LISP VXLAN Fabric Overview

LISP VXLAN Fabric is a wired and wireless connectivity solution offering scalable policy-based segmentation at the network edge.

Note This document describes the configurations required to deploy a LISP VXLAN fabric in a campus network. If you are not familiar with the LISP routing architecture and VXLAN networking, we recommend that you go over the fundamentals of LISP and VXLAN before you proceed with the configurations described below.

What is LISP VXLAN Fabric

A network fabric is made of network devices such as wireless access points, switches, and routers that are interconnected, to transport data to its destination. These physical devices form the underlay network that forwards the traffic. A virtual network is built over the underlay network using tunneling technologies such as VXLAN, and is called an overlay. Endpoints or users are logically connected to the overlay network, which transports the user data.

While there are several routing protocols that enable the transport of data in a fabric, this particular fabric uses a combination of Locator/ID Separation Protocol (LISP) and VXLAN.

The Locator/ID Separation Protocol (LISP) is an overlay routing technology that provides improved routing scalability and dynamic host mobility. LISP works with two separate IP address spaces: one to indicate routing locators (RLOCs) for routing traffic to the external network and a second address called endpoint identifier (EID), which is used to identify the endpoints.

VXLAN, a Layer 2 tunneling mechanism, forms the data plane in the overlay network and uses a MAC-in-IP encapsulation method to carry the data packets through the tunnel.

A LISP VXLAN fabric solution uses virtual networks (overlay networks) that run on a physical network (underlay network). The overlay network creates a logical topology to virtually connect the physical devices that are part of the underlay network. In the underlay network, IP connectivity is established among the physical devices through a routing protocol.

Three fundamental components work together to provision a LISP VXLAN fabric. These enable flexible attachment of devices, data transmission and enhanced security through segmentation and group-based policies:

- Control Plane: Uses LISP for mapping endpoint identity (IP addresses or MAC addresses) to their location within the fabric.
- Data Plane: Uses Virtual Extensible LAN (VXLAN) encapsulation method to transmit data packets.
- Policy Plane: (Optional) Uses Cisco Security Group Tags (SGTs) and Group-Based Policy for microsegmentation.

Benefits of Provisioning a LISP VXLAN Fabric

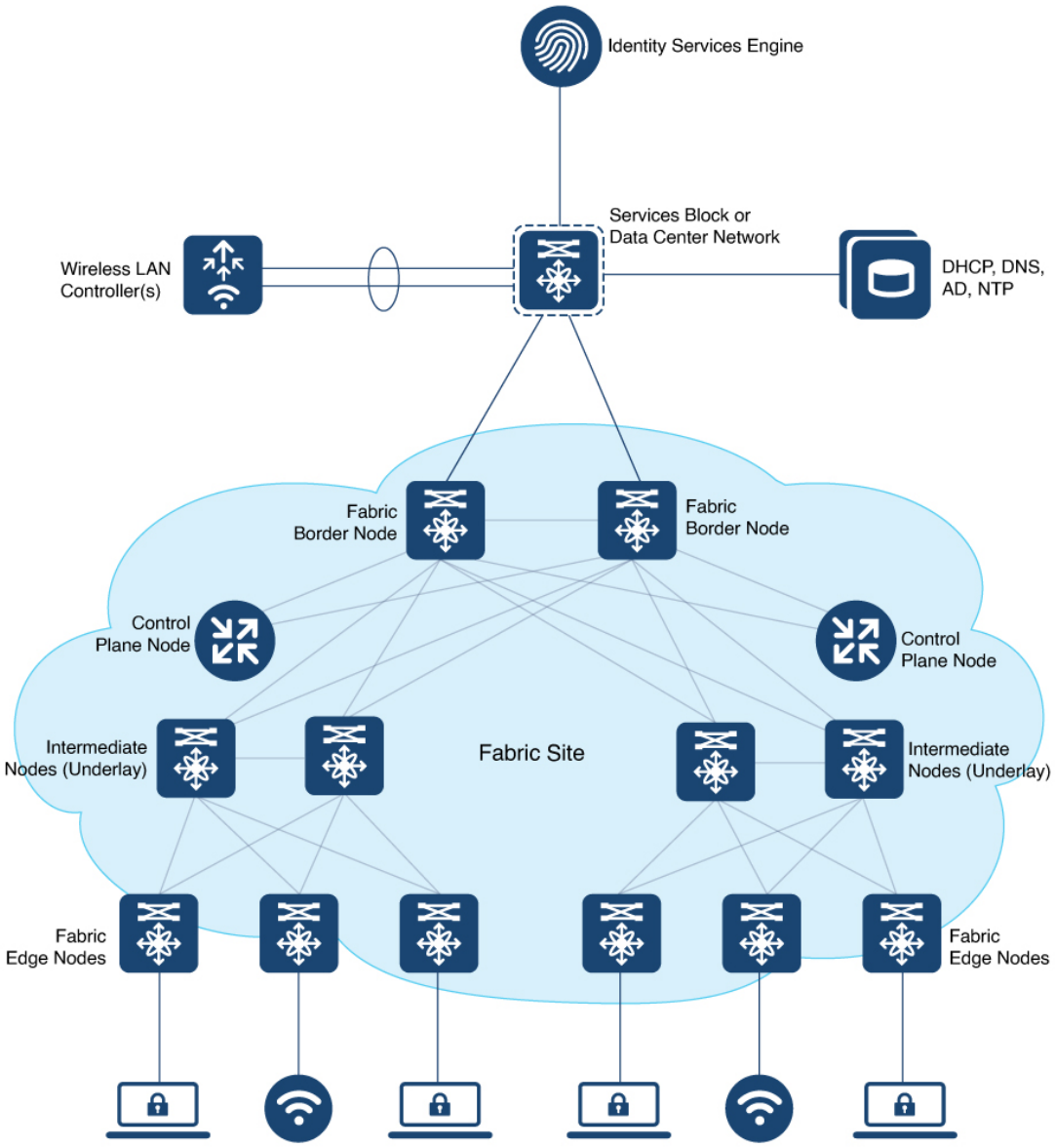
- Use of LISP helps decouple the host address and its location, simplifying the routing operations, and improving scalability.
- Provides end-to-end segmentation using LISP Virtualization technology wherein only the fabric edge and border nodes must be LISP-aware. The rest of the components are just IP forwarders.
- Eliminates Spanning Tree Protocol (STP), improves link utilization, and brings in faster convergence and equal cost multipath (ECMP) load balancing.
- Fabric header (VXLAN) supports Security 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.

LISP VXLAN Fabric Constructs

The LISP VXLAN fabric comprises wired and wireless devices that make up the underlay and the overlay network. The wired and wireless devices perform different roles, providing end-to-end segmentation enabling efficient traffic movement within the fabric.

Use of Identity Services Engine (ISE) for access control and policy enforcement is optional.

Figure 1: Components of a LISP VXLAN Fabric



- **Fabric Edge Node**: Identifies and authenticates end points and registers 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 network.
- **Fabric Border Node**: Serves as the gateway between the fabric and networks external to the fabric. The border node device is physically connected to a transit or to a next-hop device that is connected to the external network. The border node helps translate the reachability and policy information, such as virtual routing and forwarding (VRF) and SGT.

  A fabric border node can be configured as an internal border node, or an external border node, or both internal and external border node.

An internal border node is used for known and registered routes for example, when the traffic needs to go to a datacenter, the LAN or the Shared Services. This internal-only border node advertises the endpoints to the external network and imports external routes into the fabric.

An external border is similar to a default gateway. It is used as a gateway for the traffic from the fabric to unknown destinations or unregistered routes for example, the internet. It advertises the fabric endpoints to the external network but does not import any external routes into the fabric domain.

A border can be both internal and external. An internal and external border is used to access registered and unregistered routes. It advertises the endpoints to the external network and imports external routes into the fabric. It also acts a default gateway for traffic to destinations that are unknown to the control plane database.

- **Fabric Control Plane Node**: Based on the LISP Map-Server and Map-Resolver (MSMR) functionality, a control plane node provides overlay reachability information and end points-to-routing locator (EID-to-RLOC) mapping. A control plane node is a Map Server that receive registrations from fabric edge devices with local end points. A control plane node is also a Map Resolver (MR) that resolves requests from edge devices to locate the remote end points.
- **Intermediate Nodes (Underlay Network)**: Part of the Layer 3 network that physically connects the devices operating in a certain fabric role, such as the interconnection between a border node and an edge node. For example, if a three-tier campus deployment provisions the core switches as the border nodes and the access switches as the edge nodes, the distribution switches are the intermediate nodes. Intermediate nodes simply route and transport IP traffic between the devices operating in fabric roles. The underlay network provides IP reachability, physical connectivity, and supports the additional MTU requirement to accommodate the larger-sized IP packets encapsulated with fabric VXLAN information.
- **Fabric Site**: A network that is composed of a unique set of devices operating in a fabric role (control plane node, border node, edge node) along with the intermediate nodes that are used to connect those devices.
- **Fabric In a Box**: Combines the roles of a border node, a control plane node, and an edge node on the same device. This may be a single switch, a switch with hardware stacking, or a StackWise Virtual deployment. In certain implementations, the same switch can also serve as a Wireless LAN Controller for Fabric-enabled Wireless designs.
- **Wireless LAN Controller**: Provides Access Point image and configuration management, client session management, and mobility services. Additionally, it registers the MAC address of wireless clients in the host tracking database at the time of client join events, as well as updates the location at the time of client roam events.
- **Virtual Network**: Network created in the policy application and provisioned to the fabric nodes as a VRF instance.
- **VXLAN Overlay**: Virtual network that is built over a Layer 3 network by forming a static or dynamic tunnel that runs on top of the physical network infrastructure.
- **Security Group Tag (SGT):** An attribute that is applied to the endpoint traffic to provide logical segmentation based on group membership. When an endpoint connects to a network, it is authenticated and based on the results of the authentication, the network assigns it a specific security group, with the help of SGT.

Fabric Roles Supported by Cisco Catalyst 9000 Series Switches

Platform Family	Fabric Role Support			
	Edge Node	Control Plane Node	Border Node	Embedded 9800 Wireless Controller
Cisco Catalyst 9300 Series	✓	✓	✓	✓
Cisco Catalyst 9400 Series	✓	✓	✓	✓
Cisco Catalyst 9500 Series	✓	✓	✓	✓
Cisco Catalyst 9600 Series	–	✓	✓	–

Deployment Options for a LISP VXLAN Fabric

LISP VXLAN fabric supports the following deployment models:

- A fabric site with multiple control plane nodes and border nodes. The control plane and border nodes are dedicated devices, usually deployed as redundant pairs.
- A fabric site with colocated border and control plane nodes, usually deployed in pairs for redundancy.
- A fabric site with a single device that performs all the fabric roles (control plane, border node, fabric edge node, and a wireless controller). This type of deployment is called a Fabric in a Box and is suitable for small deployments such as a branch office.

Prerequisites for Configuring a LISP VXLAN Fabric

- All fabric nodes must have a Loopback interface with an IPv4 address.

  We recommend that the /32 routes of these Loopbacks be propagated by the underlay Interior Gateway Protocol (IGP) throughout the fabric site (without summarization). This is important to quickly detect the fabric edges that are going down.
- All switches in the network including fabric edge, border, control plane, and intermediate nodes should support jumbo MTU. VXLAN header adds 50 bytes of encapsulation to a data packet that is sourced from an endpoint. We recommend an MTU of 9100 to support packet forwarding without fragmentation.
- Ensure that the underlay has routed access network configured.
- Ensure that there is IP reachability between all fabric nodes.

- There should be 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 irrespective of fabric-enabled wireless or centralized wireless.
- Ensure that all the Cisco Catalyst 9000 Series switches in the fabric operate Cisco IOS XE 17.9.3 or later releases.

  Cisco Identity Services Engine (ISE) operates ISE 3.1 Patch 1 or later releases.

Restrictions for Configuring LISP VXLAN Fabric

- LISP VXLAN fabric solution is supported only on the Cisco Catalyst 9000 Series switches.
- LISP VXLAN fabric underlay network supports only IPv4 addressing. LISP VXLAN overlay network supports both IPv4 and IPv6 addressing. Only the Border Gateway Protocol (BGP) is supported for handoff to external networks.
- Endpoints cannot be assigned to a default instance. (A default instance is an overlay virtual network which connects the infrastructure elements like access points, and Layer 2 switches to the fabric access layer.) Ensure that the endpoint subnets are all assigned to overlay VRFs.
- LISP VXLAN fabric does not support In-Service Software Upgrade (ISSU).
- LISP VXLAN fabric supports only those configurations that are described in this document.

How to Configure LISP VXLAN Fabric

Before you start configuring a LISP VXLAN fabric, ensure that the underlay physical network with the wired devices is configured with routed access.

Configuring a LISP VXLAN Fabric involves the following stages:

1. Configuring a control plane node to map the endpoint IDs to their routing locators. A control plane is LISP-based and serves as the Map Server and Map Resolver.
2. Configuring a border node to provide an exchange point for the traffic. A border node is LISP-based and performs the function of the Proxy Tunnel Router.

Note We recommend that you configure both the border and control plane nodes on a single fabric device.

3. Configuring edge nodes that are LISP-based and act as ingress and egress tunnel routers for endpoint traffic.
4. Configuring support for wireless infrastructure and endpoints.
5. Configuring Multicast in the overlay.
6. Configuring fabric security to provide secure fabric access to the wired and wireless endpoints that connect to the fabric. This involves configuring IEEE 802.1x and Group-based policy on the fabric edge.

Troubleshooting LISP VXLAN Fabric

See Troubleshooting LISP VXLAN Fabric on Cisco Catalyst 9000 Series Switches document to learn how to troubleshoot issues in a LISP VXLAN fabric.