Configuring Campus Fabric

Campus Fabric provides the basic infrastructure for building virtual networks based on policy-based segmentation constructs.

Note Beginning with Cisco IOS Release 3.9.1E, Campus Fabric is supported on Cisco Catalyst 4500-E series switches on Supervisor Engine 8-E.
Campus Fabric is not supported on Supervisor Engines 7-E, 7L-E, 8L-E, and on Cisco Catalyst 4500-X series switches.

This chapter includes the following major sections:

Note For complete syntax and usage information for the switch commands used in this chapter, see the Cisco IOS Command Reference Guides for the Catalyst 4500 Series Switch.

About Campus Fabric

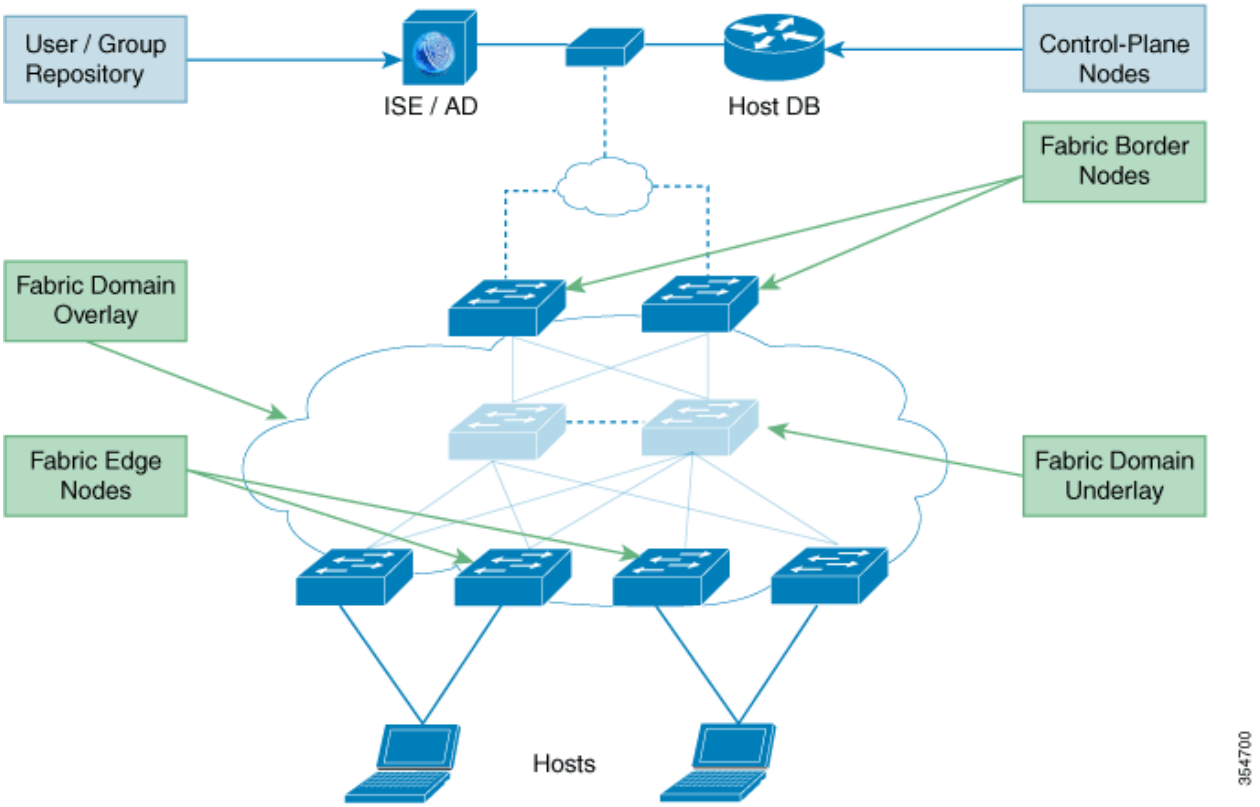
Campus Fabric Overlay provisioning uses three components to enable flexible attachment of users and devices, and enhanced security through user-based and device-group based policies:

- Control-Plane
- Data-Plane
- Policy-Plane

This feature is supported on the Enterprise Services software image.

Understanding Fabric Domain Elements

The following figure displays the elements that make up the fabric domain.



- Fabric Edge Devices — Provide connectivity to users and devices that connect to the fabric domain. Fabric edge devices identify and authenticate endpoints, and register endpoint ID information in the fabric host-tracking database. They encapsulate at ingress and decapsulate at egress, to forward traffic to and from endpoints connected to the fabric domain.
- Fabric Control-Plane Devices — Provide overlay reachability information and endpoints-to-routing-locator mapping, in the host-tracking database. The control-plane device receives registrations from fabric edge devices with local endpoints, and resolves requests from edge devices to locate remote endpoints. You can configure a total of 3 control-plane devices, internally (a fabric border device) and externally (a designated control-plane device such as a Cisco CSR1000v), to allow redundancy on 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 VRF and SGT information, from one domain to another. You can configure up to 2 border devices to allow redundancy on your network.
- Virtual Contexts — Provide virtualization at the device level, using virtual routing and forwarding (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 endpoints in the fabric domain into IP pools, and identify them with a VLAN ID and an IP subnet.

Supported Platforms in Campus Fabric

Table 41-1

Platform Support	Fabric Edge	Fabric Control-Plane	Fabric Border
Cisco Catalyst 4500-E Series Switches	Yes	No	No
Cisco Catalyst 6800 Series Switches	No	Yes	Yes
Cisco Catalyst 3850 Series Switches	Yes	Yes	Yes
Cisco Nexus 7700 Series Switches	No	Yes	Yes

Campus Fabric Configuration Guidelines

Consider the following guidelines and limitations when configuring campus fabric elements:

- Configure no more than 3 control-plane devices in each fabric domain.
- Configure no more than 2 border devices in each fabric domain.
- Each fabric edge device supports up to 2000 endpoints.
- Each control-plane device supports up to 5000 fabric edge device registrations.
- Configure no more than 32 virtual contexts in each fabric domain.
- Ensure that you use 10-Gigabit-Ethernet supervisor uplinks when configuring underlay connectivity.

Limitations and Restrictions

- You can configure Cisco Catalyst 4500-E series switches as edge devices only.
- Campus Fabric is not supported in Virtual Switching System (VSS) mode and in VSS wireless mode.
- Virtual Extensible LAN (VXLAN) encapsulation is supported on the Supervisor uplink modules only. Ensure that you use supervisor uplink modules for underlay connections between fabric elements.
- Campus Fabric is supported only on Cisco Catalyst 4500-E series switches, on Supervisor Engine 8-E.
- IPv6 hosts are not supported in the fabric domain.
- Policy-based routing (PBR) and Web Cache Communication Protocol (WCCP) are not supported within the fabric domain.
- Cisco TrustSec SGT Exchange Protocol (SXP) cannot be used to propagate SGTs across devices within the fabric domain.
- On the edge device, Cisco TrustSec links are not supported only on uplink interfaces connected to the underlay.
- Layer 3 source group tags cannot be applied to uplink interfaces connected to the underlay.

- Multicast in Campus Fabric is supported with PIM Sparse mode and PIM SSM. Dense mode is not supported.
- Multicast Rendezvous-point (RP) redundancy is not supported in the fabric domain.
- Auto-RP is not supported in the fabric domain.

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.
- Policy Management — Setting up virtual contexts or VRFs, endpoint groups and policies.
- Endpoint On-boarding — Setting up authentication and IP pools.
- Monitoring and Troubleshooting — Verifying reachability to all fabric devices.

Configuring Fabric Edge Devices

You can configure Cisco Catalyst 4500-E series switches as edge devices only.

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.
- Configure control-plane devices and border devices in your fabric domain. Cisco Catalyst 4500-E series switches cannot be configured as control-plane or border devices. For more information on configuring control-plane and border devices, see the How to Configure Fabric Overlay section in *Software Configuration Guide, Cisco IOS XE Denali 16.3.x (Catalyst 3850 Switches)*

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# fabric auto`	Enables automatic fabric provisioning and enters automatic fabric configuration mode.
Step 3	`Switch(config-fabric-auto)# domain {default | name fabric domain name}`	Configures the default fabric domain and enters domain configuration mode. The **name** keyword allows you to add a new fabric domain. The **no** version of this command deletes the fabric domain. You can configure either the default domain, or create a new fabric domain and not both.
Step 4	`Switch(config-fabric-auto-domain)# control-plane ipv4 address auth_key key`	Specifies the control-plane device IP address and the authentication key, to allow the fabric edge device to communicate with the control-plane device. The **no control-plane** *ipv4 address* **auth_key** *key* command deletes the control-plane device from the fabric domain. You can specify up to 3 control-plane IP addresses for the edge device.

	Command	Purpose
Step 5	`Switch(config-fabric-auto-domain)# border ipv4 address`	Specifies the IP address of the border device, to allow the edge device to communicate with the fabric border device. You can specify up to 2 border IP addresses for the edge device.
Step 6	`Switch(config-fabric-auto-domain)# context name eg-context ID ID`	Creates a new context in the fabric domain and assigns an ID to it. 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. This step is mandatory if you want to associate a context to a host-pool.
Step 7	`Switch(config-fabric-auto-domain)# host-pool name name`	Creates an IP pool to group endpoints in the fabric domain, and enters host-pool configuration mode.
Step 8	`Switch(config-fabric-auto-domain-host-pool)# host-vlan ID`	Configures a VLAN ID to associate with the host-pool.
Step 9	`Switch(config-fabric-auto-domain-host-pool)# context name name`	(Optional) Associates the context or VRF you created with the host-pool.
Step 10	`Switch(config-fabric-auto-domain-host-pool)# gateway IP address/mask`	Configures the routing gateway IP address and the subnet mask for the host-pool. This address and subnet mask are used to map the endpoint to the uplink interface connecting to the underlay.
Step 11	`Switch(config-fabric-auto-domain-host-pool)# use-dhcp IP address`	Configures a DHCP server address for the host-pool. You can configure multiple DHCP addresses for your host-pool. To delete a DHCP server address, use the **no use-dhcp** *IP address* command.
Step 12	`Switch(config-fabric-auto-domain-host-pool)# end`	Returns to Privileged EXEC mode.
Step 13	`Switch# show fabric domain`	Displays your fabric domain configuration.

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. When you configure a Cisco Catalyst 4500-E series switch as an edge device, the **ipv4 sgt** command is auto-generated. 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 Cisco TrustSec Switch Configuration Guide.

Auto-Configured Commands on Fabric Edge Devices

As a part of Fabric Overlay provisioning, some LISP-based configuration, SGT (security group tag) configuration and endpoint to uplink interface mapping configuration is auto-generated, and is displayed in your running configuration.

For example, consider this configuration scenario for an edge device (loopback address 2.1.1.1/32):

```
device(config)#fabric auto
device(config-fabric-auto)#domain default
device(config-fabric-auto-domain)#control-plane 192.168.1.4 auth-key example-key1
device(config-fabric-auto-domain)#control-plane 192.168.1.5 auth-key example-key2
device(config-fabric-auto-domain)#border 192.168.1.6
```

```
device(config-fabric-auto-domain)#context name eg-context ID 10
device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN
device(config-fabric-auto-domain-host-pool)#vlan 10
device(config-fabric-auto-domain-host-pool)#context eg-context
device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24
device(config-fabric-auto-domain-host-pool)#use-dhcp 209.165.201.6
```

This is sample output for the fabric edge configuration:

```
device#show running-config
!
ip vrf eg-context
description Auto-provisioned vrf for eg-context
!
ip dhcp relay information option vpn
ip dhcp relay information option
!
ip dhcp snooping vlan 10
ip dhcp snooping
!
!
fabric auto
!
domain default
control-plane 192.168.1.4 auth-key example-key1
control-plane 192.168.1.5 auth-key example-key2
border 192.168.1.6
context name eg-context id 10
!
host-pool name VOICE_DOMAIN
context eg-context
vlan 10
gateway 192.168.1.254/24
use-dhcp 209.65.201.6
exit
exit
exit
!
vlan 10
name VOICE_DOMAIN
!
interface Vlan10
ip vrf forwarding eg-context
ip dhcp relay source-interface Loopback0
ip address 192.168.1.254 255.255.255.0
ip helper-address global 209.65.201.6
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility eg-context.EID.VOICE_DOMAIN
!
router lisp
encapsulation vxlan
locator-set default.RLOC
IPv4-interface Loopback0 priority 10 weight 10
exit
!
eid-table default instance-id 0
exit
!
eid-table vrf eg-context instance-id 10
dynamic-eid eg-context.EID.VOICE_DOMAIN
database-mapping 192.168.1.0/24 locator-set default.RLOC
```

```
exit
!
exit
!
loc-reach-algorithm lsb-reports ignore
disable-ttl-propagate
ipv4 sgt
ipv4 use-petr 192.168.1.6 priority 10 weight 10
ipv4 itr map-resolver 192.168.1.4
ipv4 itr map-resolver 192.168.1.5
ipv4 itr
ipv4 etr map-server 192.168.1.4 key example-key1
ipv4 etr map-server 192.168.1.5 key example-key2
ipv4 etr
exit
```

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 at 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 in Campus Fabric.

Configuring Multicast PIM Sparse Mode in Campus Fabric

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip multicast-routing`	Enables IP multicast routing.
Step 3	`Switch(config)# ip pim rp-address` *rp address*	Statically configures the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups.
Step 4	`Switch(config)# interface LISP` *interface number*	Specifies the LISP interface and the subinterface on which to enable Protocol Independent Multicast (PIM) sparse mode.
Step 5	`Switch(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on the interface for sparse-mode operation.
Step 6	`Switch(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 7	`Switch(config)# interface` *interface type interface number*	Configures the interface facing the endpoint, and enters interface configuration mode.
Step 8	`Switch(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on interface for sparse-mode operation.
Step 9	`Switch(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

	Command	Purpose
Step 10	`Switch# show ip mroute multicast-ip-address`	Verifies the multicast routes on the device.
Step 11	`Switch# ping multicast-ip-address`	Verifies basic multicast connectivity by pinging the multicast address.
Step 12	`Switch# show ip mfib`	Displays the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB)

Configuring Multicast PIM SSM in Campus Fabric

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip multicast-routing`	Enables IP multicast routing.
Step 3	`Switch(config)# ip pim ssm {default | range {access-list-name | access-list-name}`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses.
Step 4	`Switch(config)# interface LISP interface number`	Specifies the LISP interface and the subinterface on which to enable Protocol Independent Multicast (PIM) sparse mode and enters interface configuration mode.
Step 5	`Switch(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on the interface for sparse-mode operation.
Step 6	`Switch(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 7	`Switch(config)# interface interface type interface number`	Configures the interface facing the endpoint, and enters interface configuration mode.
Step 8	`Switch(config-if)# ip pim sparse-mode`	Enables Protocol Independent Multicast (PIM) on interface for sparse-mode operation.
Step 9	`Switch(config-if)# ip igmp version 3`	Configures IGMP version 3 on the interface.
Step 10	`Switch(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 11	`Switch# show ip mroute multicast-ip-address`	Verifies the multicast routes on the device.
Step 12	`Switch# ping multicast-ip-address`	Verifies basic multicast connectivity by pinging the multicast address.
Step 13	`Switch# show ip mfib`	Displays the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB)

Dataplane Security

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.

Configuring Dataplane Security on Fabric Edge Devices

You can configure Cisco Catalyst 4500-E series switches as edge devices only.

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.
- Configure control-plane devices and border devices in your fabric domain. Cisco Catalyst 4500-E series switches cannot be configured as control-plane or border devices. For more information on configuring dataplane security control-plane and border devices, see the How to Configure Fabric Overlay section in *Software Configuration Guide, Cisco IOS XE Denali 16.3.x (Catalyst 3850 Switches).*

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	`Switch(config-router-lisp)# decapsulation filter rloc source member`	Enables source RLOC address validation of encapsulated packets in the fabric domain.
Step 4	`Switch(config-router-lisp)# exit`	Exits LISP configuration mode and returns to global configuration mode.
Step 5	`Switch(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 6	`Switch(config)# show lisp [session [established] | vrf` *`[vrf-name [session [peer-address]]]`*	Displays reliable transport session information. If there is more than one transport session, the corresponding information is displayed.
Step 7	`Switch(config)# show lisp decapsulation filter` *`[IPv4-rloc-address I IPv6-rloc-address]`* `[eid-table` *`eid-table-vrf`* `|instance-id` *`iid]`*	Displays RLOC address configuration details (whether manually configured or discovered) on the edge device.

To configure dataplane security in static mode:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# router lisp`	Enters LISP configuration mode.
Step 3	`Switch(config-router-lisp)# locator-set locator-set-name`	Specifies a locator set for the border device and enters LISP locator set configuration mode.
Step 4	`Switch(config-router-lisp-locator-set)# ipv4 address`	Configures the LISP locator set address.
Step 5	`Switch(config-router-lisp-locator-set)# exit`	Exits LISP locator set configuration mode.
Step 6	`Switch(config-router-lisp)# decapsulation filter rloc source locator-set locator-set-name`	Enables source RLOC address validation of encapsulated packets in the fabric domain.

Campus Fabric Configuration Examples

This is sample output for the **show running-configuration** command for an edge configuration:

```
fabric auto
!
domain default
  control-plane 198.51.100.2 auth-key example-key1
  border 192.168.1.6
  context name eg-context id 10
   !
   host-pool name VOICE_VLAN
    context eg-context
    vlan 10
    gateway 192.168.1.254/24
    use-dhcp 172.10.1.1
    exit
  exit

router lisp
locator-set default.RLOC
  IPv4-interface Loopback0 priority 10 weight 10
  exit
!
encapsulation vxlan
eid-table default instance-id 0
  exit
!
eid-table vrf eg-context instance-id 10
  dynamic-eid eg-context.EID.VOICE_VLAN
   database-mapping 192.168.1.0/24 locator-set default.RLOC
   exit
  !
  exit
!
loc-reach-algorithm lsb-reports ignore
disable-ttl-propagate
ipv4 sgt
ipv4 use-petr 192.168.1.6 priority 10 weight 10
ipv4 itr map-resolver 192.168.1.4
ipv4 itr map-resolver 192.168.1.5
```

```
ipv4 itr
ipv4 etr map-server 192.168.1.4 key example-key1
ipv4 etr map-server 192.168.1.5 key example-key2
ipv4 etr
exit
```

This is sample output for the **show running-configuration** command for the following control-plane configuration:

```
device(config)#fabric auto
device(config-fabric-auto)#domain default
device(config-fabric-auto-domain)#control-plane self auth-key example-key1
device(config-fabric-auto-domain)#host-prefix 192.168.1.0/24 context name eg-context id 10
device(config-fabric-auto-domain)#exit


!
fabric auto
  domain default
    control-plane auth-key example-key1
  exit
!
ip vrf eg-context
!
vlan name VOICE_VLAN id 10
interface Vlan 10
    ip address 192.168.1.254 255.255.255.0
   ip helper-address global 172.10.1.1
    no ip redirects
    ip local-proxy-arp
    ip route-cache same-interface
    no lisp mobility liveness test
    lisp mobility default.EID.VOICE_VLAN
  router lisp
    eid-table default
       dynamic-default.EID.VOICE_VLAN
           database-mapping 192.168.1.0/24 locator-set FD_DEFAULT.RLOC

 router lisp
   site FD_Default
     authentication-key example-key1
     exit
   ipv4 map-server
   ipv4 map-resolver
  exit
```

This is sample output for the **show running-configuration** command for the following border configuration:

```
device(config)#fabric auto
device(config-fabric-auto)#domain default
device(config-fabric-auto-domain)#border self
device(config-fabric-auto-domain)#control-plane 198.51.100.2 auth-key example-key1
device(config-fabric-auto-domain)#context name eg-context id 10
device(config-fabric-auto-domain)#host-prefix 192.168.1.0/24 context name eg-context id 10
device(config-fabric-auto-domain)#exit

device#show running-config
!fabric auto
 !
 domain default
  control-plane 198.51.100.2 auth-key example-key1
  border self
```

```
  context name eg-context id 10
  !
  host-prefix 192.168.1.0/24 context name eg-context
   !
   host-pool name Voice
    context eg-context
    use-dhcp 172.10.1.1
     exit
   !
   host-pool name doc
     exit
  exit
 exit

router lisp
 encapsulation vxlan
 loc-reach-algorithm lsb-reports ignore
 disable-ttl-propagate
 ipv4 sgt
 ipv4 proxy-etr
 ipv4 proxy-itr 1.1.1.1
 ipv4 itr map-resolver 198.51.100.2
 ipv4 etr map-server 198.51.100.2 key example-key1
 exit
```