Lab 6: Virtual Networks with VRF and LISP Instance-ID

Adding Virtual Network Segmentation to the Fabric

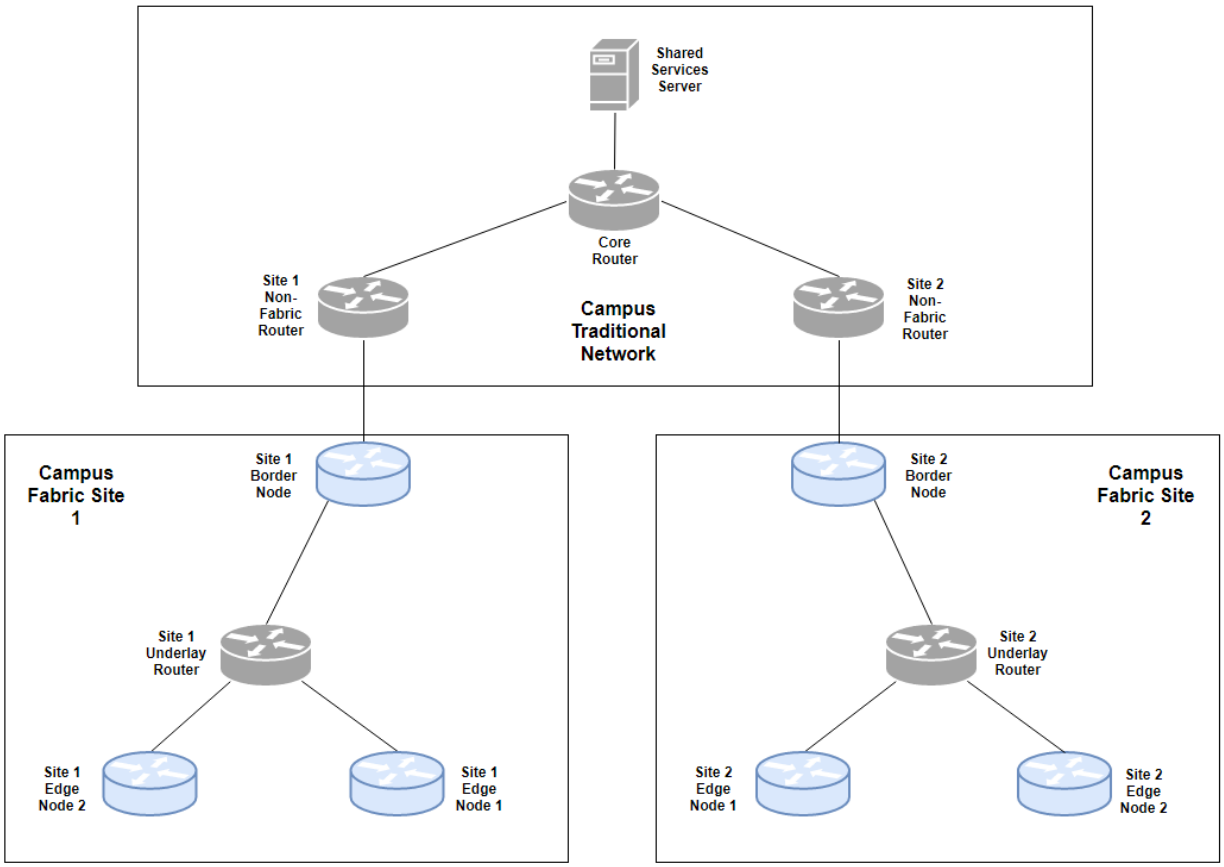
Please refer to folder containing Lab 6 Configurations to see what configuration should be preloaded on the network devices prior to starting this exercise.

In this lab we will add another VRF segment to our fabric and move hosts into it. This is a common deployment where macrosegmentation at the network layer is required. In traditional networks doing this becomes complicated because VRFs are configured per-router and often extending segmentation requires a lot of VRF-lite configuration or a technology like MPLS. With LISP, we use the underlay global routing table to route packets, but the segmentation happens with LISP instance-id. Because LISP/VXLAN encapsulates the original packet (which is not VRF-aware) but uses a VXLAN VNI/LISP Instance-id, segmentation is preserved without having to do complicated VRF-lite extension through the underlay network.

By the end of this lab, there will be two LISP instances running. The Infrastructure subnet we have been using will remain in LISP instance-id 0, or the global routing table, and the Users subnet will be in LISP instance-id 1010 tied to VRF 1010_USER1.

Configure VRF and LISP Instance-ID for Network Segmentation

Goal: Provide macrosegmentation between network segments without having to extend VRF-lite throughout the campus.



Task 1

On the Site 1 Edge nodes:

- Create a VRF called 1010_USER1 using a method which supports different address-families.
- Use a route distinguisher of 1010:1010 for this VRF and use route-targets that match this for import and export under the IPv4 address-family.
- The interface for the Users subnet (10.10.1.0/24) should be placed into this VRF.
- Add LISP instance-id 1010 to the LISP configuration.
- Ensure that the VRF 1010_USER1 is used as the routing table associated for this instance.
- A local database mapping should be added for the EID covering the Users subnet.
- A LISP Map Request should be sent for all prefixes.

- Add the LISP host mobility configuration to trigger dynamic host discovery to the interface used as the gateway for the Users subnet.

Task 2

On the Site 1 Border-CP node:

- Create a VRF called 1010_USER1 using a method which supports different address-families.
- Use a route distinguisher of 1010:1010 for this VRF and use route-targets that match this for import and export under the IPv4 address-family.
- Add LISP instance-id 1010 to the LISP configuration.
- Ensure that the VRF 1010_USER1 is used as the routing table associated for this instance.
- Ensure the LISP site SITE1 will register the host EIDs for the Users subnet in the correct LISP instance.

Task 3

Verify the new LISP instance and VRF are active.

- On the Site 1 Edge nodes, how can you verify that the User gateway interfaces are in the correct VRF? How will you make sure the VRF routing table shows the network?
- In this lab the SITE1-USER1 device was connected to the Users subnet so there would be a host to register. From SITE1-USER1 ping the gateway IP (10.10.1.1).
- How can we check the LISP mapping database on the SITE1-EDGE1 node to make certain that the host was discovered?
- How can we check this on the Border-CP node to make certain the host prefix was registered?

Bonus Tasks

If you would like to learn more about how LISP operates, try these bonus tasks. They are not required to continue, and indeed some of these tasks will break the fabric with a goal of doing so to understand LISP/VXLAN better. If you wish to do the bonus tasks, save the working configurations, and then reload after completing the bonus tasks.

- Ping the gateway IP of 10.10.1.1 from SITE1-USER1 to ensue host discovery takes place. Do the same for SITE1-USER2, pinging 10.99.1.1. These two users are connected to different Edge nodes and are in different LISP instances, but the Border-CP node has entries for both hosts. Will a ping between them be successful?
- The non-fabric server at 100.64.100.100 should still be reachable by SITE1-USER2 on the Infrastructure subnet. Can it be pinged by that user? Can the SITE1-USER1 host ping that server? Why or why not?