

router lisp
 locator-table default
 locator-set WLC
  192.168.224.4
  exit-locator-set
 !
 service ipv4
  encapsulation vxlan
  sgt distribution
  sgt
  map-server
  map-resolver
  exit-service-ipv4
 !
 service ipv6
  encapsulation vxlan
  sgt distribution
  sgt
  map-server
  map-resolver
  exit-service-ipv6
 !
 service ethernet
  map-cache-limit 32768
  map-server
  map-resolver
  exit-service-ethernet
 !
 	
 instance-id 4097
  service ipv4
   eid-table default
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4100
  service ipv4
   eid-table vrf Campus
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  service ipv6
   eid-table vrf Campus
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv6
  !
  exit-instance-id
 !
 instance-id 4101
  service ipv4
   eid-table vrf Guest
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
	router lisp
	 locator-table default
	 locator-set rloc_set
	  IPv4-interface Loopback0 priority 10 weight 10
	  exit-locator-set
	 !
	 locator default-set rloc_set
	 service ipv4
	  encapsulation vxlan
	  itr map-resolver 192.168.94.1
	  etr map-server 172.16.1.66 key some-key
	  etr map-server 172.16.1.66 proxy-reply
	  etr
	  sgt
	  no map-cache away-eids send-map-request
	  use-petr 172.16.1.67
	  proxy-itr 172.16.1.69
	  exit-service-ipv4
	 !
	 service ipv6
	  encapsulation vxlan
	  itr map-resolver 192.168.94.1
	  etr map-server 172.16.1.66 key some-key
	  etr map-server 172.16.1.66 proxy-reply
	  etr
	  sgt
	  no map-cache away-eids send-map-request
	  use-petr 172.16.1.67
	  proxy-itr 172.16.1.69
	  exit-service-ipv6
	 !
	 service ethernet
	  itr map-resolver 192.168.94.1
	  itr
	  etr map-server 172.16.1.66 key some-key
	  etr map-server 172.16.1.66 proxy-reply
	  etr
	  exit-service-ethernet
	 !
	 instance-id 4097
	  remote-rloc-probe on-route-change
	  dynamic-eid AVlan91-IPV4
	   database-mapping 10.91.1.0/24 locator-set rloc_set2
	   exit-dynamic-eid
	  !
	  dynamic-eid APVlan92-IPV4
	   database-mapping 10.92.1.0/28 locator-set rloc_set
	   exit-dynamic-eid
	  !
	  service ipv4
	   eid-table default
	   exit-service-ipv4
	  !
	  exit-instance-id
	 !
	 instance-id 4099
	  remote-rloc-probe on-route-change
	  dynamic-eid AVlan50-IPV4
	   database-mapping 10.50.1.0/24 locator-set rloc_set2
	   exit-dynamic-eid
	  !
	  dynamic-eid AVlan50-IPV6

Control Plane Node Configuration	Fabric Edge Node Configuration
exit-service-ipv4 ! exit-instance-id ! map-server session passive-open WLC site site_uci description map-server authentication-key some-key eid-record instance-id 4097 10.92.1.0/28 accept-more-specifics eid-record instance-id 4099 10.51.1.0/24 accept-more-specifics eid-record instance-id 4099 2001:DB8:2051::/64 accept-more-specifics eid-record instance-id 4097 0.0.0.0/0 accept-more-specifics eid-record instance-id 4097 10.91.1.0/24 accept-more-specifics eid-record instance-id 4099 0.0.0.0/0 accept-more-specifics eid-record instance-id 4099 10.50.1.0/24 accept-more-specifics eid-record instance-id 4099 ::/0 accept-more-specifics eid-record instance-id 4099 2001:DB8:2050::/64 accept-more-specifics eid-record instance-id 8194 any-mac eid-record instance-id 8197 any-mac eid-record instance-id 8189 any-mac eid-record instance-id 8190 any-mac eid-record instance-id 8191 any-mac allow-locator-default-etr instance-id 4097 ipv4 allow-locator-default-etr instance-id 4099 ipv4 allow-locator-default-etr instance-id 4099 ipv6 exit-site ! ipv4 source-locator Loopback0 ipv6 source-locator Loopback0 exit-router-lisp	database-mapping 2001:DB8:2050::/64 locator-set rlo exit-dynamic-eid ! service ipv4 eid-table vrf VN3 map-cache 0.0.0.0/0 map-request exit-service-ipv4 ! service ipv6 eid-table vrf VN3 map-cache ::/0 map-request exit-service-ipv6 ! exit-instance-id ! instance-id 4100 remote-rloc-probe on-route-change dynamic-eid wireless-Campus-ipv4 database-mapping 10.51.1.0/24 locator-set rloc_se exit-dynamic-eid ! dynamic-eid wireless-Campus-ipv6 database-mapping 2001:DB8:2051::/64 locator-set rl exit-dynamic-eid ! service ipv4 eid-table vrf Campus map-cache 0.0.0.0/0 map-request exit-service-ipv4 ! service ipv6 eid-table vrf Campus map-cache ::/0 map-request exit-service-ipv6 ! exit-instance-id ! instance-id 4101 //guest remote-rloc-probe on-route-change dynamic-eid Campus-guest database-mapping 192.168.167.0/24 locator-set rlo service ipv4 eid-table vrf Guest map-cache 0.0.0.0/0 map-request exit-service-ipv4 ! exit-instance-id ! instance-id 8194 remote-rloc-probe on-route-change service ethernet eid-table vlan 91 database-mapping mac locator-set rloc_set2 exit-service-ethernet ! exit-instance-id ! ! instance-id 8197

Control Plane Node Configuration	Fabric Edge Node Configuration

```
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 50
   database-mapping mac locator-set rloc_set2
   exit-service-ethernet
  !
  exit-instance-id
 !
 !
//APs in Global Instance
 instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 92
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
//Wireless client in Custom VLAN
 instance-id 8190
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 51
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
//Guest VLAN
instance-id 8191
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 52
   database-mapping mac locator-set rloc_set
   exit-service-ethernet
  !
  exit-instance-id
 !
 ipv4 locator reachability minimum-mask-length 32
proxy-etr-only
 ipv4 source-locator Loopback0
 ipv6 locator reachability minimum-mask-length 128
proxy-etr-only
 ipv6 source-locator Loopback0
 exit-router-lisp
!
 vrf definition VN3
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!

 vrf definition Campus
 address-family ipv4
 exit-address-family
 !
ip dhcp relay information option
ip dhcp snooping vlan 50,91
ip dhcp snooping
```

Control Plane Node Configuration	Fabric Edge Node Configuration
	! device-tracking policy IPDT_POLICY tracking enable ! interface GigabitEthernet1/0/3 device-tracking attach-policy IPDT_POLICY ! vlan configuration 50 ipv6 nd raguard ipv6 dhcp guard ! vlan 50 name AVlan50 ! vlan 91 name AVlan91 ! interface Vlan50 description server1 mac-address 0000.0c9f.f18e vrf forwarding VN3 ip address 10.50.1.1 255.255.255.0 ip helper-address 172.16.2.2 no ip redirects ipv6 address 2001:DB8:2050::1/64 ipv6 enable ipv6 nd dad attempts 0 ipv6 nd prefix 2001:DB8:2050::/64 2592000 604800 no-autoconfig ipv6 nd managed-config-flag ipv6 nd other-config-flag ipv6 nd router-preference High ipv6 dhcp relay destination 2001:DB8:2::2 ipv6 dhcp relay source-interface Vlan50 ipv6 dhcp relay trust no lisp mobility liveness test lisp mobility AVlan50-IPV4 lisp mobility AVlan50-IPV6 ! interface Vlan91 description server2 mac-address 0000.0c9f.f984 ip address 10.91.1.1 255.255.255.0 ip helper-address 172.16.2.2 no ip redirects no lisp mobility liveness test lisp mobility AVlan91-IPV4 ! interface Vlan51 description For Wirless Clients mac-address 0000.0c9f.f3b7 vrf forwarding Campus ip address 10.51.1.1 255.255.255.0 ip helper-address 192.168.136.1. //DHCP IP no ip redirects no lisp mobility liveness test lisp mobility wireless-Campus-ipv4 lisp mobility wireless-Campus-ipv6 ipv6 address 2001:192:168:166::1/96 ipv6 enable

Control Plane Node Configuration	Fabric Edge Node Configuration
	ipv6 nd ra-interval msec 1000 ipv6 nd dad attempts 0 ipv6 nd managed-config-flag ipv6 nd other-config-flag ipv6 nd router-preference High ipv6 dhcp relay destination 2001:192:168:136::1 ipv6 dhcp relay source-interface Vlan51 ipv6 dhcp relay trust ! interface Vlan92 description For APs mac-address 0000.0c9f.ff39 ip address 10.92.1.1 255.255.255.240 no ip redirects no lisp mobility liveness test lisp mobility APVlan92-IPV4 ! ip dhcp snooping vlan 51,92

Fabric Wireless Controller Configuration

Fabric Wireless Controller Configuration

This table shows only those configurations on the wireless controller that are required to enable it for fabric operations. For complete configuration of a wireless controller, refer to the *Cisco Catalyst 9800 Wireless Controller Configuration Guide*.

```
wireless management interface Vlan224
wireless fabric control-plane default-control-plane
 ip address 192.168.94.1 key some-key
!
wireless fabric name wireless-Campus l2-vnid 8190
                       control-plane-name default-control-plane
wireless fabric name APVlan92-IPV4 l2-vnid 8189 l3-vnid 4097
ip 10.92.1.1 255.255.255.0 control-plane-name default-control-plane
!
wireless profile fabric diy-psk_profile
 client-l2-vnid 8190
 description diy-psk_profile
wireless profile fabric diy-dot1x_profile
 client-l2-vnid 8190
 description diy-dot1x_profile
wireless profile fabric diy-open_profile
 client-l2-vnid 8190
 description diy-open_profile
!
wlan diy-psk_profile 17 diy-psk
 security ft over-the-ds
 security wpa psk set-key ascii 0 Cisco123
 no security wpa akm dot1x
 security wpa akm psk
 no shutdown
!
wireless profile policy diy-psk_profile
 no central dhcp
 no central switching
 description diy-psk_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric diy-psk_profile
 http-tlv-caching
 service-policy input platinum-up
 service-policy output platinum
 no shutdown
!

wlan diy-open_profile 18 diy-open
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
!
wireless profile policy diy-open_profile
 no central dhcp
 no central switching
 description diy-open_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric diy-open_profile  <-- fabric wireless profile
 http-tlv-caching
```

Fabric Wireless Controller Configuration

```
 service-policy input platinum-up
 service-policy output platinum
 session-timeout 1800
 no shutdown
!
wlan diy-dot1x_profile 19 diy-dot1x
 security ft over-the-ds
 security dot1x authentication-list default
 security pmf optional
 no shutdown

wireless profile policy diy-dot1x_profile
 no central dhcp
 no central switching
 description diy-dot1x_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric diy-dot1x_profile
 http-tlv-caching
 service-policy input platinum-up
 service-policy output platinum
 no shutdown
!
wireless tag policy wireless-policy-tag-psk
  wlan diy-psk_profile policy diy-psk_profile
!
wireless tag policy wireless-policy-tag-open
  wlan diy-open_profile policy diy-open_profile
!
wireless tag policy wireless-policy-tag-dot1x
  wlan diy-dot1x_profile policy diy-dot1x_profile
!
```

Verify the Fabric Enabled Wireless Configuration

You can verify the wireless fabric configurations using the show commands. This section provides the sample outputs for the show commands on the fabric wireless controller, control plane node and the fabric edge node in the topology shown Figure 4: Fabric-enabled Wireless Topology.

Show Commands on the Fabric Wireless Controller

```
wlc# show wireless fabric summary

Fabric Status      : Enabled

Control-plane:
Name                              IP-address        Key                              Status
--------------------------------------------------------------------------------------------
default-control-plane             172.16.1.66      a021544b825b420e                  Up

Fabric VNID Mapping:
  Name             L2-VNID    L3-VNID   IP Address      Subnet       Control plane name

----------------------------------------------------------------------------------------
wireless-Campus   8190         0         0.0.0.0                      default-control-plane

APVlan92-IPV4     8189       4097       10.92.1.1     255.255.255.0    default-control-plane
```

```
wlc# show fabric wlan summary

Number of Fabric wlan : 3

WLAN Profile Name                     SSID                           Status
---------------------------------------------------------------------------
17   diy-psk_profile                  diy-psk                          UP
18   diy-open_profile                 diy-open                         UP
19   diy-dot1x_profile                diy-dot1x                        UP

wlc# show fabric ap summary
Number of Fabric AP : 4
fabric
AP Name                            Slots    AP Model             Ethernet MAC    Radio MAC
       Location                Country    IP Address      State
------------------------------------------------------------------------------------------

AP0CD0.F894.6540                    2      C9117AXI-B             0cd0.f894.6540
0cd0.f897.f6c0  default location        US       192.168.156.11  Registered
AP24D7.9C8D.464C                    2      C9120AXI-B             24d7.9c8d.464c
24d7.9cbf.3fa0  default location        US       192.168.156.15  Registered
9115-ts325-9500H                    2      C9115AXE-B             7069.5a76.7a50
2c4f.5241.3540  Global/BLR/BL1/FL1      US       192.168.156.14  Registered
9115-ts340-katarxtr                 2      C9115AXI-B             70f0.966c.a0f0
a488.737f.0780  Global/BLR/BL1/FL2      US       192.168.156.13  Registered


wlc# show wireless client summary
Number of Clients: 1

MAC Address    AP Name                Type ID   State    Protocol Method     Role
------------------------------------------------------------------------------------------

4c34.889a.06be AP0CD0.F894.6540       WLAN 18   Run      11ac     None       Local


Number of Excluded Clients: 0


wlc# show wireless client mac-address 4c34.889a.06be details

Client MAC Address : 4c34.889a.06be
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.51.1.12
Client IPv6 Addresses : fe80::311d:6e13:9d40:9dab
Client Username: N/A
AP MAC Address : 0cd0.f897.f6c0
AP Name: AP0CD0.F894.6540
AP slot : 1
Client State : Associated
Policy Profile : diy-open_profile
Flex Profile : default-flex-profile
Wireless LAN Id: 18
WLAN Profile Name: diy-open_profile
Wireless LAN Network Name (SSID): diy-open
BSSID : 0cd0.f897.f6ce
Connected For : 41 seconds
Protocol : 802.11ac
Channel : 140
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1764 sec)
Session Warning Time : Timer not running
```

```
Input Policy Name  : None
Fabric status : Enabled    <--- displays status of the fabric and other details
  RLOC    : 172.16.1.69
  VNID    : 8190
  SGT     : 0
  Control plane name  : default-control-plane

<snip output>
…..
…..
<snip output>
wlc#
```

Show Commands on the Fabric Edge Node where the AP Joins

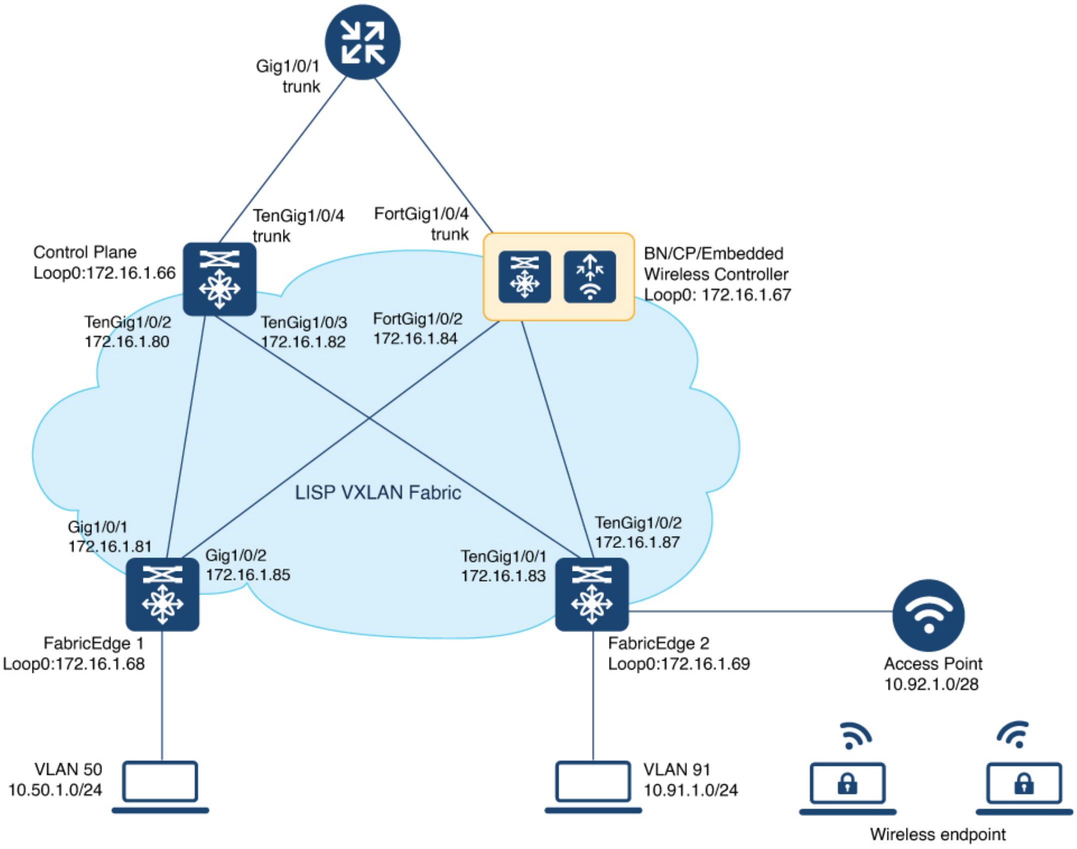
```
fabricedge# show access-tunnel summary

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2


Name    RLOC IP(Source)  AP IP(Destination)  VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------
Ac0     172.16.1.69      192.168.156.15      0       N/A          4789
Ac1     172.16.1.69      192.168.156.11      0       N/A          4789


Name   IfId            Uptime
------ ---------- --------------------
Ac0    0x00000041 0 days, 00:10:24
Ac1    0x00000042 0 days, 00:03:24

fabricedge#
```

Configuration Example for Embedded Wireless in a LISP VXLAN Fabric

The example configurations described below are for the colocated control plane and border node, and the fabric edge node shown in the Figure 5: LISP VXLAN Fabric with Embedded Wireless to enable embedded wireless controller. The colocated control plane and border node has an loopback IP address of 172.16.1.67. A fabric enabled AP (10.92.1.0/24) is connected to Fabric Edge 2 (Loopback IP address 172.16.1.69) and is on VLAN 92. The wireless client IP subnet is 10.51.1.0/24.

For information on installing the embedded wireless controller, refer to List item..

Figure 5: LISP VXLAN Fabric with Embedded Wireless



This table only shows the LISP configurations on the fabric nodes, which are required to enable wireless operations.

Before you proceed, ensure that the you have configured the fabric for a wired network. For the sample configurations, refer to *Configuration Example for Colocated Border and Control Plane Node* and *Configuration Example for Fabric Edge Node*.

Control Plane, Border Node, and Embedded Wireless Controller	Fabric Edge Node

Control Plane, Border Node, and Embedded Wireless Controller	Fabric Edge Node

router lisp
 locator-table default
 locator-set WLC
  172.16.1.67
  exit-locator-set
 !
 locator-set rloc_set
  IPv4-interface Loopback0 priority 10 weight
 10
  auto-discover-rlocs
  exit-locator-set
 !
 locator default-set rloc_set
 service ipv4
  encapsulation vxlan
  itr map-resolver 172.16.1.67
  etr map-server 172.16.1.67 key some-key
  etr map-server 172.16.1.67 proxy-reply
  etr
  sgt distribution
  sgt
  no map-cache away-eids send-map-request
  proxy-etr
  proxy-itr 172.16.1.67
  map-server
  map-resolver
  exit-service-ipv4
 !
 service ethernet
  map-cache-limit 65536
  itr map-resolver 172.16.1.67
  itr
  etr map-server 172.16.1.67 key 7 some-key
  etr map-server 172.16.1.67 proxy-reply
  etr
  map-server
  map-resolver
  exit-service-ethernet
 !
 instance-id 4097
  remote-rloc-probe on-route-change
  service ipv4
   eid-table default
   map-cache 10.92.1.0/24 map-request
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4099
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf CLIENT_VN
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
	router lisp
	 locator-table default
	 locator-set rloc_set2
	  IPv4-interface Loopback0 priority 10 weight
	 10
	  exit-locator-set
	 !
	 locator default-set rloc_set2
	 service ipv4
	  encapsulation vxlan
	  itr map-resolver 172.16.1.67
	  etr map-server 172.16.1.67 key some-key
	  etr map-server 172.16.1.67 proxy-reply
	  etr
	  sgt distribution
	  sgt
	  no map-cache away-eids send-map-request
	  use-petr 172.16.1.67
	  proxy-itr 172.16.1.69
	  exit-service-ipv4
	 !
	 service ethernet
	  itr map-resolver 172.16.1.67
	  itr
	  etr map-server 172.16.1.67 key some-key
	  etr map-server 172.16.1.67 proxy-reply
	  etr
	  exit-service-ethernet
	 !
	 instance-id 4097
	  remote-rloc-probe on-route-change
	  dynamic-eid APVlan92-IPv4
	   database-mapping 10.92.1.0/24 locator-set
	 rloc_set2
	   exit-dynamic-eid
	  !
	  service ipv4
	   eid-table default
	   exit-service-ipv4
	  !
	  exit-instance-id
	 !
	 instance-id 4099
	  remote-rloc-probe on-route-change
	  dynamic-eid wireless-VN-IPV4
	   database-mapping 10.51.1.0/24 locator-set
	 rloc_set2
	   exit-dynamic-eid
	  !
	  service ipv4
	   eid-table vrf CLIENT_VN
	   map-cache 0.0.0.0/0 map-request
	   exit-service-ipv4
	  !
	  exit-instance-id
	 !
	 instance-id 8190
	  remote-rloc-probe on-route-change
	  service ethernet
	   eid-table vlan 1023

Control Plane, Border Node, and Embedded Wireless Controller	Fabric Edge Node
exit-instance-id ! map-server session passive-open WLC site site_uci description map-server1 authentication-key some-key eid-record instance-id 4097 10.92.1.0/24 accept-more-specifics eid-record instance-id 4099 10.51.1.0/24 accept-more-specifics eid-record instance-id 8190 any-mac eid-record instance-id 8191 any-mac exit-site ! ipv4 locator reachability exclude-default ipv4 source-locator Loopback0 exit-router-lisp !! wireless profile fabric diy_open_profile client-l2-vnid 8191 description diy_open_profile wireless profile policy diy_open_profile no central dhcp no central switching description diy_open_profile dhcp-tlv-caching exclusionlist timeout 180 fabric diy_open_profile http-tlv-caching ip nbar protocol-discovery service-policy input platinum-up service-policy output platinum no shutdown wlan diy_open_profile 17 diy_open no security ft adaptive no security wpa no security wpa wpa2 no security wpa wpa2 ciphers aes no security wpa akm dot1x no shutdown ! wireless management interface Loopback0 wireless fabric wireless fabric name APVlan92 l2-vnid 8190 l3-vnid 4097 ip 10.92.1.0 255.255.255.0 control-plane-name default-control-plane wireless fabric name wireless-VN l2-vnid 8191 control-plane-name default-control-plane wireless fabric control-plane default-control-plane ip address 172.16.1.67 key 0 auth-key ! interface Loopback1023 description Loopback Border ip address 10.92.1.1 255.255.255.255 ! interface Loopback1024 description Loopback Border	database-mapping mac locator-set rloc_set2 exit-service-ethernet ! exit-instance-id ! instance-id 8191 remote-rloc-probe on-route-change service ethernet eid-table vlan 1024 database-mapping mac locator-set rloc_set2 exit-service-ethernet ! exit-instance-id ! ipv4 locator reachability minimum-mask-length 32 proxy-etr-only ipv4 source-locator Loopback0 exit-router-lisp snmp-server enable traps ! interface Vlan92 description AP SVI mac-address 0000.0c9f.fcae ip address 10.92.1.1 255.255.255.0 ip helper-address 192.168.132.1 no ip redirects no lisp mobility liveness test lisp mobility APVlan92-IPv4 end interface Vlan51 description Client SVI mac-address 0000.0c9f.fd96 vrf forwarding CLIENT_VN ip address 10.51.1.1 255.255.255.0 ip helper-address 192.168.132.1 no ip redirects no lisp mobility liveness test lisp mobility wireless-VN-IPV4 end ip dhcp snooping vlan 51,92 !

Control Plane, Border Node, and Embedded Wireless Controller	Fabric Edge Node

` vrf forwarding CLIENT_VN`
` ip address 10.51.1.1 255.255.255.255`
`!`
`!`
`router bgp 700`
` bgp router-id interface Loopback0`
` bgp log-neighbor-changes`
` bgp graceful-restart`
` !`
` address-family ipv4`
`  bgp redistribute-internal`
`  bgp aggregate-timer 0`
`  network 10.92.1.1 mask 255.255.255.255`
` exit-address-family`
` !`
` address-family ipv4 vrf CLIENT_VN`
`  bgp aggregate-timer 0`
`  network 10.51.1.1 mask 255.255.255.255`
` exit-address-family`
 	
`!`	