Campus Fabric Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 3850 Switches)

First Published: 2017-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

CHAPTER 1

Campus Fabric

Information about Campus Fabric

Campus Fabric, also refered to as Software Defined Access, provides the basic infrastructure for building virtual networks on policy-based segmentation constructs. It is based on the Locator ID Separator Protocol (LISP) overlay network built on top of an arbitrary underlay network.

Overlay networks can run across all the underlay network devices or a subnet of these devices. Multiple overlay networks can spread across the same underlay network to support multitenancy.

Cisco IOS XE Everest 16.6.1 supports Layer 2 and Layer 3 overlay networks.

Campus Fabric Overlay provisioning uses three components to enable flexible attachment of users and devices, and enhanced security through user-based and device-group based policies:

- Control Plane
- Data Plane
- Policy Plane

The Campus Fabric feature is supported on the Enterprise Services and IP Base software images.

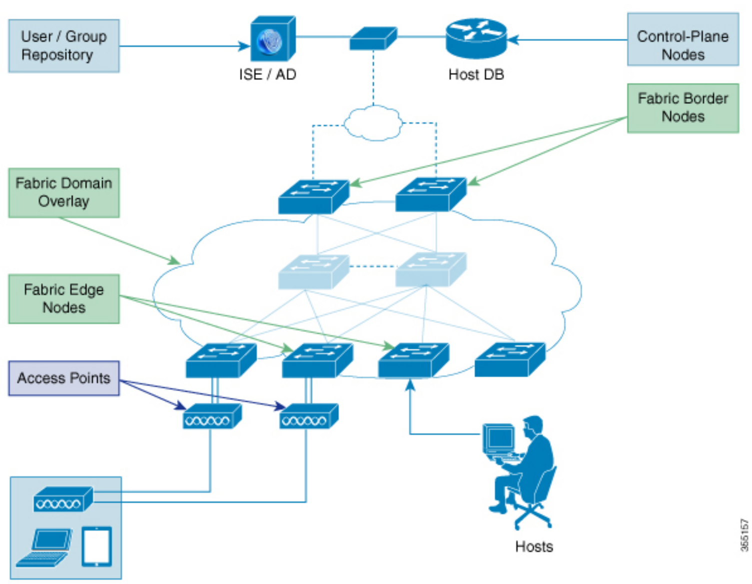
Benefits of Provisioning a Campus Fabric Network

- A hybrid Layer 2 and Layer 3 overlay offers the best of both these services.
- Provides end-to-end segmentation using LISP Virtualization technology wherein only the Fabric Edge and Border nodes have to be LISP aware. The rest of the components are just IP forwarders.
- Eliminates Spanning Tree Protocol (STP), improves link utilization, and brings in faster convergence and equal cost multipath (ECMP) load balancing.
- Fabric header supports Secure Group Tag (SGT) propagation, which helps in having a uniform policy model across the network. SGT-based policy constructs are subnet independent.
- Provides host mobility for both wired and wireless clients.
- Use of LISP helps decouple the host address and its location, simplifying the routing operations, and improving scalability and support.

Understanding Fabric Domain Elements

Figure 1: Elements of a Fabric Domain displays the elements that make up the fabric domain.

Figure 1: Elements of a Fabric Domain



The following is a description of the fabric domain elements illustrated in the Figure 1: Elements of a Fabric Domain.

- Fabric Edge Devices—Provide connectivity to users and devices that connect to the fabric domain. Fabric edge devices identify and authenticate end points, and register end-point ID information in the fabric host-tracking database. These devices encapsulate at ingress and decapsulate at egress, to forward traffic to and from the end points connected to the fabric domain.

- Fabric Control-Plane Devices—Provide overlay reachability information and end points-to-routing locator mapping, in the host-tracking database. A control-plane device receives registrations from fabric edge devices having local end points, and resolves requests from edge devices to locate remote end points. You can configure up to three control-plane devices-internally (a fabric border device) and externally (a designated control-plane device, such as Cisco CSR1000v), to allow redundancy in your network.
- Fabric Border Devices — Connect traditional Layer 3 networks or different fabric domains to the local domain, and translate reachability and policy information, such as virtual routing and forwarding (VRF) and SGT information, from one domain to another.
- Virtual Contexts—Provide virtualization at the device level, using VRF to create multiple instances of Layer 3 routing tables. Contexts or VRFs provide segmentation across IP addresses, allowing for overlapped address space and traffic separation. You can configure up to 32 contexts in the fabric domain.
- Host-Pools—Group end points that are present in the fabric domain into IP pools, and identify them with a VLAN ID and an IP subnet.

Campus Fabric Configuration Guidelines and Limitations

- Configure no more than three control-plane devices in each fabric domain.
- Configure no more than two border devices in each fabric domain..
- Each fabric edge device supports up to 2000 end points.
- Each control-plane device supports up to 5000 fabric edge device registrations.
- Configure no more than 64 virtual contexts in each fabric domain.
- Layer 2 (IPv4 host) and Layer 3 (IPv6 Host) LISP overlay functionality is supported on Cisco IOS XE Everest 16.6.1 and later releases.
- On the edge device, Cisco TrustSec links are not supported on uplink interfaces connected to the underlay.
- Layer 3 source group tags cannot be applied to uplink interfaces connected to the underlay.
- Cisco IOS XE 16.6.1 does not support Dense Mode or Bidirectional Protocol Independent Multicast (PIM). Only PIM Sparse Mode (SM) and PIM Source Specific Multicast (SSM) modes are supported.
- Multicast does not support group-to-rendezvous point (RP) mapping distribution mechanisms, Auto-RP, and Bootstrap Router (BSR). Only Static RP configuration is supported.
- Multicast RP redundancy is not supported in the fabric domain.

Important Virtual Extensible LAN (VXLAN) and LISP must be configured as part of campus fabric network. They are not supported as standalone features.

Campus Fabric: Scale and Performance

- The maximum number of Layer 2 EID VLANs that is possible is 2048.

- The maximum number of local and remote hosts on each fabric edge is 32000.
- The maximum number of access points that can be connected to the fabric is 100.
- The maximum number of wireless clients that a campus fabric can onboard is 2000.

CLI Changes From Cisco IOS XE Everest 16.6.1

Starting Cisco IOS XE Everest 16.6.1, the CLI model for L2 LISP configuration is redesigned to better reflect the configuration flow and to configure LISP behavior that is specific to different functionalities such as support for Layer 2 MAC address as EID prefixes, and so on.

The following is a list of CLI changes:

- The new CLI provides two levels of inheritance in two paths:
    - **router lisp > service**- called the global service or top service mode
    - **router lisp > instance-id > service**-called the instance-service mode
- The end point identifier table,**eid-table**, is decoupled from the **instance-id**. You can now configure **eid-table** without specifying the **instance-id**. The hierarchy is **router lisp > instance-id > service > eid-table.**
- You can have the common configuration under global service mode and instance ID-specific configuration under instance-service mode.
- CLI that is configured at the global level of the hierarchy affects the operational state of all the instance services at lower levels of the hierarchy, unless explicitly overridden.
- All the { ipv4 | ipv6} [proxy] {itr | etr} commands appear under their respective service mode without their address family prefix.
- All the LISP show commands commence with the **show lisp** prefix.
- A new command, **locator default-set**, which is configured at the global level marks one of the locater set as default.
- service-ethernet is a new sub mode that enables Layer 2 MAC ID as EID space.

Note After you enter the commands in the changed configuration style, the earlier CLIs are not supported. To switch to the earlier CLIs, reload the system.

How to Configure Campus Fabric

Configuring Campus Fabric involves the following stages:

- Network Provisioning—Setting up the management plane and the underlay mechanism
- Overlay Provisioning—Setting up the fabric overlay, which includes fabric edge and fabric border devices.

- Policy Management—Setting up virtual contexts or VRFs, end point groups and policies.

Configure Fabric Edge Device

Follow these steps to configure fabric edge devices:

Before You Begin

- Configure a loopback0 IP address for each edge device to ensure that the device is reachable. Ensure that you run the **ip lisp source-locator loopback0** command on the uplink interface.
- Ensure that your underlay configuration is set up.
- Configure control-plane devices and border devices in your fabric domain.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	**locator-table** *name* {**default** | **vrf** *vrf-name*} **Example:** `Switch(config-router-lisp)# locator-table loc-table default`	Associates a virtual routing and forwarding (VRF) table through which the router can reach the locator address space.
Step 4	**locator-set** *name* {*ip-address* {**priority** *priority_value* | **weight** *weight*} | **auto-discover-rlocs** **Example:** `Switch(config-router-lisp-locator-table)# locator-set rloc1 1.1.1.1 priority 1 weight 1`	Specifies a named locator set.
Step 5	**IPv4-interface loopback** *Loopback-address* { **priority** *priority_value* |**weight** *weight*} **Example:** `Switch(config-router-lisp-locator-set)# IPv4-interface loopback0 priority 1 weight 1`	Configure the loopback IP address to ensure that the device is reachable.
Step 6	**exit-locator-set** **Example:** `Switch(config-router-lisp-locator-set)# exit-locator-set`	Exits the locator-set configuration mode.

	Command or Action	Purpose
Step 7	**instance-id** *instance* **Example:** `Switch(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.
Step 8	**dynamic-eid** *dynamic-EID* **Example:** `Switch(config-router-lisp-instance)# dynamic-eid DEFAULT.EID.eng`	Creates the dynamic-eid policy and enters the dynamic-eid configuration mode.
Step 9	**database-mapping** *eid* **locator-set** *RLOC name* **Example:** `Switch(config-router-lisp-instance-dynamic-eid)# database-mapping 10.1.1.0/24 locator-set set1`	Configures EID to RLOC mapping relationship.
Step 10	**exit-dynamic-eid** **Example:** `Switch(config-router-lisp-instance-dynamic-eid)# exit-dynamic-eid`	Exits dynamic-eid configuration mode
Step 11	**service ipv4** **Example:** `Switch(config-router-lisp-instance)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 12	**eid-table vrf** *vrf-table* **Example:** `Switch(config-router-lisp-instance-service)# eid-table vrf vrf2`	Associates the LISP instance ID configured earlier with a VRF table through which the end-point identifier address space is reachable.
Step 13	**map-cache** *destination-eid* **map-request** **Example:** `Switch(config-router-lisp-instance-service)# map-cache 10.1.1.0/24 map-request`	Generates a static map request for the destination EID.
Step 14	**itr map-resolver** *map-resolver-address* **Example:** `Switch(config-router-lisp-instance-service)# itr map-resolver 2.1.1.6`	Configures the map-resolver IP from where it needs to query the RLOC corresponding to destination EID IP.
Step 15	**itr** **Example:** `Switch(config-router-lisp-instance-service)# itr`	Specifies that this device acts as an Ingress Tunnel Router (ITR).
Step 16	**etr map-server** *map-server-addr* **key {0 | 6}** *authentication key*	Configures the locator address of the LISP map server to be used by the Egress Tunnel Router (ETR) when registering the IPv4 EIDs.

	Command or Action	Purpose
	Example: `Switch(config-router-lisp-instance-service)# etr map-server 2.1.1.6 key foo`	
Step 17	**etr** **Example:** `Switch(config-router-lisp-instance-service)# etr`	Specifies that this device acts as an ETR.
Step 18	**use-petr** *locator-address* { **priority** *priority_value* | **weight** *weight_value* **Example:** `Switch(config-router-lisp-instance-service)# use-petr 14.1.1.1`	Configures the device to use Proxy Egress Tunnel Router (PETR).
Step 19	**exit-service-ipv4** **Example:** `Switch(config-router-lisp-instance-service)# exit-service-ipv4`	Exits service submode.
Step 20	**exit-instance-id** **Example:** `Switch(config-router-lisp-instance)# exit-instance-id`	Exits instance submode.

Configure a Fabric Edge Node as an Anycast Switch Virtual Interface (SVI)

Follow these steps to configure a fabric edge node as an anycast SVI:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface** *interface* **Example:** `switch(config)# interface vlan10`	Enters SVI configuration mode.

	Command or Action	Purpose
Step 3	**ip vrf forwarding** *vrf-name* **Example:** `Switch(config-if)# ip vrf forwarding EMP`	Configures VRF on the interface.
Step 4	**ip address** *ipv4-address* **Example:** `Switch(config-if)# ip address 192.168.10.1/24`	Configures IP address on the interface.
Step 5	**ip helper-address** *ipaddress* **Example:** `Switch(config-if)# ip helper-address 172.168.1.1`	DHCP broadcasts will be forwarded as a unicast to this specific helper address rather than be dropped by the router
Step 6	**lisp mobility** **Example:** `Swtich(config-if)# lisp mobility`	Configures the interface to participate in LISP virtual machine mobility, which is dynamic EID roaming.

Configure a Fabric Edge Node as a DHCP Relay Agent

These steps describe how to configure fabric edge as a DHCP relay agent. For more information on configuring DHCP Client-Server in a Campus Fabric, see the *Cisco IOS XE 16.6.1 Configure DHCP for Campus Fabric* document.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ip dhcp snooping** **Example:** `Switch(config)# ip dhcp snooping`	Enables DHCP snooping globally.
Step 3	**ip dhcp snooping vlan** **Example:** `Switch(config-if)# ip dhcp snooping vlan`	Enables DHCP snooping on a specified VLAN.

	Command or Action	Purpose
Step 4	**ip dhcp relay information option** **Example:** `Switch(config-if)# ip dhcp relay information option`	Enables the system to insert the DHCP relay agent information option (Option-82 field) in the messages forwarded to a DHCP server.

Configure a Fabric Border Device

Follow these steps to configure a fabric border device:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	**service ipv4** **Example:** `Switch(config-router-lisp)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 4	**map-cache** *destination-eid* **map-request** **Example:** `Switch(config-router-lisp-service)# map-cache 10.1.0.0/16 map-request`	Specifies the destination EID to which map-requests are sent.
Step 5	**encapsulation vxlan** **Example:** `Switch(config-router-lisp-service)# encapsulation vxlan`	Specifies VXLAN-based encapsulation.
Step 6	**itr map-resolver** *ip-address* **Example:** `Switch(config-router-lisp-service)# itr map-resolver 2.1.1.6`	Configures the locator address of the LISP map resolver to which this device will send Map-Request messages for IPv4 EID-to-RLOC mapping resolutions.

	Command or Action	Purpose
Step 7	**proxy-itr** *locator-address* **Example:** `Switch(config-router-lisp-service)# proxy-itr 7.7.7.7`	Enables the LISP ITR functionality.
Step 8	**proxy-etr** **Example:** `Switch(config-router-lisp-service)# proxy-etr`	Enables the PETR functionality on the device.
Step 9	**exit-service-ipv4** **Example:** `Switch(config-router-lisp-service)# exit-service-ipv4`	Exits service sub-mode.
Step 10	**exit-router-lisp** **Example:** `Switch(config-router-lisp)# exit-router-lisp`	Exits LISP configuration mode.

Configure Fabric Control Plane

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	**site** *site-name* **Example:** `Switch(config-router-lisp)# site fabric`	Configures a LISP site on a control plane device and enters LISP site configuration mode.

	Command or Action	Purpose
Step 4	**authentication-key** *key* **Example:** `Switch(config-router-lisp-site)# authentication-key lisp`	Configures the password used to create the Hashed Message Authentication Code (HMAC) Secure Hash Algorithm (SHA-1) hash for authenticating the map-register messages sent by edge devices when registering with the control-plane device.
Step 5	**eid-record** [**instance-id** *instance-id*] *record* [**route-tag** *tag*] [**accept-more-specifics**] **Example:** `Switch(config-router-lisp-site)# eid-record instance-id 30 10.1.0.0/16`	Configures a host pool or a list of endpoint identifier (EID) prefixes that are allowed in a map-register message sent by the edge device when registering with the control-plane device.
Step 6	**exit-site** **Example:** `Switch(config-router-lisp-site)# exit-site`	Exits LISP site configuration mode and returns to LISP configuration mode.
Step 7	**exit-router-lisp** **Example:** `Switch(config-router-lisp)# exit-router-lisp`	Exits LISP configuration mode.

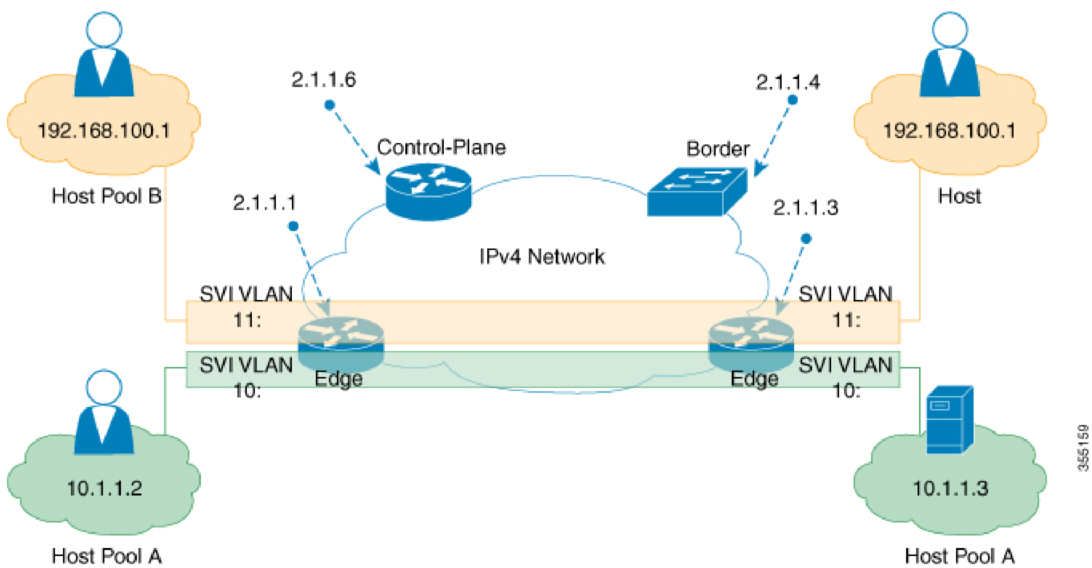
show Commands for Troubleshooting LISP Configuration

- **show lisp** [*router-lisp-id*] {**instance_id** *id* **| eid-table** *table*} {**ipv4 | ipv6 | ethernet**} {**database | map-cache | server** [*address-resolution*]}
- **show lisp instance-id** *id* **ipv4 database**
- **show lisp instance-id** *id* **ipv4 map-cache**
- **show lisp service ipv4 summary**
- **show lisp instance-id** *id* { **ipv4 | ipv6 | ethernet**}
- **show lisp instance-id** *id* **dynamic-eid**

Configuration Examples for LISP Configuration on Fabric Edge Node

Consider the following campus fabric topology:

Figure 2: Sample Campus Fabric topology



The following is the output of **show running-configuration** command on the fabric edge node in the Figure 2: Sample Campus Fabric topology , on page 12

```
interface Loopback0
ip address 2.1.1.1 255.255.255.255
!
interface Vlan10
mac-address ba25.cdf4.ad38
ip address 10.1.1.1 255.255.255.0
lisp mobility DEFAULT.EID.eng
end
!
interface Vlan11
mac-address ba25.cdf4.bd38
ip address 192.168.101.1 255.255.255.0
end
!
router lisp
locator-table default
locator-set set1
IPv4-interface Loopback0 priority 1 weight 1
exit-locator-set
!
locator default-set set1
service ipv4
proxy-itr 2.1.1.6
map-cache 0.0.0.0/0 map-request
itr map-resolver 2.1.1.6
etr map-server 2.1.1.6 key foo
etr map-server 2.1.1.6 proxy-reply
etr
```

```
use-petr 14.1.1.1
exit-service-ipv4
!
service ethernet
proxy-itr 2.1.1.6
map-cache 0.0.0.0/0 map-request
itr map-resolver 2.1.1.6
etr map-server 2.1.1.6 key foo
etr map-server 2.1.1.6 proxy-reply
etr
exit-service-ethernet
!
instance-id 30
dynamic-eid DEFAULT.EID.eng
database-mapping 10.1.1.0/24 locator-set set1
exit-dynamic-eid
!
service ipv4
eid-table default
exit-service-ipv4
!
exit-instance-id
!
instance-id 101
service ethernet
eid-table vlan 10
database-mapping mac locator-set set1
map-cache-limit 1000
database-mapping limit dynamic 2000
proxy-itr 2.1.1.6
map-cache 0.0.0.0/0 map-request
itr map-resolver 2.1.1.6
etr map-server 2.1.1.6 key foo
etr map-cache-ttl 10000
etr
exit-service-ethernet
!
exit-instance-id
!
instance-id 102
service ethernet
eid-table vlan 11
database-mapping mac locator-set set1
map-cache-limit 1000
database-mapping limit dynamic 2000

proxy-itr 2.1.1.6
map-cache 0.0.0.0/0 map-request
itr map-resolver 2.1.1.6
etr map-server 2.1.1.6 key foo
etr map-cache-ttl 10000
etr
exit-service-ethernet
!
exit-instance-id
exit-router-lisp
!
```

The following is the output of **show running-configuration** command on Control Plane in the Figure 2: Sample Campus Fabric topology , on page 12:

```
interface Loopback0
ip address 2.1.1.6 255.255.255.255
!
router lisp
locator-set WLC // enables wireless and access points to be registered.
3.3.3.20
exit-locator-set
!
service ipv4
map-server
map-resolver
exit-service-ipv4
```

```
!
service Ethernet // enables service ethernet on the map-server
map-server
map-resolver
exit-service-ethernet
!
map-server session passive-open WLC
site Shire
authentication-key cisco123
eid-record 10.1.1.0/24 accept-more-specifics
eid-record 20.1.1.0/24 accept-more-specifics
eid-record instance-id 1 any-mac
exit
!
exit-router-lisp
```

The following is the output of **show running-configuration** command on the fabric border node in the Figure 2: Sample Campus Fabric topology , on page 12

```
router lisp
locator-set default.RLOC
IPv4-Interface Loopback0 priority 10 weight 10
exit
!
service ipv4
sgt
itr map-resolver 2.1.1.6
proxy-etr
proxy-itr 2.1.1.4
exit-service-ipv4
!
instance-id 0
service ipv4
eid-table default
map-cache 10.1.1.0/24 map-request
map-cache 20.1.1.0/24 map-request
exit-service-ipv4
!
exit-instance-id
!
instance-id 100
service ipv4
eid-table vrf guest
map-cache 192.168.100.0/24 map-request
exit-service-ipv4
!
exit-instance-id
exit-router-lisp
```

Data Plane Security in Campus Fabric

Campus Fabric Data Plane Security ensures that only traffic from within a fabric domain can be decapsulated, by an edge device at the destination. Edge and border devices in the fabric domain validate that the source Routing Locator (RLOC), or the uplink interface address, carried by the data packet is a member of the fabric domain.

Data Plane Security ensures that the edge device source addresses in the encapsulated data packets cannot be spoofed. Packets from outside the fabric domain carry invalid source RLOCs that are blocked during decapsulation by edge and border devices.

Configure Data Plane Security on an Edge Device

Before You Begin

- Configure a loopback0 IP address for each edge device to ensure that the device is reachable. Ensure that you apply the **ip lisp source-locator loopback0** command to the uplink interface.
- Ensure that your underlay configuration is set up.
- Ensure that you have configured edge, control plane, and border devices.

Procedure

	Command or Action	Purpose
Step 1	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 2	**instance-id** *instance-id* **Example:** `Switch(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configuration under this instance ID applies to all the services underneath it.
Step 3	**decapsulation filter rloc source member** **Example:** `Switch(config-router-lisp-instance)# decapsulation filter rloc source member`	Enables the validation of the source RLOC (uplink interface) addresses of encapsulated packets in the fabric domain.
Step 4	**exit** **Example:** `Switch(config-router-lisp-instance)# exit`	Exits LISP instance configuration mode and returns to LISP configuration mode.
Step 5	**exit** **Example:** `Switch(config-router-lisp)# exit`	Exits LISP configuration mode and returns to global configuration mode.

Configure Data Plane Security on a Control Plane Device

Before You Begin

- Configure a loopback0 IP address for each control plane device to ensure that the device is reachable. Ensure that you apply the **ip lisp source-locator loopback0** command to the uplink interface.

- Ensure that your underlay configuration is set up.
- Ensure that you have configured edge, control-plane, and border devices.

Procedure

	Command or Action	Purpose
Step 1	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 2	**map-server rloc members distribute** **Example:** `Switch(config-router-lisp)# map-server rloc members distribute`	Enables the distribution of the list of EID prefixes, to the edge devices in the fabric domain.
Step 3	**exit** **Example:** `Switch(config-router-lisp)# exit`	Exits LISP configuration mode.
Step 4	**show lisp** [**session** [**established**] | **vrf** [*vrf-name* [**session** [*peer-address*]]]] **Example:** `Switch# show lisp session`	Displays reliable transport session information. If there is more than one transport session, the corresponding information is displayed.
Step 5	**show lisp decapsulation filter** [*IPv4-rloc-address* | *IPv6-rloc-address*] [**eid-table** *eid-table-vrf* | **instance-id** *iid*] **Example:** show lisp decapsulation filter	Displays the uplink interface address configuration details that are manually configured or discovered.

Configure a Fabric Border Device

Follow these steps to configure a fabric border device:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	**service ipv4** **Example:** `Switch(config-router-lisp)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 4	**map-cache** *destination-eid* **map-request** **Example:** `Switch(config-router-lisp-service)# map-cache 10.1.0.0/16 map-request`	Specifies the destination EID to which map-requests are sent.
Step 5	**encapsulation vxlan** **Example:** `Switch(config-router-lisp-service)# encapsulation vxlan`	Specifies VXLAN-based encapsulation.
Step 6	**itr map-resolver** *ip-address* **Example:** `Switch(config-router-lisp-service)# itr map-resolver 2.1.1.6`	Configures the locator address of the LISP map resolver to which this device will send Map-Request messages for IPv4 EID-to-RLOC mapping resolutions.
Step 7	**proxy-itr** *locator-address* **Example:** `Switch(config-router-lisp-service)# proxy-itr 7.7.7.7`	Enables the LISP ITR functionality.
Step 8	**proxy-etr** **Example:** `Switch(config-router-lisp-service)# proxy-etr`	Enables the PETR functionality on the device.
Step 9	**exit-service-ipv4** **Example:** `Switch(config-router-lisp-service)# exit-service-ipv4`	Exits service sub-mode.
Step 10	**exit-router-lisp** **Example:** `Switch(config-router-lisp)# exit-router-lisp`	Exits LISP configuration mode.

Security Group Tags and Policy Enforcement in Campus Fabric

Campus Fabric overlay propagates source group tags (SGTs) across devices in the fabric domain. Packets are encapsulated using virtual extensible LAN (VXLAN) and carry the SGT information in the header. The SGT mapped to the IP address of the edge device is carried within the encapsulated packet and propagated to the destination device, where the packet is decapsulated and the Source Group Access Control List (SGACL) policy is enforced.

For more information on Cisco TrustSec and Source Group Tags, see the Cisco TrustSec Switch Configuration Guide

Multicast Using Campus Fabric Overlay

You can use Campus Fabric overlay to carry multicast traffic over core networks that do not have native multicast capabilities. Campus Fabric overlay allows unicast transport of multicast traffic with head-end replication in the edge device.

Note Only Protocol Independent Multicast (PIM) Sparse Mode and PIM Source Specific Multicast (SSM) are supported in Campus Fabric; dense mode is not supported.

Information about LISP Multicast

LISP multicast includes the following features:

- Mapping of multicast source addresses as LISP EIDs. (Destination group addresses are not topology dependent.)
- Building the multicast distribution tree across LISP overlays.
- Unicast head-end replication of multicast data packets from sources within a root ingress tunnel router site to receiver egress tunnel route.
- Support for Any Source Multicast (ASM) and Source Specific Multicast (SSM) service models for unicast replication. Support for only SSM in core tree for multicast replication.
- Support for various combinations of LISP and non-LISP capable source and receiver sites.
- Support for IPv6 EIDs with head-end replication multicast mode.
- IPv6 multicast routing is supported only in default VRF.
- By default, IPv6 multicast is enabled on IPv6 interfaces. Hence, EID-facing interface does not require explicit IPv6 multicast configuration.

Note If a LISP xTR is also a PIM First Hop Router (FH) or a Rendezvous Point (RP), and the device is only receiving traffic, ensure that at least one interface on the device is covered by local LISP database mapping. No additional configuration is required to ensure that the proper address is selected.

Configure IPv4 Layer 3 LISP Multicast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast-routing** **Example:** `Switch(config)# ip multicast-routing`	Enables IP multicast routing.
Step 3	Enter one of the following: • **ip pim rp-address** *rp-address* • **ip pim ssm {default | range** *{access-list-name | access-list-number}* **Example:** `Switch(config-if)# ip pim rp-address 66.66.66.66`	Statically configures the address of a PIM RP for multicast groups. Defines the Source Specific Multicast (SSM) range of IP multicast addresses.
Step 4	**interface** *LISP-interface number* **Example:** `Switch(config-if)# interface lisp0`	Specifies the LISP interface and the subinterface on which to enable PIM sparse mode.
Step 5	Enter one of the following: • **ip pim sparse-mode** • **ip pim transport multicast** **Example:** `Switch(config-if)# ip pim sparse-mode`	Enables PIM on the interface for the sparse-mode operation. Enables PIM on the interface for the sparse-mode operation. Use the **ip pim transport multicast** command when the core network has native multicast capabilities.
Step 6	**exit** **Example:** `Swtich(config-if)# exit`	Exits the interface configuration mode and enters global configuration mode.
Step 7	**interface** *interface-type interface-number* **Example:** `Switch(config)# interface GigabitEthernet0/1`	Configures the interface facing the end point, and enters interface configuration mode.

	Command or Action	Purpose
Step 8	**ip pim sparse-mode** **Example:** `Switch(config-if)# ip pim sparse-mode`	Enables PIM on the interface for sparse-mode operation.
Step 9	**end** **Example:** `Swtich(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

Configure Layer 2 Overlay Broadcast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	**instance-id** *instance* **Example:** `Switch(config-router-lisp)# instance-id 0`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id applies to all services underneath it.
Step 4	**service ethernet** **Example:** `Switch(config-router-lisp-instance)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 5	**eid-table vlan** *vlan-number* **Example:** `Switch(config-router-lisp-instance-service)# eid-table vlan 3`	Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.
Step 6	**broadcast-underlay** *multicast-group* **Example:** `Switch(config-router-lisp-instance-service)# broadcast-underlay 225.1.1.1`	Specifies the multicast group used by the underlay to carry the overlay Layer 2 broadcast traffic.

	Command or Action	Purpose
Step 7	exit-service-ethernet **Example:** `Switch(config-router-lisp-instance-service)# exit-service-ethernet`	Exits service sub mode.
Step 8	**exit-instance-id** **Example:** `Switch(config-router-lisp-instance)# exit-instance-id`	Exits instance mode..

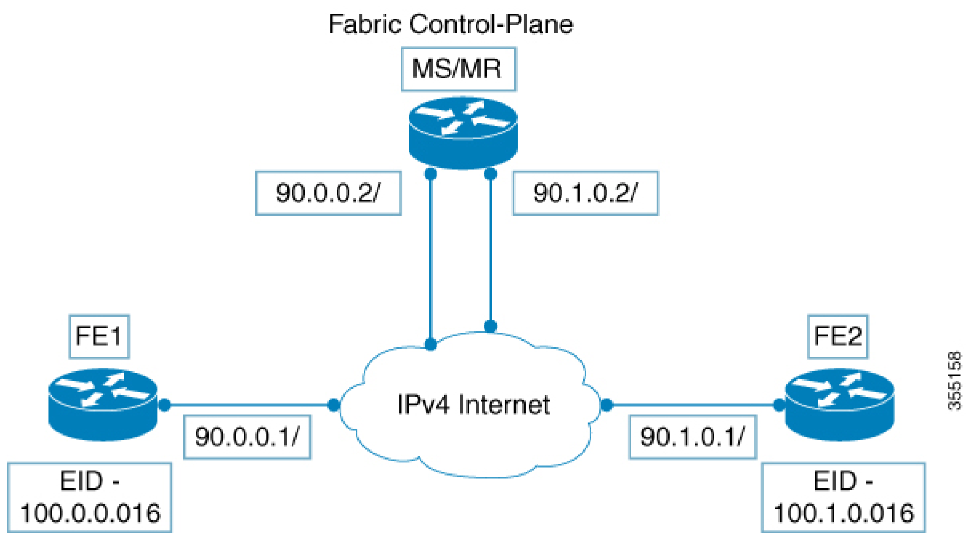
show Commands for Troubleshooting LISP Multicast Configuration

- **show ip pim vrf vrf_name rp mapping**
- **show ip pim vrf vrf_name neighbor**
- **show ip pim vrf vrf_name tunnel**
- **show ip mroute vrf vrf_name**
- **show ip mfib vrf vrf_name**
- **show ip mfib vrf vrf_name count**
- **show ip multicast interface**

Configuration Examples for LISP Multicast

Consider the following topology in campus fabric:

Figure 3: Campus Fabric Topology to Configure Multicast



The following is a sample configuration of LISP multicast on fabric edge node FE1 in the figure Figure 3: Campus Fabric Topology to Configure Multicast, on page 22

```
ip multicast-routing
ip pim ssm default
!
interface Loopback0
ip address 11.1.1.1 255.0.0.0
!
interface Loopback100
ip address 66.66.66.66 255.255.255.255
ip pim sparse-mode
!
interface GigabitEthernet0/1
ip address 90.0.0.1 255.255.255.0
ip pim sparse-mode
!
Interface Vlan100
ip address 100.0.0.1 255.255.0.0
no ip redirects
ip local-proxy-arp
ip pim sparse-mode
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility vl_100
ip pim sparse-mode
!
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
!
!
interface LISP0
ip pim sparse-mode
ip pim lisp transport multicast

!
```

```
router lisp
locator-table default
locator-set rloc_1
  IPv4-interface Loopback0 priority 1 weight 1
  exit-locator-set
!
instance-id 0
  dynamic-eid vl_100
   database-mapping 100.0.0.0/16 locator-set rloc_1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   database-mapping 66.66.66.66/32 locator-set rloc_1
   itr map-resolver 30.3.1.1
   itr
   etr map-server 30.3.1.1 key lisp
   etr
   use-petr 14.1.1.1
   exit-service-ipv4
  !
  exit-instance-id
!
encapsulation vxlan
exit-router-lisp
!
ip pim rp-address 66.66.66.66
```

The following is a sample configuration of control plane (MS/MR) in Figure 3: Campus Fabric Topology to Configure Multicast, on page 22

```
interface Loopback0
ip address 30.3.1.1 255.255.255.255
!
interface GigabitEthernet0/1
ip address 90.0.0.2 255.255.255.0
Ip pim sparse-mode
!
interface GigabitEthernet0/2
ip address 90.1.0.2 255.255.255.0
Ip pim sparse-mode
!
router lisp
site Fabric
authentication-key lisp
eid-record 100.0.0.0/16 accept-more-specifics
eid-record 66.66.66.66/32 accept-more-specifics
eid-record 77.77.77.77/32 accept-more-specifics
eid-record 88.88.88.88/32 accept-more-specifics
exit
!
ipv4 map-server
ipv4 map-resolver
exit
```

Feature History for Campus Fabric

Release	Modification
Cisco IOS XE Denali 16.3.2	This feature was introduced with support for auto commands.
Cisco IOS XE Everest 16.6.1	Support for **auto** commands removed. New mode of CLI introduced.

CHAPTER 2

Software-Defined Access Wireless

Introduction to 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.

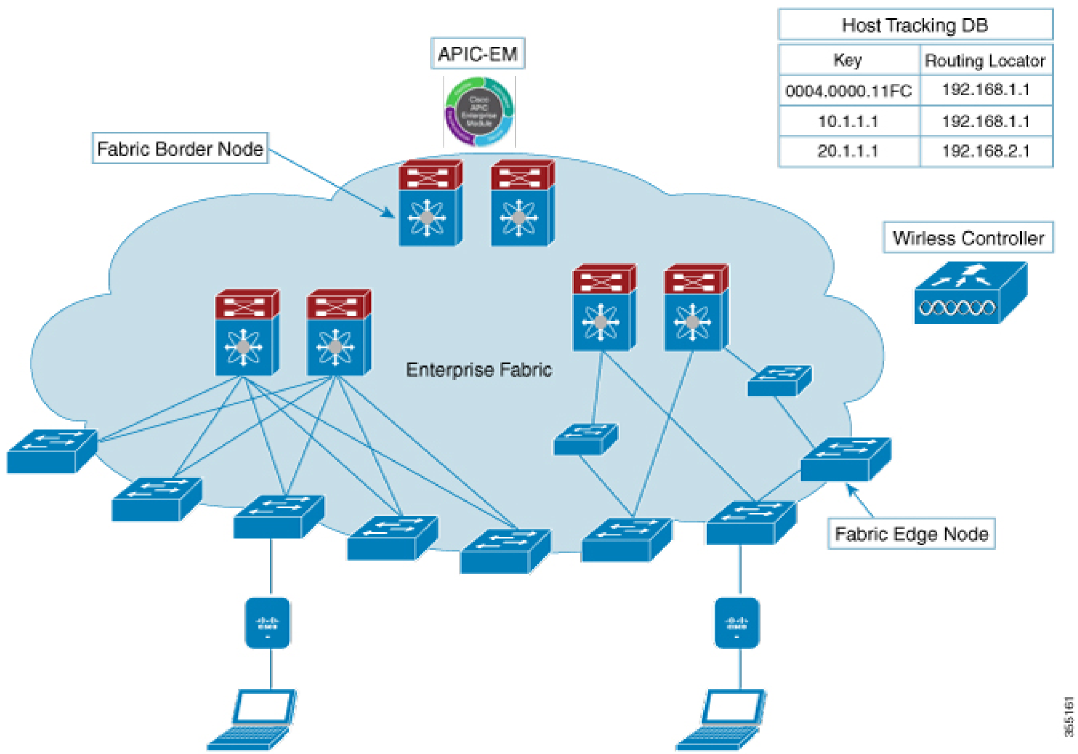
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which 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 (WLC), Application Policy Infrastructure Controller - Enterprise Module (APIC-EM), and Host Tracking Database (HDB).

Figure 4: Software-Defined Access Wireless



APIC-EM Controller: Fabric service, developed on the APIC-EM controller, drives the management and orchestration of enterprise fabric. It also provisions policies for attached users and devices.

Host ID Tracking Database(map-server and map-resolver in LISP): 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 WLC 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, etc. It establishes CAPWAP control and data tunnel to WLC. 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

AP Bring-up Process

The sequence of bringing up an AP is given below:

- Switch powers up the AP (POE or UPOE)
- AP gets an IP address from the DHCP server.
- Switch registers the IP address of the AP with the map server.
- AP discovers Cisco WLC through CAPWAP discovery.
- After Datagram Transport Layer Security (DTLS) handshake, CAPWAP control tunnel is created between AP and Cisco WLC for control packets. CAPWAP data tunnel is created for IEEE 802.11 management frames. The AP image is downloaded and the configuration is pushed on AP from controller.
- Cisco WLC queries the map server for the switch (RLOC IP) behind which the AP has been registered.
- Cisco WLC registers a dummy MAC address with the map server.
- Map server sends a dummy MAC address notification to the switch to create a VXLAN tunnel to AP.
- AP is ready to accept clients.

Onboarding the Wireless Clients

The sequence of on boarding the clients are given below:

- The wireless client associates itself to the AP.
- Client starts IEEE 802.1x authentication on Cisco WLC (if configured) using CAPWAP data tunnel.
- After Layer 2 authentication is complete, Cisco WLC registers MAC address of the client with map server.
- Map server sends a notify message to switch with the client details.
- Switch adds the client mac to the Layer 2 forwarding table.

- Client gets an IP address from DHCP server.
- AP sends IP address of the client to Cisco WLC.
- Cisco WLC moves the client to RUN state and the client can start sending traffic.
- Switch registesr the IP address of the client to the MAP server.
- The switch decapsulates the VXLAN packet.
- The switch forwards the DHCP packet to the DHCP server or relay.
- The switch receives the DHCP ack for the wireless client. Switch learns the IP address of the client and sends an update to the map server.
- Switch broadcasts the DHCP ack to all ports in the VLAN, including the AP facing VXLAN tunnels.
- DHCP ack reaches AP, which forwards it to client.
- AP sends IP address of the client to WLC.
- Cisco WLC puts the client in RUN state.

Platform Support

Table 1: Supported AireOS Controllers

Controller	Support
2504	No
3504	Yes
5508	No
WiSM2	No
8510	Supported only on the local mode AP
5520	Supported only on the local mode AP
8540	Supported only on the local mode AP
7510	No
vWLC	No

Table 2: AP Support

AP	Support
11N	No

AP	Support
11AC Wave 1	Yes
11AC Wave 2	Yes
Mesh	No

Table 3: Client Security

Security	Support
Open and Static WEP	No
WPA-PSK	Yes
802.1x (WPA/WPA2)	Yes
MAC Filtering	Yes
CCKM Fast Roaming	Yes
Local EAP	Yes. However, it is not recommended.
AAA Override	Supported for SGT, L2 VNID, ACL policy, and QoS policy.
Internal WebAuth	IPv4 clients
External Webauth	IPv4 clients
Pre Auth ACL	IPv4 clients
FQDN ACL	No

Table 4: IPv6 Support

IPv6	Support
IPv6 Infra Support	No
IPv6 Client Support	No

Table 5: Polciy, QoS, and Feature Support

Features	Support
IPv4 ACL for Clients	Yes. Flex ACL for ACL at AP.
IPv6 ACL for Clients	No
P2P Blocking	Supported through security group tag (SGT) and security group ACL (SGACL) on the switch for clients on the same AP.
IP Source Guard	Switches
AVC Visibility	AP
AVC QOS	AP
Downloadable Protocol Pack updates	No
Device profiling	No
mDNS Proxy	No
MS Lync Server QOS Integration	No
Netflow Exporter	No
QOS	Yes (Metal profiles and rate limiting)
Passive Client/Silent Host	No
Location tracking / Halo	Yes
Wireless Multicast	Yes. Video streaming is not supported.
URL Filtering	No
HA	WLC to WLC

Migration From Converged Access

The following list shows the migration process from converged access to fabric wireless:

1. Bring up the WLC with image supporting fabric mode.
2. Configure the network with the fabric mode for the appropriate subnets, using an APIC-EM or CLIs. We recommed that you use APIC-EM for this purpose.

3 Configure the discovery mechanism such that the DHCP discovery on the new AP subnet should lead to the controller supporting fabric mode.

4 When the AP comes up, do a DHCP request and get the IP address in the AP VLAN.

5 The AP creates a control plane CAPWAP tunnel with the WLC.

6 Based on the configuration, the WLC programs the AP for the fabric mode.

7 After this, AP follows the SDA for wireless flow.

Note Mobility between fabric and non-fabric SSIDs are not supported

Note AP images and licenses are hosted on the Cisco WLC and the AP fetches the images and licenses directly from it. APIC-EM is responsible for managing the AP licenses on the Cisco WLC.

Note After a TCP connection flap in the WLC, it takes about five to six minutes to reestablish the connection. During this time, the access tunnels gets reset during client join.

Configuring SD-Access Wireless (CLI)

Perform the following steps to configure fabric on a WLAN.

Before You Begin

- Configure the AP in local mode to enable fabric on it.

Procedure

Step 1 **config wlan fabric enable** *wlanid*

Example:
```
config wlan fabric enable wlan1
```
Enables Fabric on the WLAN.

Step 2 **config wlan fabric vnid** *vnid wlanid*

Example:
```
config wlan fabric vnid 10 wlan1
```
Configures a Virtual Extensible LAN (VXLAN) network identifier (VNID) on fabric WLAN.

Step 3 **config wlan fabric encap vxlan** *wlanid*

Example:
```
config wlan fabric encap vxlan wlan1
```
Maps a VNID to the fabric WLAN.

Step 4 **config wlan fabric switch-ip** *ip-address wlanid*

Example:
```
config wlan fabric switch-ip 1.1.1.1 wlan1
```
Sets a VLAN peer ip to WLAN.

Step 5 **config wlan fabric acl** *fabric-acl-name wlanid*

Example:
```
config wlan fabric acl fabric-acl wlan1
```
Configures a flex ACL on the WLC and associates it with the fabric WLAN.

Step 6 **config wlan fabric avc-policy** *fabric-avc-policy wlanid*

Example:
```
config wlan fabric fabric-avc-policy wlan1
```
Configures an AVC profile name associates it with the fabric WLAN.

Step 7 **config wlan fabric controlplane guest-fabric enable** *wlanid*

Example:
```
config wlan fabric controlplane guest-fabric enable wlan1
```
(Optional) Enables guest fabric for this WLAN .

Step 8 **show fabric summary**

Example:
```
show fabric summary
```
(Optional) Displays the fabric configuration summary.

CHAPTER 3

Configure DHCP in Campus Fabric

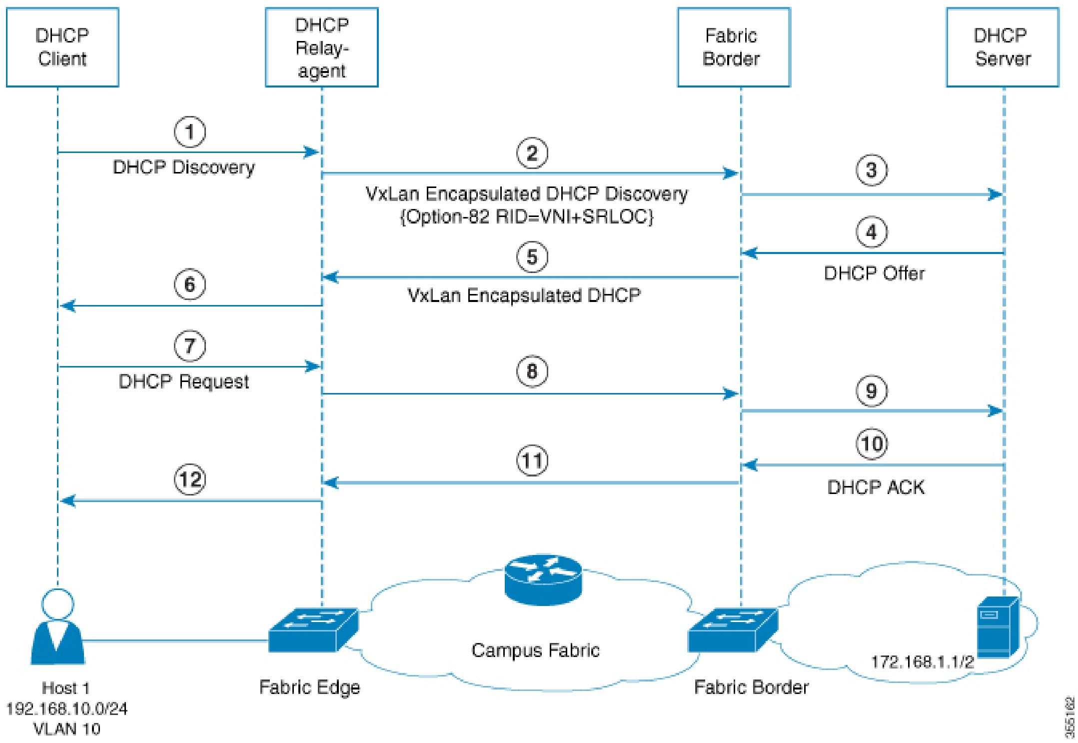
DHCP Configuration for Campus Fabric

In a Campus fabric network, DHCP server is deployed as a shared service located in a network that is different from the fabric endpoints. Every fabric edge is configured as a DHCP Relay agent to relay the DHCP traffic between fabric endpoints and DHCP server. DHCP server is located in the non-EID space in the enterprise fabric network and the fabric edge node uses the fabric border as Proxy Tunnel Router (PxTR) to communicate with the DHCP server.

DHCP solution deployment in Campus Fabric is based on Fabric Anycast Gateway model where the Gateway IP for the clients is an anycast Switched Virtual Interface (SVI) IP address configured on all the fabric edge nodes. DHCP is implemented in layer 3 overlay with anycast address support and network address transparency.

DHCP Packet Flow

Figure 5:



In this topology that implements Option-82 Remote-ID Suboption for DHCP:

- Fabric edge node is configured as LISP Ingress or Egress Tunnel Router (xTR) with locator address as 1.1.1.1
- Fabric border node is configured as LISP Proxy Tunnel Router (PxTR).
- Host 1 is the DHCP client attached to fabric edge, VLAN 10, prefix 192.168.10.0/24.
- Layer 3 interface (SVI) connects to mobility subnet, interface VLAN 10.
- DHCP relay agent configured for SVI VLAN 10 on fabric edge node.
- DHCP server attached to the native network and its address is 172.168.1.1/24, reachable via fabric border node.

Sequence of Operations in Assigning IP Address to DHCP Client in Campus Fabric Network

DHCP Client: (Host 1)

1. Host 1 generates a DHCP discovery message and broadcasts it on the network.

DHCP Relay Agent

2. The DHCP relay agent (fabric edge node) intercepts the packet, and sets the following fields in the packet:

- GIADDR: Set to incoming Anycast SVI interface IP address (192.168.10.1).
- Option-82 Remote-ID Sub Option: String encoded as "SRLOC IPv4 address" and "VxLAN L3 VNI ID" associated with Client segment.

  Locator address is set to 1.1.1.1

  L3 VNI ID is set to 20
- Circuit ID Suboption: Encoded in VLAN-PORT-Module format, with VLAN=10, Port/Module set to incoming port and switch number.

3. Builds the DHCP message by re-writing the inner DHCP source address, inner VXLAN Mac header, VXLAN header, UDP header, Outer IP header, and Outer L2 Header. It then forwards this VxLAN encapsulated DHCP unicast packet to the fabric border node.

Fabric Border Node:

4. Fabric Border device decapsulates the VXLAN encapsulated DHCP packet and natively forwards the packets destined to DHCP server address, to the next-hop router.

DHCP Server:

5. The following process occurs on the DHCP server after receiving the DHCP packet from the DHCP relay agent:

- DHCP server selects the IP pool (192.168.10.0/24) based on the value of GIADDR (192.168.10.1) set in the incoming message.
- Allocates IP address (192.168.10.2) from the IP pool.
- Generates DHCP OFFER messages, with the destination address set to the value of GIADDR received. This is piggy-backed with the Option-82 sub-options that incude Circuit ID and Remote ID.

6. DHCP server routes the DHCP reply packets toward the DHCP relay agent through the fabric border. (Fabric border is the entry point for all in-bound traffic toward the fabric).

Fabric Border Node:

7. Fabric border node configured as LISP PxTR acts as an ingress LISP tunnel router for all packets destined to the fabric subnets. When it receives the DHCP reply message (DHCP OFFER) destined to DHCP relay agent address, the fabric border device makes the DHCP OFFER message VXLAN encapsulated using the Option 82 Remote ID fields (Src RLOC IP and VNI fields) and forwards it to the DHCP relay agent.

DHCP Relay agent:

8. DHCP relay agent receives the DHCP OFFER packet, processes it and forwards it to the client.

DHCP Client:

9. DHCP client receives the DHCP OFFER packet, and initiates DHCP request packet to request for the IP address (192.168.10.2).

The DHCP Request packet is then treated the same way as explained in steps 2 to 4 until it reaches the DHCP server.

The DHCP server does a regular processing of DHCP request packet and sends back a DHCP ACK to the DHCP relay agent. DHCP ACK follows the same forwarding procedure as mentioned in steps 5 to 9.

How to Configure DHCP Client / Server

The following configuration can be done in any order. Ensure that the device is configured before on-boarding a host.

Configure a Fabric Edge Node as a DHCP Relay Agent

These steps describe how to configure fabric edge as a DHCP relay agent. For more information on configuring DHCP Client-Server in a Campus Fabric, see the *Cisco IOS XE 16.6.1 Configure DHCP for Campus Fabric* document.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ip dhcp snooping** **Example:** `Switch(config)# ip dhcp snooping`	Enables DHCP snooping globally.
Step 3	**ip dhcp snooping vlan** **Example:** `Switch(config-if)# ip dhcp snooping vlan`	Enables DHCP snooping on a specified VLAN.
Step 4	**ip dhcp relay information option** **Example:** `Switch(config-if)# ip dhcp relay information option`	Enables the system to insert the DHCP relay agent information option (Option-82 field) in the messages forwarded to a DHCP server.

Configure Fabric Edge Node as Anycast SVI

Procedure

	Command or Action	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **interface** *interface*	Enters SVI configuration mode.
Step 3	Switch(config-if)# **ip vrf forwarding** *vrf-name*	Configures VRF on the interface.
Step 4	Switch(config-if)# **ip address** *ip address*	Configures the IP address on the interface..
Step 5	Switch(config-if)# **ip helper-address** *ipaddress*	DHCP broadcasts will be forwarded as a unicast to this specific helper address rather than be dropped by the router.
Step 6	Switch(config-if)# **lisp mobility** *dynamic-EID*	Configures the interface to participate in LISP virtual machine mobility which is dynamic-EID roaming.
Step 7	Switch(config-if)# **no lisp mobility liveness test**	Disables the liveness test on the interface.

Configure LISP on the Fabric Edge node

Follow these steps to configure fabric edge devices:

Procedure

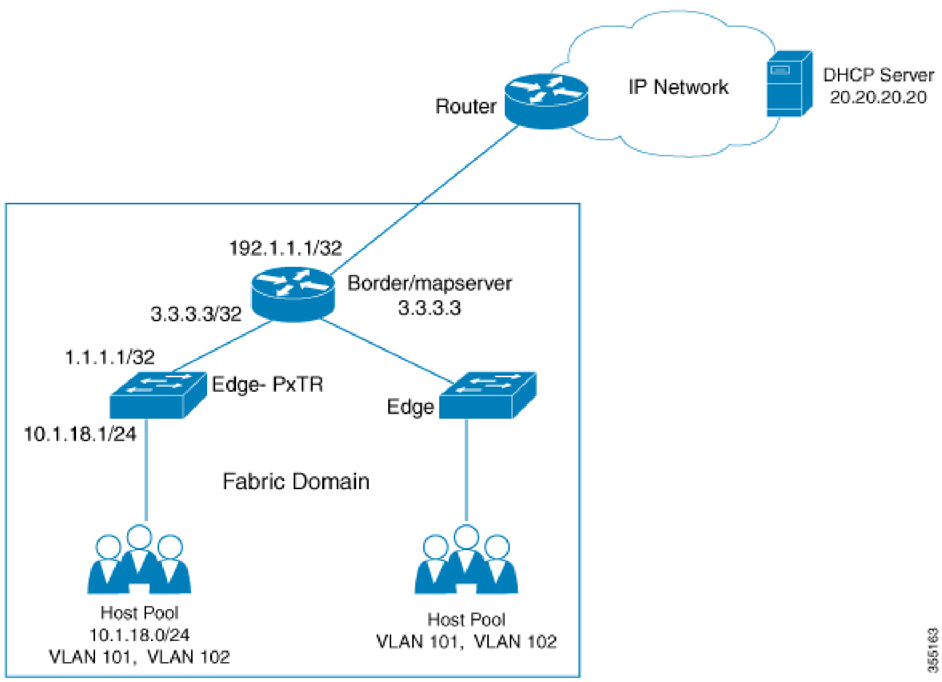
	Command or Action	Purpose
Step 1	switch#**configure terminal**	Enters the global configuration mode.
Step 2	switch(config)#**router lisp**	Enters LISP configuration mode.
Step 3	Switch(config-router-lisp)#**locator-set** *name*	Specifies a named locator set.
Step 4	Switch(config-router-lisp-locator-set)# **IPv4-interface loopback** *Loopback-address* { **priority** *priority_value* |**weight** *weight*}	Configure the loopback ip address to ensure the device is reachable.

	Command or Action	Purpose
Step 5	Switch(config-router-lisp-locator-set)#**exit-locator-set**	Exits the locator-set configuration mode.
Step 6	Switch(config-router-lisp)#**instance-id** *instance*	Creates a LISP EID instance to group multiple services. Configuration under this instance-id will apply to all services underneath it.
Step 7	Switch(config-router-lisp-instance)#**dynamic-eid** *dynamic-EID*	Creates the dynamic-eid policy and enters the dynamic-eid configuration mode.
Step 8	Switch(config-router-lisp-instance-dynamic-eid)#**database-mapping** *eid* **locator-set** *RLOC name*	Configures EID to RLOC mapping relationship.
Step 9	Switch(config-router-lisp-instance-dynamic-eid)#**exit-dynamic-eid**	Exits the dynamic-eid configuration mode
Step 10	Switch(config-router-lisp-instance)#**service ipv4**	Enables layer 3 network services for the IPv4 Address family and enters the service submode.
Step 11	Switch(config-router-lisp-instance-service)#**eid-table vrf** *vrf-table*	Associates the LISP instance-id configured earlier with a virtual routing and forwarding (VRF) table through which the endpoint identifier address space is reachable.
Step 12	Switch(config-router-lisp-instance-service)#**map-cache** *destination-eid* **map-request**	Generates a static map request for the destination-eid.
Step 13	Switch(config-router-lisp-instance-service)#**itr map-resolver** *map-resolver-address*	Configures the map-resolver IP from where it needs to query the RLOC corresponding to destination endpoint identifier (EID) IP.
Step 14	Switch(config-router-lisp-instance-service)#**itr**	Specifies that this device acts as an Ingress Tunnel Router (ITR).
Step 15	Switch(config-router-lisp-instance-service)#**etr map-server** *map-server-addr* **key {0 | 6}** *authentication key*	Configures the locator address of the LISP map server to be used by the Egress Tunnel Router (ETR)

	Command or Action	Purpose
		when registering the IPv4 endpoint identifiers.
Step 16	Switch(config-router-lisp-instance-service)#**etr**	Specifies that this device acts as an Egress Tunnel Router (ETR).
Step 17	Switch(config-router-lisp-instance-service)#**use-petr** *locator-address* { **priority** *priority_value* | **weight** *weight_value*}	Configures the device to use Proxy Egress Tunnel Router (PETR).
Step 18	Switch(config-router-lisp-instance-service)#**exit-service-ipv4**	Exits the service submode.
Step 19	Switch(config-router-lisp-instance)# **exit-instance-id**	Exits the instance submode.

DHCP Configuration Example

Consider the following topology:



Configure Loopback 0 on the fabric edge node

```
Configure terminal
interface loopback 0
ip address 1.1.1.1/32
exit
```

Configure fabric edge as Proxy ITR with a 0/0 map-cache for the DHCP request to be sent in the Overlay.

```
router lisp
 locator-set edge1
 IPv4-interface loopback 0
 exit-locator-set
 !
 instance-id 4098
  dynamic-eid user
   database-mapping 10.1.18.0/24 locator-set edge1
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf User
   map-cache 0.0.0.0/0 map-request
   itr map-resolver 3.3.3.3
   proxy-itr 1.1.1.1
   etr map-server 3.3.3.3 key uci
   etr
   use-petr 3.3.3.3
   exit-service-ipv4
  !
  exit-instance-id
!
exit-router-lisp
```

Enable DHCP snooping on all the VLANs in the fabric

```
ip dhcp relay information option
ip dhcp snooping
ip dhcp snooping vlan 101
```

Discover/Request Packets are sent via overlay in VRF "dhcp" destined to 20.20.20.20 (DHCP Server IP). Configure the DHCP server helper address under the SVI which is the gateway.

```
interface Vlan101
 ip vrf forwarding User
 ip address 10.1.18.1 255.255.255.0
 ip helper-address 20.20.20.20
 no lisp mobility liveness test
 lisp mobility user
end
```

Configure host facing ports on the fabric edge.

```
interface GigabitEthernet1/0/38
 description conn_IX_0104
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast
end
```

Configure fabric border which is also the Mapserver router that connects to the network where DHCP server is located.

```
router lisp
locator-table default
locator-set border
  IPv4-interface Loopback0 priority 10 weight 10
!
instance-id 4098
  service ipv4
   eid-table vrf PACAF
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
  exit-service-ipv4
  !
exit-instance-id
```

```
router bgp 65002
 bgp log-neighbor-changes
!
address-family ipv4 vrf USER
  aggregate-address 10.1.18.0 255.255.255.0 summary-only
  redistribute lisp metric 10
  neighbor 30.1.1.1 remote-as 200
  exit-address-family
```

Create Loopback interface for Anycast SVI IP Address per VNI at the border to facilitate punting the DHCP packets received from the DHCP server to the CPU.

```
interface Loopback3000
 vrf forwarding User
 ip address 10.1.18.1 255.255.255.255
end
```

Advertise Anycast SVI address to BGP peers.

```
router bgp 100
 address-family ipv4 vrf User
  bgp router-id 23.1.1.1
  network 10.1.18.1 mask 255.255.255.255
  aggregate-address 10.1.18.0 255.255.0.0 summary-only
  redistribute lisp metric 10
  neighbor 23.1.1.2 remote-as 200
  neighbor 23.1.1.2 ebgp-multihop 3
  neighbor 23.1.1.2 activate
 exit-address-family
```

Create DHCP Pool. On the DHCP server, ensure that the default-router IP address is the SVI gateway within LISP.

```
ip dhcp excluded-address 10.1.18.1
ip dhcp excluded-address 10.1.18.202 10.1.18.255
!

ip dhcp pool User
   network 10.1.18.0 255.255.255.0
   default-router 10.1.18.1
!
```

Feature History for DHCP Solution in Campus Fabric

Release	Modification
Cisco IOS XE Everest 16.6.1	This feature was introduced.