The bridge to possible

White Paper
Cisco Public

Cisco Integrated System for Microsoft Azure Stack Hub border connectivity to Cisco Application Centric Infrastructure

Contents

Executive summary

In today's world, enterprises are undergoing increasing pressure to innovate rapidly, to keep up with competition and to increase IT agility to meet customer demands. To achieve these goals, businesses are choosing different infrastructure environments for deploying different types of applications.

As some workloads shift to the cloud, enterprises are also seeking to transform their internal data centers and services into offerings that provide cloud-like scale, flexibility, resiliency, and operational methods, with similar positive economic outcomes.

However, in a hybrid cloud environment it is becoming more and more challenging to maintain a homogeneous enterprise operational model, comply with corporate security policies, and gain visibility across hybrid environments.

The Cisco Integrated System for Microsoft Azure Stack Hub enables your organization to access development tools, data repositories, and related Azure services to reinvent your applications and gain new information from your secured data. Azure Stack Hub provides the same APIs and user interface as the Azure public cloud. The Integrated System enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations on data location and accessibility. Cisco's infrastructure leverages the key automation benefits of the Cisco Unified Computing System (Cisco UCS) with leading Cisco Nexus networking and data security technology, while ensuring an industry-leading performing design to meet your future hybrid-cloud growth requirements.

Cisco Integrated System for Microsoft Azure Stack Hub with Cisco Application Centric infrastructure (ACI) enabled datacenters can accelerate your journey to true Hybrid Cloud and help you reap many benefits such as enhanced business agility, reduced TCO, automated IT tasks, and accelerated data center application deployments.

Cisco ACI is an industry-leading SDN (Software Defined Networking) solution that provides policy-driven automation through an integrated underlay and overlay, is hypervisor agnostic, and extends policy automation to any workload – including virtual machines, physical bare-metal servers, and containers.

While customers benefit from an ACI policy driven infrastructure in the on-premises environment, Cisco Cloud Application Centric Infrastructure (Cloud ACI) allows them to automate the management of end-to-end connectivity, as well as the agentless enforcement of consistent security policies, for workloads across on-premises and in public clouds through a single pane of glass.

Document Purpose

During the installation of Azure Stack Hub, it is the customer's responsibility to ensure a direct Layer 3 connection from data center border switches to the Azure Stack Hub Top-of-Rack (TOR) switches; and ensuring accessibility to the data center, among other required tasks.

This document is intended to provide information, education and guidance for individuals or organizations who are interested in connecting Cisco Integrated System for Microsoft Azure Stack Hub to an existing Cisco ACI fabric in their data centers as an external routed domain. The document provides fundamental information and recommended configurations based upon internal testing of the solution. As such, the document does not cover the installation and configuration of Cisco ACI Fabric as well as details on setting up the Cisco Integrated System for Microsoft Azure Stack Hub.

Note: The Azure Stack Hub internal networks are not maganed using Cisco ACI in this solution. Azure Stack Hub system is connected to the Cisco ACI fabric as an external Layer 3 routed domain only, with ACI

fabric acting as a transit network to allow Azure Stack Hub networks to reach Internet and other internal network services in the datacenter.

Solution Overview

Azure Stack Hub is Microsoft's hybrid cloud solution for on-premises data centers. Azure Stack Hub provides an organization with three core benefits: Azure services on the premises, a consistent application development environment, and a predictable delivery experience.

The Azure Stack Hub solution requires a resilient and highly available physical infrastructure to support its operation and services. The data center network Integration is crucial for deployment, operation, and management of Azure Stack Hub systems.

This solution details Azure Stack Hub integration with Cisco ACI enabled data center networks.The Azure Stack Hub system Top-of-Rack Nexus 9336C-FX2 switches connect using a direct Layer 3 piont-to-pont connection to the data center ACI border leaf switches using Layer 3 Out (L3Out) connectivity. The L3Out in Cisco ACI is a set of configurations that define connectivity to outside of ACI via routing.

The design also includes another Layer 3 connectivity outside the ACI fabric to existing, non-ACI datacenter infrastructure within the Enterprise and providing access to non-ACI networks and Internet for cloud-based services. This Layer 3 access is enabled in ACI using a Shared Layer 3 Outside (Shared L3Out) connection. In this design, the Shared L3Out connection leverages OSPF routing protocol and the Azure Stack Hub L3Out configuration leverages BGP routing protocol, with optional support for static routing.

The ACI fabric supports transit routing, which enables border routers to perform bidirectional traffic redistribution between Azure Stack Hub and Shared L3Out routing domains. This allows the Azure Stack Hub networks to be able to access Internet via ACI fabric and the other necessary services with in the data center.

Note: The links between the ACI border leaf switches and the Layer 3 gateways can vary based on the customer environment. Also, the Nexus 7000 switches were used as gateways in the Shared L3Out which can be replaced with any existing and supported devices at the customer environment.

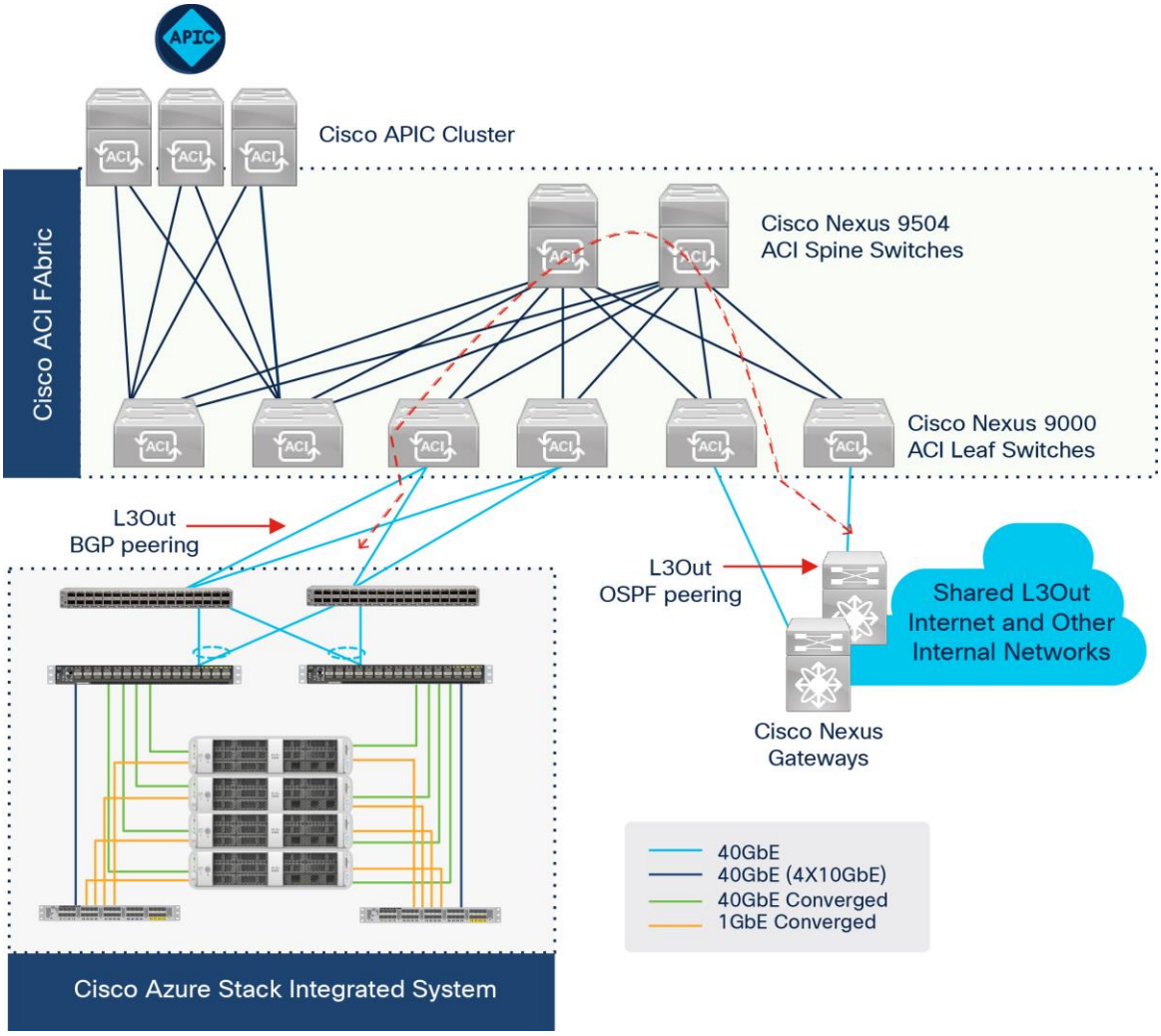


Figure 1.
Solution Overview

Technology Overview

This section introduces the technologies used in the solution described in this document.

Cisco Integrated System for Microsoft Azure Stack Hub

The Cisco Integrated System for Microsoft Azure Stack Hub enables your organization to access the development tools, data repositories, and related Azure services to reinvent your applications and gain new information from your secured data (Figure 2). Azure Stack Hub provides the same APIs and user interface as the Azure public cloud. This integrated system enables your team to save time building cloud-enabled applications, even when disconnected from Azure, and manage customer data while adhering to regulations about data location and accessibility.

This solution offers the following benefits:

- Design by Cisco: All major system components are designed, developed, and manufactured by Cisco, which simplifies system management, enables single-source support, and helps you avoid unforeseen product roadmap issues.

- Leading system performance: The latest Intel® Xeon® Scalable processors, up to 3072 GB of memory per server, NonVolatile Memory Express (NVMe) standard storage cache, and optional solid-state disk (SSD) drives are part of the package.
- Capability to maintain your data center standards for system racks and networking: Maintain your IT organization's data center standards for Cisco Nexus switching and system racks by installing all system components in your racks and using your networking team's existing expertise.
- Freedom to choose: Purchase Azure services from any vendor.
- Proven tools: Cisco UCS Manager and Cisco Intersight SaaS management platform that empowers you to deploy, maintain, and get support for your infrastructure from anywhere users are Internet-connected.

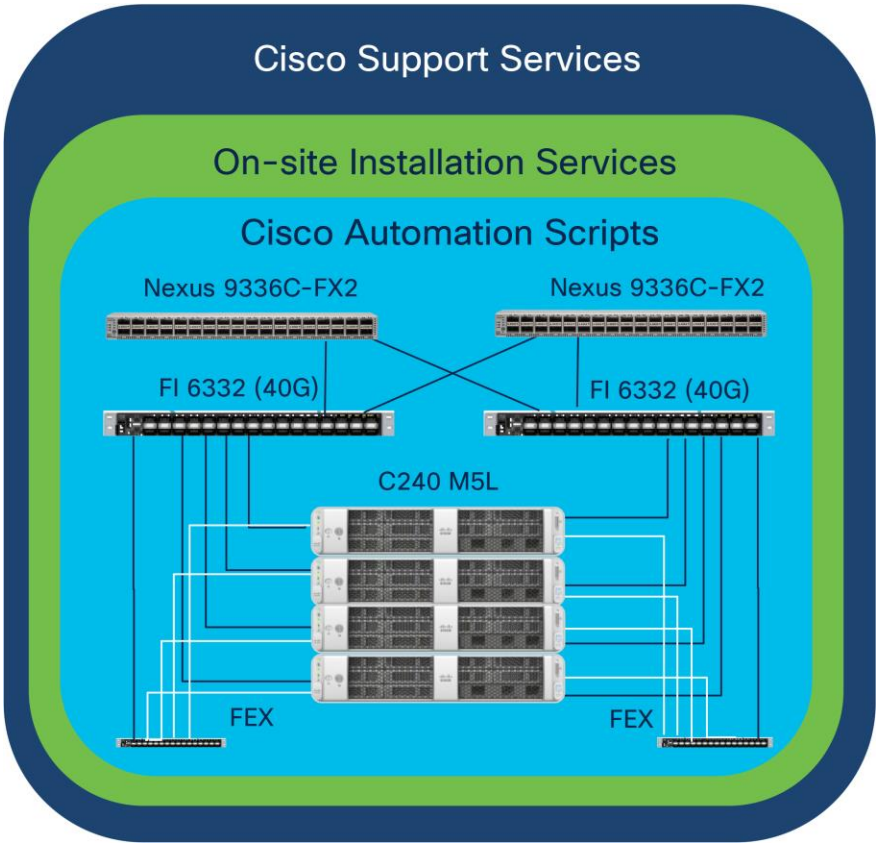


Figure 2.
Cisco Integrated System for Microsoft Azure Stack Hub (4-node solution)

Azure Stack Hub installation services managed by Cisco Advanced Services are included (typical installation takes only three days). Cisco can configure any node increment from four up to the limit supported by Azure Stack Hub. Cisco Solutions Support is also included. Solutions Support is the highest level of Cisco support and provides up to 24 x 7 x 4-hour onsite repair. In addition, your support calls are automatically routed to a team specially trained on Azure Stack Hub. This team can also move a support call to the Microsoft Case Exchange system to enable Microsoft support to engage as needed. This way, human error in reentering call details is avoided. The call flow works in reverse should you choose to contact Microsoft support initially. For additional information about the Cisco Integrated System for Azure Stack Hub, see https://www.cisco.com/go/microsoft-azure-stack.

Cisco Application Centric Infrastructure

Cisco ACI is an evolutionary leap from SDN's initial vision of operational efficiency through network agility and programmability. Cisco ACI has industry leading innovations in management automation, programmatic policies, and dynamic workload provisioning. The ACI fabric accomplishes this with a combination of hardware, policy-based control systems, and closely coupled software to provide advantages not possible in other architectures.

Cisco ACI takes a policy-based, systems approach to operationalizing the data center network. The policy is centered around the needs (reachability, access to services, security policies) of the applications. Cisco ACI delivers a resilient fabric to satisfy today's dynamic applications.

Cisco ACI Architecture

The Cisco ACI fabric is a leaf-and-spine architecture where every leaf connects to every spine using high-speed 40/100/400-Gbps Ethernet links, with no direct connections between spine nodes or leaf nodes. The ACI fabric is a routed fabric with a VXLAN overlay network, where every leaf is VXLAN Tunnel Endpoint (VTEP). Cisco ACI provides both Layer 2 (L2) and Layer 3 (L3) forwarding across this routed fabric infrastructure.

Cisco ACI Fabric Components

The following are the ACI Fabric components:

Cisco APIC: The Cisco Application Policy Infrastructure Controller (APIC) is the unifying point of automation and management for the Cisco ACI fabric. The Cisco APIC is a centralized, clustered controller that provides centralized access to all fabric information, optimizes the application lifecycle for scale and performance, and supports flexible application provisioning across physical and virtual resources. The Cisco APIC exposes northbound APIs through XML and JSON and provides both a command-line interface (CLI) and GUI which utilize the APIs to manage the fabric.

Leaf Switches: The ACI leaf provides physical connectivity for servers, storage devices and other access layer components as well as enforces ACI policies. Leaf switches also provide connectivity to existing enterprise or service provider infrastructure. The leaf switches provide options starting at 1G up through 100G Ethernet ports for connectivity.

In this design, Azure Stack Hub TOR Nexus 9336C-FX2 switches and Cisco Nexus 7000 based WAN/Enterprise routers are connected to leaf switches for L3Out routed connectivity, each of these devices are redundantly connected to a pair of leaf switches for high availability.

Spine Switches: In ACI, spine switches provide the mapping database function and connectivity between leaf switches. A spine switch can be the modular Cisco Nexus 9500 series equipped with ACI ready line cards or fixed form-factor switch such as the Cisco Nexus 9364C (used in this design). Spine switches provide high-density 40/100/400 Gigabit Ethernet connectivity between the leaf switches.

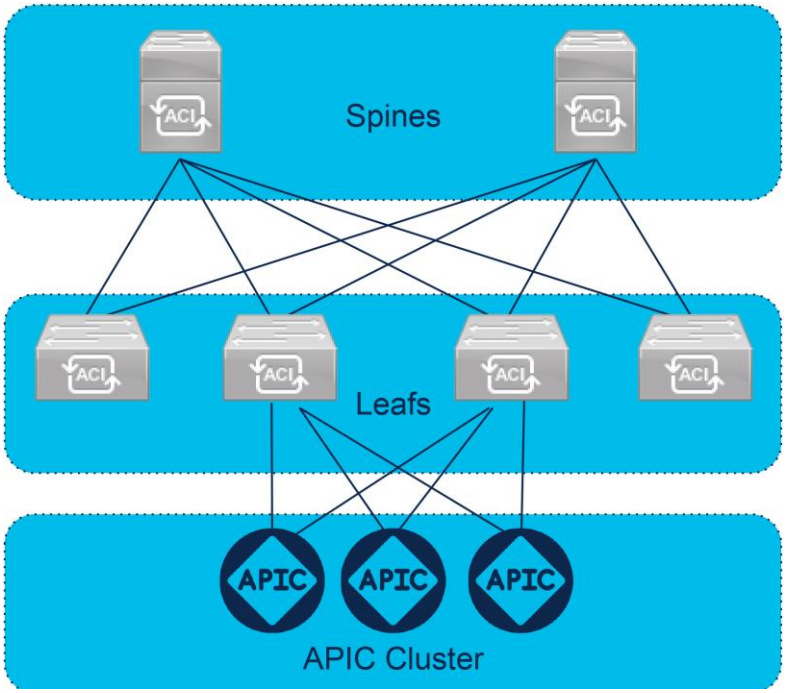


Figure 3.
Cisco ACI Fabric Components

For additional information about Cisco Application Centric Infrastructure, see https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html

Solution Design

Prior to implementation of the solution, it is important to understand the logical architecture of the Azure Stack Hub system and how it maps to the underlying physical architecture. In this section, detailed descriptions of the Cisco ACI, Cisco Azure Stack Hub, and ACI L3Out routed connectivity logical and physical architectures are provided.

Physical Architecture

The Cisco Integrated System for Microsoft Azure Stack Hub solution starts with rack-optimized Cisco UCS C240 M5 Rack Servers. Each server is connected to two Cisco 6332 third-generation fabric interconnects, which house the Cisco UCS Manager software; having two avoids the vulnerability of having a single point of failure in the architecture. These fabric interconnects in turn are connected to a pair of Cisco Nexus 9336C-FX2 Top-of-Rack (TOR) switches to enable connectivity to the data center's border switches. Each switch and fabric interconnect maintain a copy of the other's configuration to help enable easy replacement, should it be required. Each server is configured with NVMe cache storage and 40 Gigabit Ethernet dual port RoCEv2 capabled NIC. The Cisco Nexus 2348UPG fabric extender provides out-of-band management connectivity to the CIMC in each server.

To integrate Azure Stack Hub system to the ACI network it requires uplinks from the Nexus 9336C-FX2 TOR switches to the Cisco ACI border leafs, which are generally referred as Border swithes in Azure Stack Hub terms. The Cisco Nexus TORs are pre-configured by Azure Stack Hub deployment automation tool, with two 40G point to point connections between each TOR and Border switches using BGP routing and having support for static routing.

The following diagram presents the recommended high level physical architecture design:

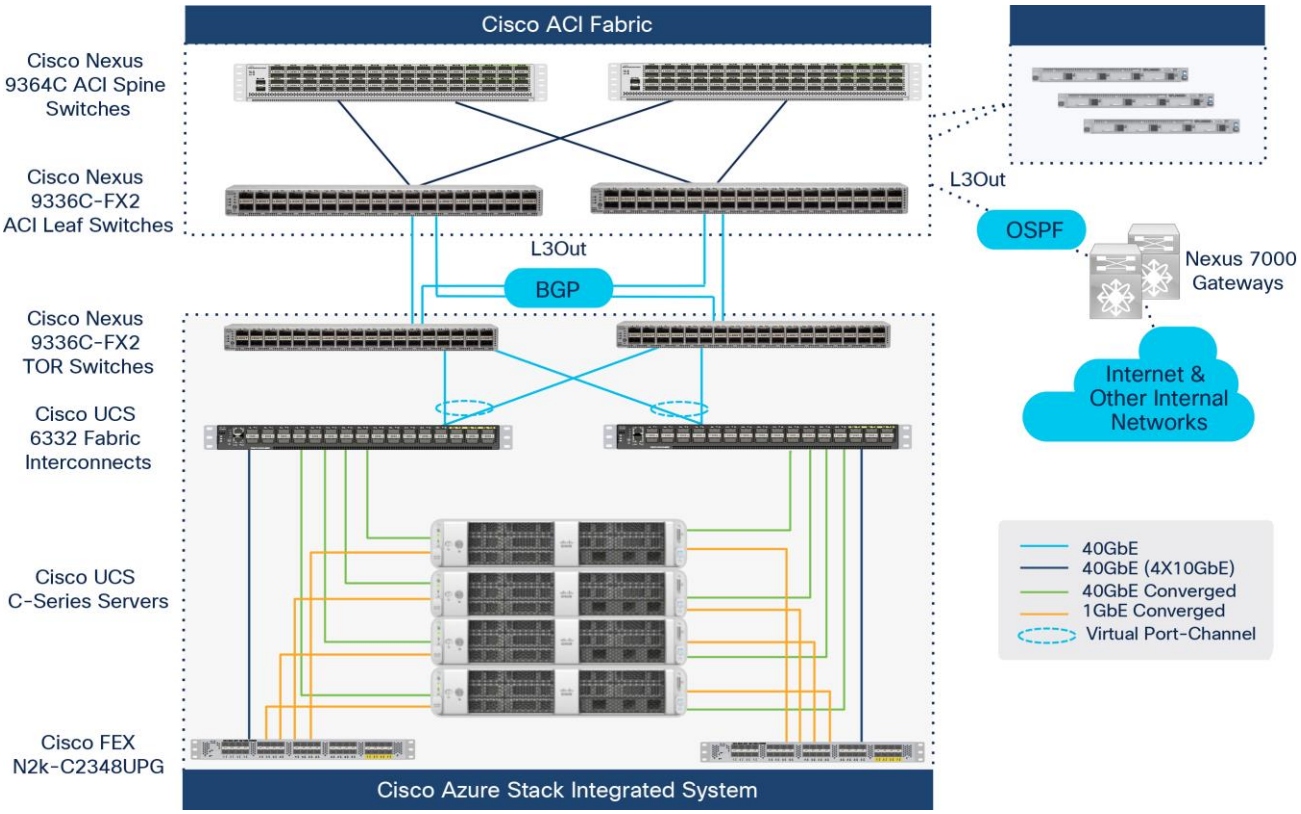


Figure 4.
Physical Architecture

Logical Architecture

The network infrastructure for Azure Stack Hub consists of several logical networks that are configured on the switches. Logical networks represent an abstraction of the underlying physical network infrastructure. They're used to organize and simplify network assignments for hosts, virtual machines (VMs), and services. As part of logical network creation, network sites are created to define the virtual local area networks (VLANs), IP subnets, and IP subnet/VLAN pairs that are associated with the logical network.

The following diagram shows these logical networks and how they integrate with the Nexus 9336C-FX2 TOR switches, Out of Band Management (OOB), and Cisco ACI border leaf switches.

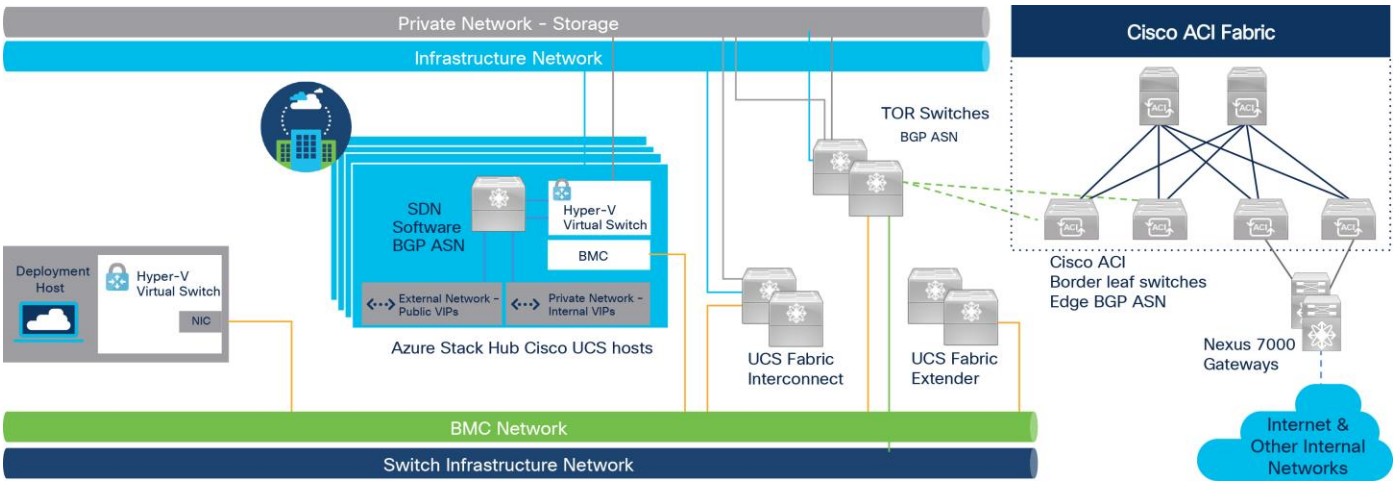


Figure 5.
Azure Stack Hub Logical Architecture

The following table shows the logical networks and associated IPv4 subnet ranges used in this design, the specific loopback and routed interface IP address to support L3Out BGP configuration are covered later in the L3Out design section of the document:

Table 1. Azure Stack Hub Logical Networks

Logical Network	Description	Size	Subnets used in deployment
Public VIP	Azure Stack Hub uses a total of 31 addresses from this network. Eight public IP addresses are used for a small set of Azure Stack Hub services and the rest are used by tenant VMs. If App Service and the SQL resource providers are used, 7 more addresses are required. The remaining 15 IPs are reserved for future Azure services.	/26 (62 hosts) - /22 (1022 hosts) Recommended = /24 (254 hosts)	10.121.170.0/24
Switch infrastructure	Point-to-point IP addresses for routing purposes, dedicated switch management interfaces, and loopback addresses assigned to the switch.	/26	15.15.15.0/26
Infrastructure	Used for Azure Stack Hub internal components to communicate.	/24	10.124.170.0/24
Private	Used for the storage network, private VIPs, Infrastructure containers and other internal functions.	/25 /25	10.123.170.0/25 10.123.179.128/25

Cisco Application Centric Infrastructure Design for Azure Stack Hub border connectivity

The Azure Stack Hub top of rack (TOR) switches require Layer 3 uplinks with Point-to-Point IPs (/30 networks) configured on the physical interfaces. Layer 2 uplinks with TOR switches supporting Azure Stack Hub operations isn't supported. The Border device can support 32-bit BGP autonomous system number (ASN).

This section explains how Azure Stack Hub can connect to Cisco ACI using Layer 3 routing and discusses the access to Shared L3Out. It explains the route exchange between Cisco ACI with Azure Stack Hub Nexus 9336C-FX2 TOR switches and the Nexus 7000 gateways in Shared L3Out, and how to use dynamic routing protocol or static routes between the Cisco ACI border leaf switches and the external gateways (Azure Stack Hub Nexus TOR switches & Nexus 7000 routers).

This design assumes that the customer already has an ACI fabric in place with spine switches and APICs deployed and connected through a pair of leaf switches. In this design, an existing POD in a multi-pod ACI Fabric consisting a pair of Nexus 9364C series spine switches, a 3-node APIC cluster and a pair of Nexus 9336C-FX2 series leaf switches that the Cisco APICs connect into was leveraged, along with a pair of border leaf switches connected to existing datacenter networks and WAN for Internet access and another pair for Azure Stack Hub Hub connectivity.

Please refer to Microsoft documentation at the following link for more details on Azure Stack Hub Border connectivity.
https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-border-connectivity?view=azs-2005

Azure Stack Hub ACI Tenant Model Overview

Figure 6 below illustrates the high-level relationship between various ACI tenant elements as deployed in the design by highlighting the Azure Stack Hub tenant. As shown in the figure, Azure Stack Hub tenant contains a Virtual Routing and Forwarding (VRF), Bridge domain (BD) and an external end point group (EPG) that represents the Azure Stack Hub networks.

For Azure Stack Hub networks to be able to commuinicate with other data center networks and access internet, a contract must exist between the Azure Stack Hub L3Out and the common shared L3Out networks.

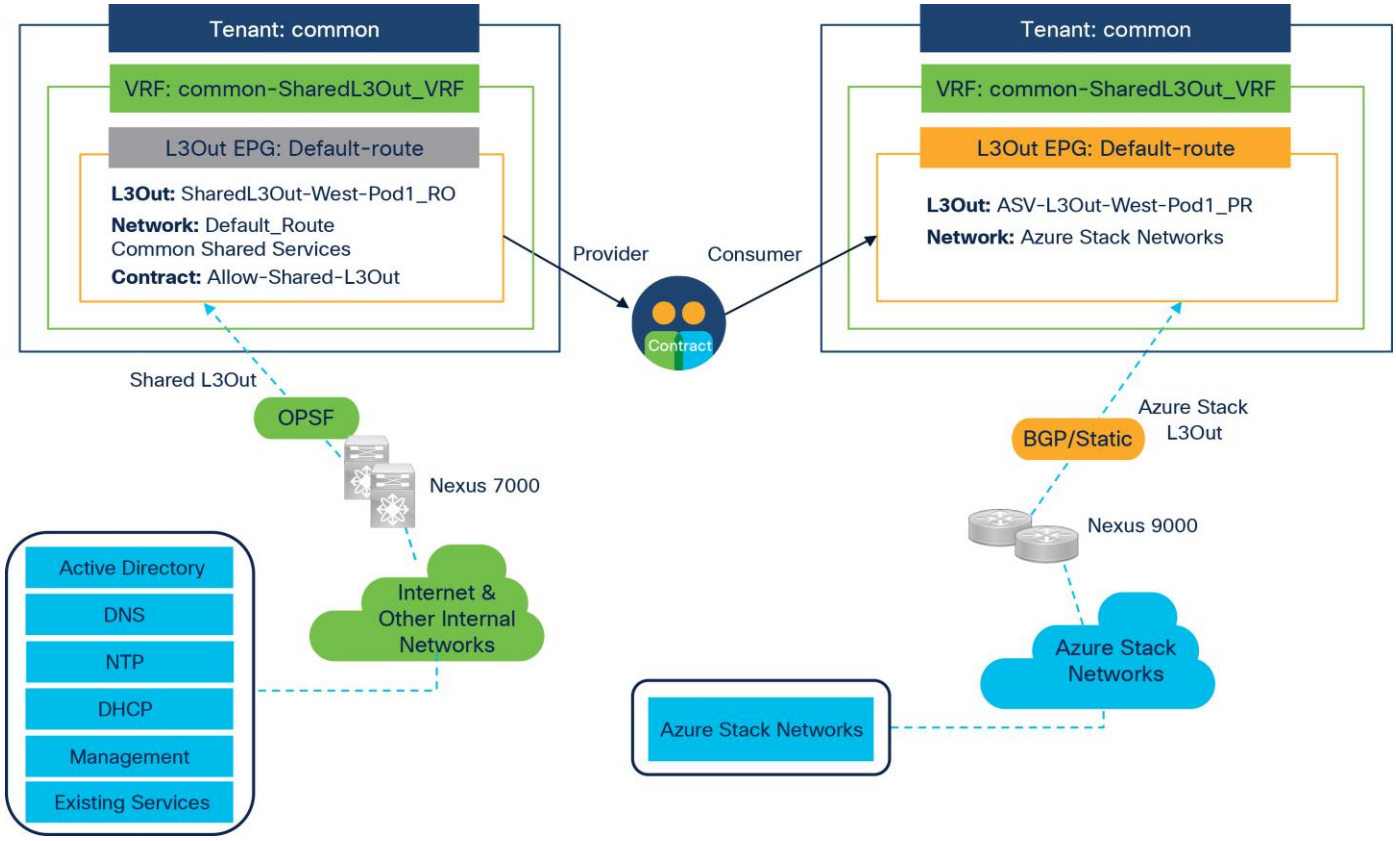


Figure 6.
Azure Stack Hub Tenant Overview

Cisco ACI Layer 3 Out for Azure Stack Hub border connectivity

The ACI fabric is formed from multiple components. Some of these components include bridge domains and endpoint groups to provide Layer (L2) connectivity or default gateway functions for a group of endpoints. Another one is the Layer 3 Out (L3Out), or external routed network in Cisco APIC GUI prior to the APIC Release 4.2), which is to provide Layer 3 (L3) connectivity to external network domains.

A L3Out policy is used to configure interfaces, protocols, and protocol parameters necessary to provide IP connectivity to external routing devices (Azure Stack Hub TOR switches and Nexus 7000 gateways). An L3Out connection is always associated with a VRF. L3Out connections are configured using the L3Out option on the Networking menu for a tenant within the Cisco APIC GUI.

In this design, the Cisco ACI fabric has two pairs of border leaf and two spine switches, that are controlled by an APIC cluster. A pair of border leaf switches have an L3Out configured providing connection to a pair of Nexus 7000 routers and thus to the Internet and Enterprise networks. Another pair of border leafs have an L3Out connecitivity to Azure Stack Hub TOR switches.

Cisco ACI supports Transit routing and ACI fabric allows Azure Stack Hub traffic traverse from Azure Stack Hub L3Out network to the Shared common L3Out as shown in the below figure to access internet and other required network services.

Cisco ACI supports Layer 3 connections using static routing (IPv4 and IPv6) or the dynamic routing protocols (OSPF, BGP & EIGRP), Azure Stack Hub however supports static routing and BGP as the only dynamic routing protocol.

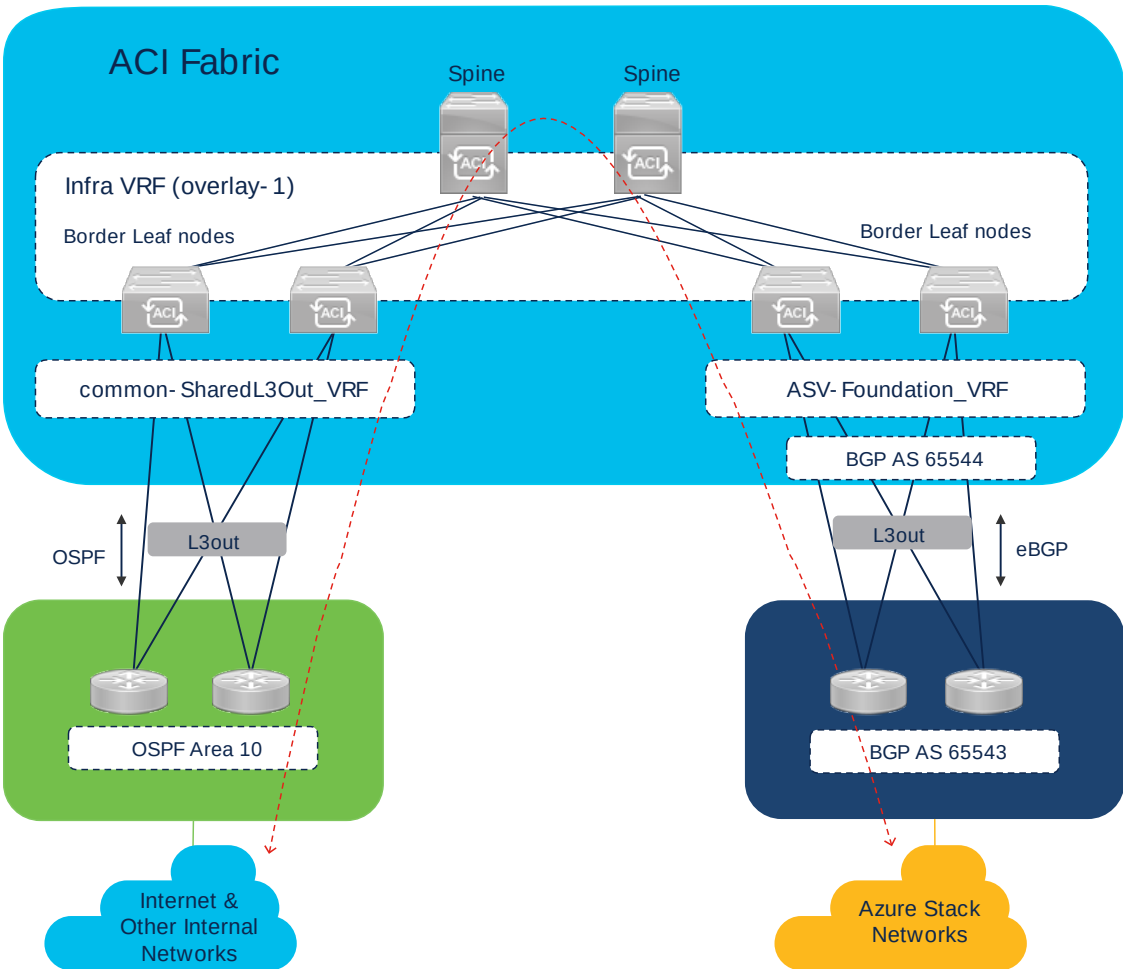


Figure 7.
Cisco ACI as Transit Network to support Azure Stack Hub

Basic Flow of Cisco Azure Stack Hub Traffic via L3Out

The basic flow of Azure Stack Hub network traffic transiting the ACI fabric between Azure Stack Hub L3Out and shared L3Out to access outside networks is described below.

1. Azure Stack Hub networks learned via BGP/Static routing protocol
2. Distribute learned external Azure Stack Hub routes to other leaf switches with in Azure Stack Hub VRF
3. Advertise learned external routes to L3Outs (Transit Routing), in this case the routes will be advertised to common tenant Shared L3Out.

Note: Advertise ACI internal routes (BD subnets) to Azure Stack Hub outside ACI (Optional)

Note: Only when Azure Stack Hub devices need reachability to servers connected to ACI, ACI needs to advertise the BD subnets to Azure Stack Hub outside

4. Allow traffic to arrive from or be sent to external networks via Shared L3Out by using a contract

Note: The same workflow applies to the Shared L3Out routed domain whereby the Azure Stack Hub L3Out learns the **default route** from Shared L3Out domain.

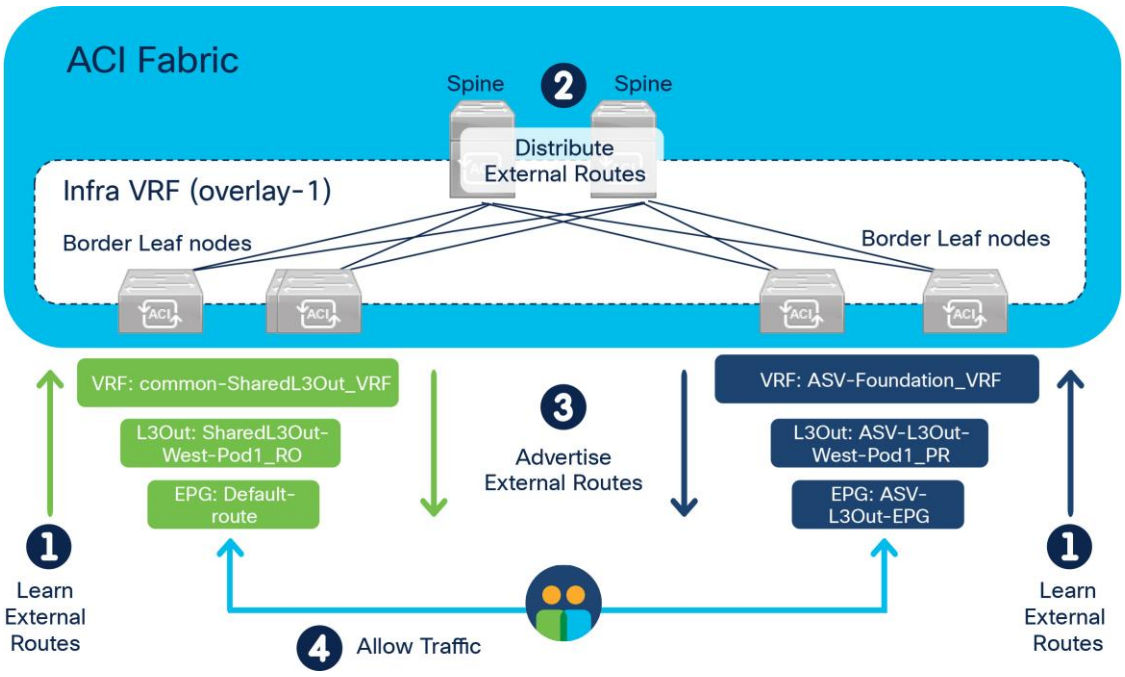


Figure 8.
Azure Stack Hub Traffic flow via ACI Fabric

Azure Stack Hub ACI L3Out object model

Figure 9 below shows the object model for Azure Stack Hub L3Out. This helps in understanding the main building blocks of the L3Out model as implemented for Azure Stack Hub connectivity.

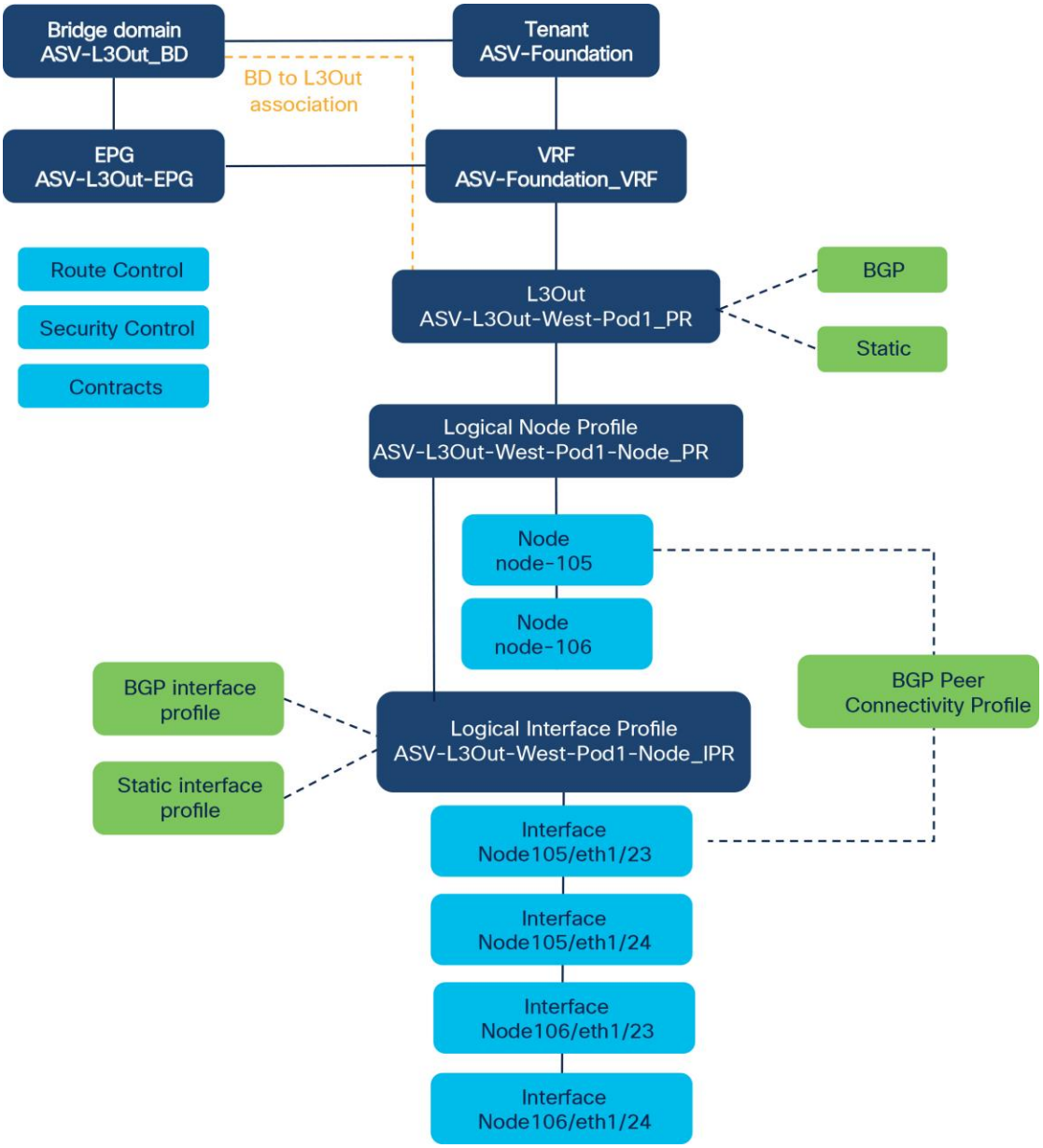


Figure 9.
Azure Stack Hub ACI L3Out object model

The L3Out policy is associated with a VRF and consists of the following:

- **Logical node profile:** This is the leaf wide VRF routing configuration, whether it is dynamic or static routing. For example, we have two border leaf nodes for Azure Stack Hub connectivity, so the logical node profile consists of two leaf nodes.
- **Logical interface profile:** This is the configuration of Layer 3 interfaces on the leaf defined by the logical node profile. The interface selected by the logical interface profile must have been configured with a routed domain in the fabric access policy.
- **External network and EPG:** This is the configuration object that classifies traffic from the outside into a security zone.

ACI L3Out Node and Interface Profiles for Azure Stack Hub point-to-point links

In this design, the ACI border leaf (Azure Stack Hub border) switches connect to the Azure Stack Hub TOR switches using four routed interfaces.

Each border leaf switch is redundantly connected to the Azure Stack Hub TOR switches using 10/40/100GbE links. The four links between ACI leaf switches and Azure Stack Hub external TOR are individual connections with a dedicated IP subnet for each link.

The main function of the L3Out Node and Interface Profiles is to specify which switch nodes should be border leaf switches and which interfaces should speak a routing protocol along with interface-level routing parameters.

There are different ways (here called “patterns”) to configure **node-105 (e1/23, e1/24)** and **node106 (e1/23,e1/24)** to be part of the L3Out and speaking the routing protocol defined in Azure Stack Hub L3Out.

In this design both interfaces are in the same Logical Interface Profile (**ASV-L3Out-West-Pod1-Node_IPR**) under a Logical Node Profile (**ASV-L3Out-West-Pod1-Node_PR**) as shown in the figure below.

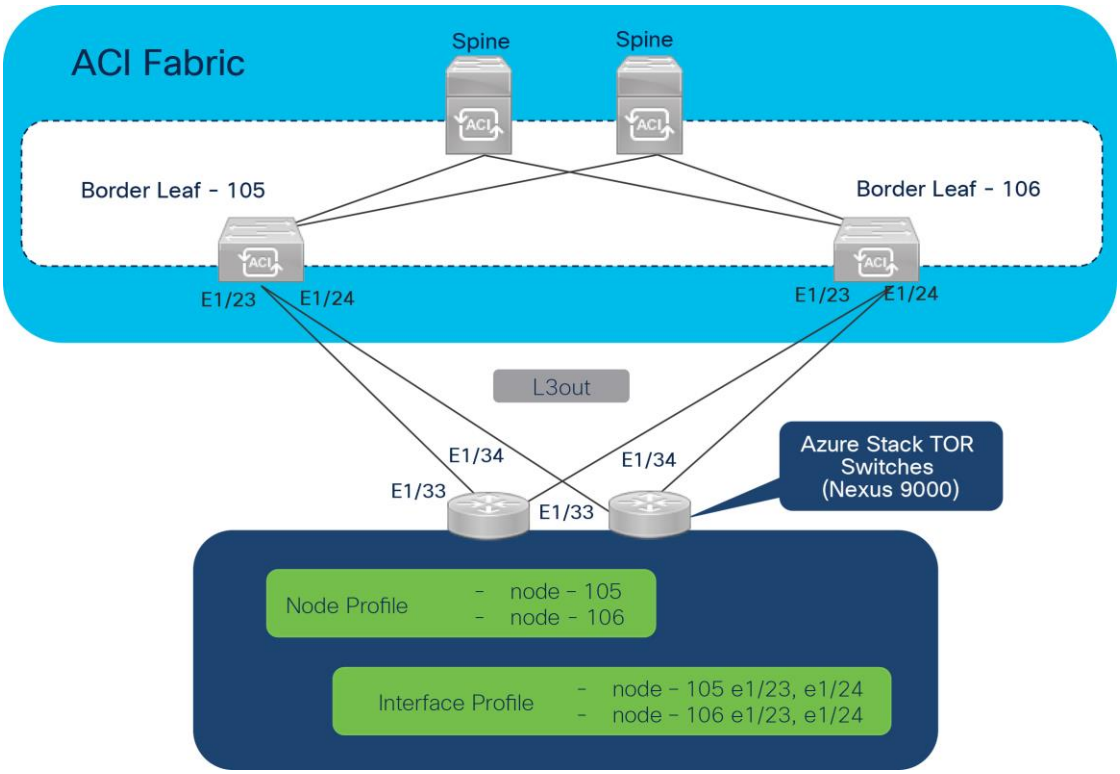


Figure 10.
L3Out Node and Interface Profiles

Azure Stack Hub L3Out BGP

Figure 11 illustrates the configuration example for Azure Stack Hub eBGP with peering on loopback interfaces.

There are two more requirements specific to eBGP peering under the BGP Peer Connectivity Profile.

- Remote AS (**65543**)
- EBGP multihop (This is only when the peer is multiple-hops away, as in the case of loopback peering.)

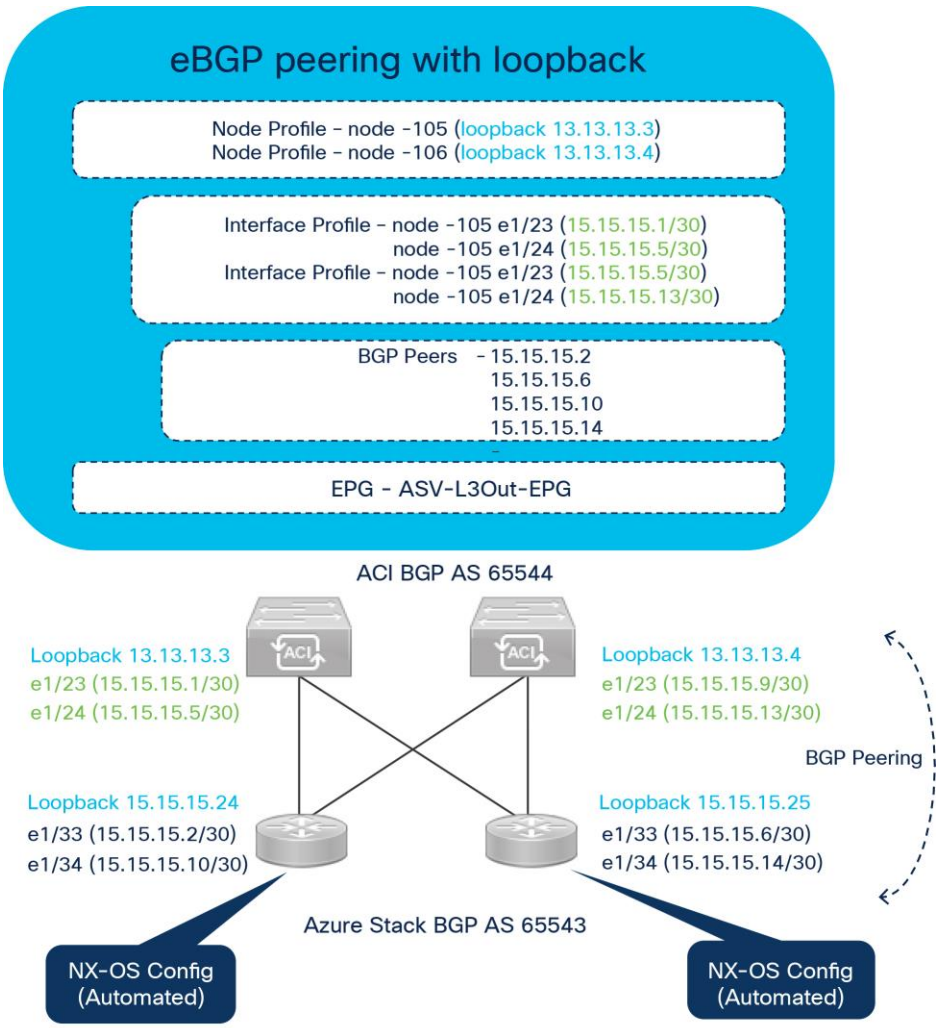


Figure 11.
Azure Stack eBGP Configuration

Azure Stack Hub L3Out static routes

As mentioned earlier, Azure Stack Hub and Cisco ACI support Static routes for Layer 3 connectivity. Static routes are configured as part of L3Out configuration similar to configuring BGP as discussed above. Static routes are configured on each Logical Node Profile under **"Tenant > *ASV-Foundation* > Networking > L3Outs > Logical Node Profiles > Node > Static Routes"**. If only static routes are required without any dynamic routing protocols, users can leave the dynamic routing protocol checkbox on the root L3Out component blank and configure only the Logical Node Profile with Static Routes and the Logical Interface Profile. This still requires associating the VRF and the External Routed Domain on the root L3Out component.

ACI L3Out subnet scope options

Layer 3 outside networks (L3Outs) for external EPGs are used to control which prefixes are allowed into or out of the fabric and which external networks are allowed to communicate with internal or other external networks.

Figure 12 shows the subnet scope options along with the aggregate options used in the validation setup.

The options shown are grouped into two different groups. One (the green group in Figure 19) is for options to manipulate the routing table and routing protocol via IP prefix-lists and route maps on a border leaf. Another one (the blue group in Figure 12) is for options related to contracts.

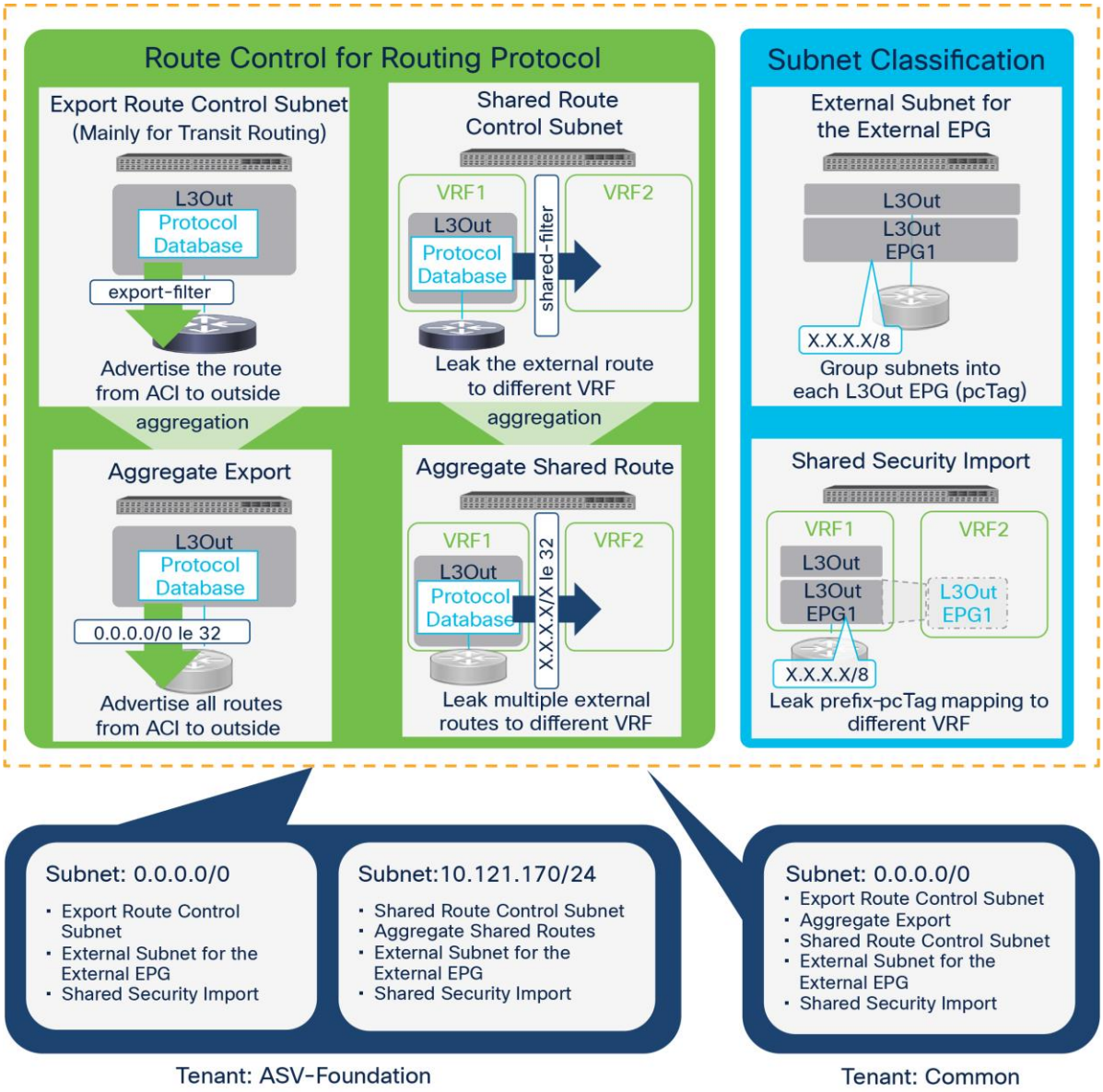


Figure 12.
L3Out Subnet Scope Options available

ASV-Foundation tenant (Azure Stack Hub L3Out)

- **Subnet**: 0.0.0.0/0
  - **Export Route Control Subnet** with **Aggregate Export disabled** to advertise only the default route in to Azure Stack Hub domain.
  - **External Subnets for External EPG** to allow packets with the configured subnet from or to the L3Out with a contract.

- **Shared Security Import Subnet** scope is used to allow packets with the configured subnet when the packets are going across VRFs with an L3Out.

- **Subnet:** 10.121.170.0/24 (Optional) : Azure Stack Hub can be deployed with just the default route advertised from the Shared L3Out, however in our setup the Azure Stack Hub portal is also accessed from the customer corporate network and to reach the Azure Stack Hub public IP network (10.121.170.0), we have advertised/leaked the network from Azure Stack Hub domain to Shared L3Out.
  - **Shared Route Control Subnet** scope is to leak an Azure Stack Hub external subnet (10.121.170.0) to VRF in Common tenant. ACI uses MP-BGP and route target to leak an external route from one Azure Stack Hub VRF to another VRFs. This scope creates an IP prefix-list with the subnet, which is used as a filter to export/import routes with the route target in MP-BGP.
  - **Aggregate Shared Routes** option is used for any subnets with "Shared Route Control Subnet", with both options enabled, ACI creates an IP prefix-list with "10.121.170.0/24 le 32", which allows more specifics of the aggregate received to be advertised .
  - **External Subnets for External EPG** and **Shared Security Import Subnet** scopes to leak routes in the routing table of Shared L3Out VRF (common-SharedL3Out_VRF) using a contract and inform the VRF of the Azure Stack Hub L3Out EPG (ASV-L3Out-EPG) that the leaked route belongs to.

common tenant (Shared L3Out)

- **Subnet**: 0.0.0.0/0
  - **Export Route Control Subnet** with **Aggregate Export enabled** to advertise any routes learned in to Shared L3Out domain.
  - **Shared Route Control Subnet** with **Aggregate Export disabled** to advertise only the default route in to the fabric and other tenants.
  - **External Subnets for External EPG** and **Shared Security Import Subnet** scopes to allow route leaking using a contract and inform the VRF of the L3Out EPG that the leaked route belongs to.

Solution Deployment

This section provides a detailed procedure for configuring the Cisco ACI fabric for use in the environment and is written where the components are added to an existing Cisco ACI fabric as new ACI components.

Note: Once the ACI L3Out configuration is completed as per the procedure in this document, Azure Stack Hub Hub can be installed. Prior to Azure Stack Hub installation, the installation engineer runs network validation scripts from the deployment host connected to the Azure Stack TOR switch. This scripts check the TOR switch border connectivity as well as access to the NTP, DNS and Internet (in the case of connected install). Unless all the checks are passed installation cannot proceed.

Note: The Cisco ACI fabric deployment and the automated installation of Azure Stack Hub are not part of this document. Previous configuration of the ACI fabric and the Shared L3Out configuration is assumed to pre-exist and the configuration details of the same have not been included as they vary based on each customers deployment.

Table 2 lists the hardware and software versions used solution validation.

Table 2. Hardware and Software Versions

Layer	Device	Software version	Comments
Cisco ACI	Cisco APIC	4.2(4i)	ACI Controller
	Cisco Nexus Switches	N9336C-FX2-14.2(4i)	ACI Spine and Leaf Switches
Cisco Azure Stack Hub		2002	Azure Stack Hub release (Includes individual releases of software for all the devices that are part of Azure Stack Hub)

Note: The Azure Stack Hub Software version and TOR Switch versions are point in time based on validated environment and the these versions may change over time and fully supported.

ACI Layer 3 Routed Connectivity to Azure Stack Hub Networks

The design assumes that an ACI fabric of spine switches and APICs already exists in the customer's environment, so this document does not cover the configuration required to bring the initial ACI fabric online and the Shared L3Out routed connectivity.

The Azure Stack Hub L3Out connection is established in a user tenant (**ASV-Foundation**). The connection uses four 40GbE interfaces between border leaf switches deployed earlier and pair of Nexus 9336C-FX2 switches functioning as Azure Stack Hub TOR switches. The Nexus 9336C-FX2 switches serve as the external gateway to the Azure Stack Hub networks. BGP is utilized as the routing protocol to exchange routes between the two networks. Some highlights of this connectivity are:

- A pair of Nexus 9336C-FX2 TOR switches used as border leaf switches outside the ACI fabric using 4 x 40GbE links. Nexus 9336C-FX2 switches serve as a gateway to the Azure networks outside the fabric.
- Routing protocol used to exchange routes between the ACI fabric and networks outside ACI is BGP
- Fabric Access Policies are configured on ACI Leaf switches to connect to the External Routed domain using VLAN pool (vlans: **411-414**).
- The Shared L3Out created in common Tenant "provides" an external connectivity contract that can be "consumed" from Azure Stack Hub Tenant.

Note: The Shared L3Out configuration has not been covered in this document.

Table 3. Azure Stack Hub Tenant details

Property	Azure L3Out, Node 105,106 (Border Leafs)
Tenant	ASV-Foundation
VRF	ASV-Foundation_VRF
Layer 3 Outside	ASV-L3Out-West-Pod1_PR
Bridge domain	ASV-L3Out_BD

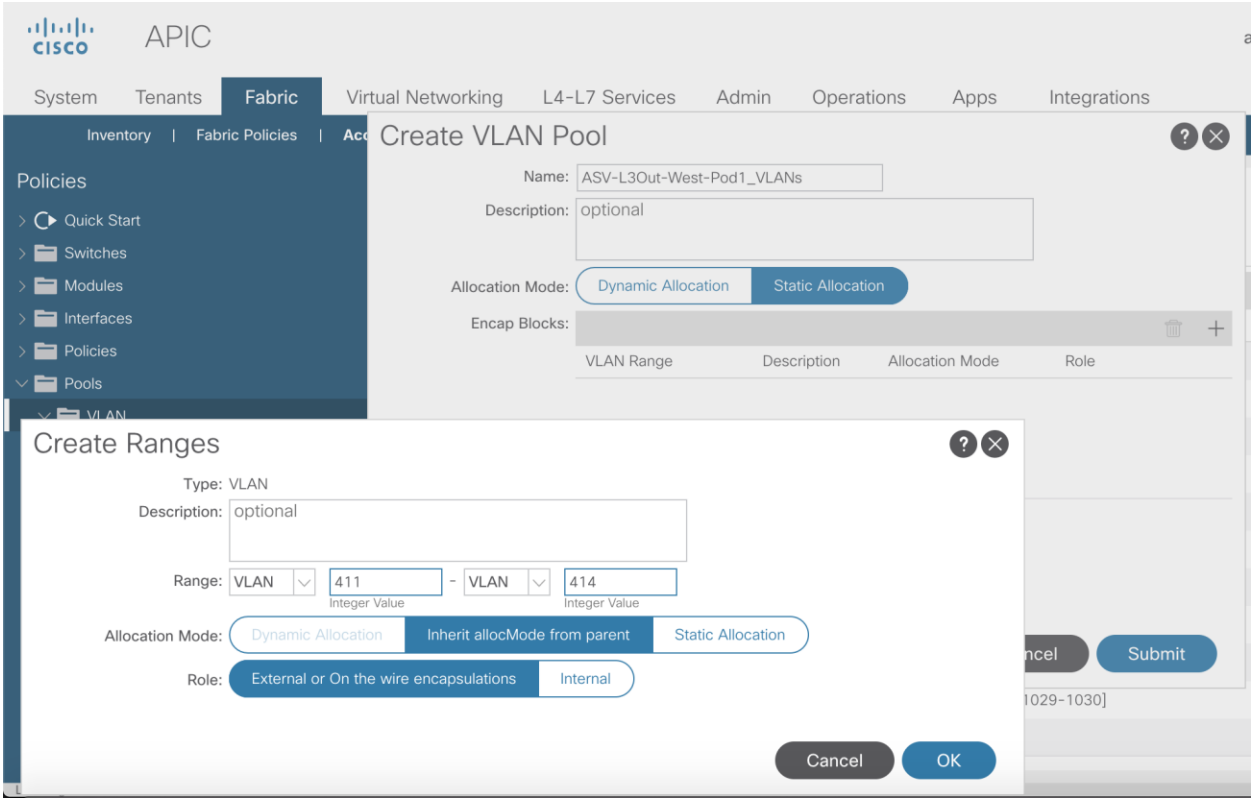
Property	Azure L3Out, Node 105,106 (Border Leafs)
Nodes	Node 105 & 106, with profile ASV-L3Out-West-Pod1-Node_PR with router IDs (13.13.13.3, 13.13.13.4)
Interface	BGP interface at eth1/23 & eth1/24 on both nodes with IP address 15.15.15.1/24, 15.15.15.5/24, 15.15.15.9/24, 15.15.15.13/24
BGP details	Peer address 15.15.15.2/24, 15.15.15.6/24, 15.15.15.10/24, 15.15.15.14/24 and ASN 65533 (Remote) , 65534 (Local)
EPG	External EPG at 0.0.0.0/0 and 10.121.170.0/24
Contract	Allow-Shared-L3Out provided by tenant common

Create VLAN Pool for Azure Stack Hub Routed Domain

In this section, a VLAN pool is created to enable connectivity to the Azure Stack Hub networks, outside the ACI fabric.

To configure a VLAN pool to connect to Azure Stack Hub TOR switches outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the **admin** account.
2. From the top navigation menu, select **Fabric** > **Access Policies**.
3. From the left navigation pane, expand and select **Pools** > **VLAN**.
4. Right-click and select **Create VLAN Pool**.
5. In the Create VLAN Pool pop-up window, specify a Name (for example, **ASV-L3Out-West-Pod1_VLANs**) and for Allocation Mode, select Static Allocation.
6. For **Encap Blocks**, use the **[+]** button on the right to add VLANs to the VLAN Pool. In the **Create Ranges** pop-up window, configure the VLANs that need to be configured from the Border Leaf switches to the external gateways outside the ACI fabric. Leave the remaining parameters as is.



7. Click **OK**.
8. Click **Submit** to complete.

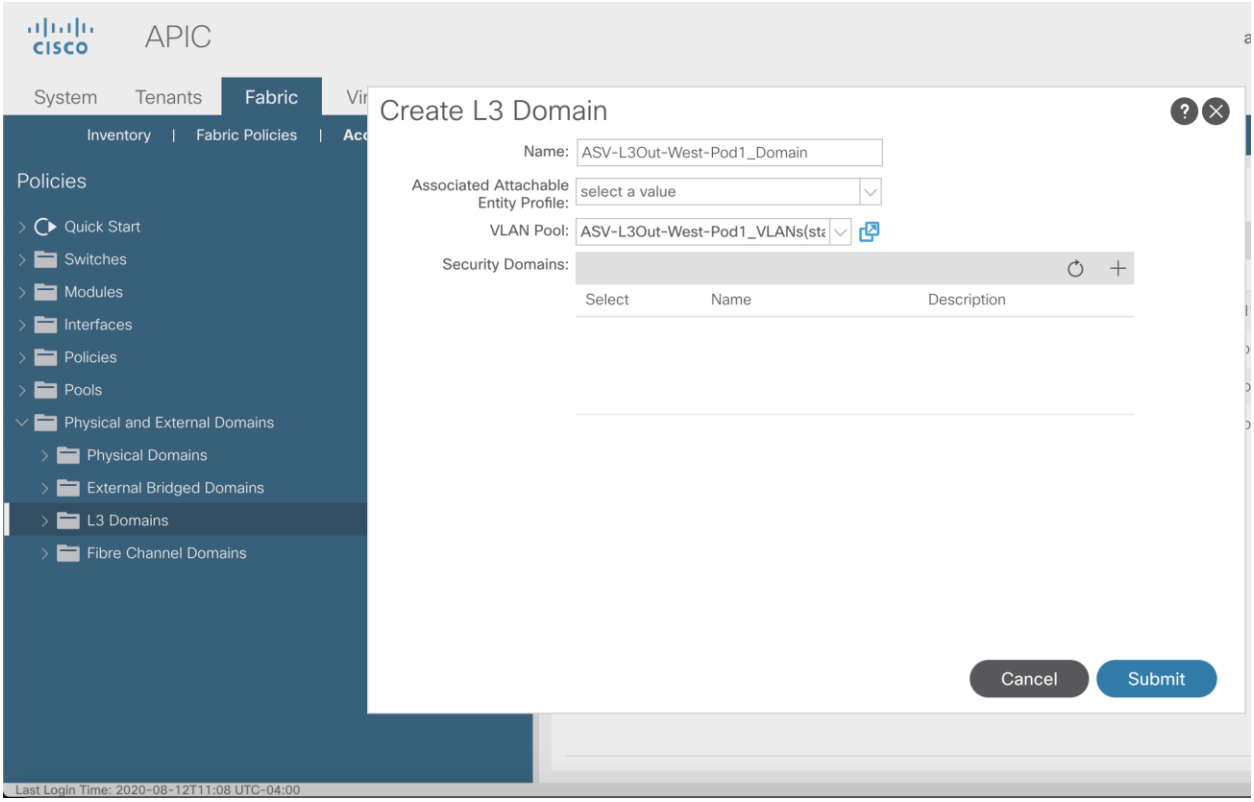
Configure Domain Type for External Routed Domain

Table 4. Domain Type for Azure Stack Hub L3Out

To Azure Stack Networks Outside ACI	Domain Name	Domain Type	VLAN Pool Name	Connects To
	ASV-L3Out-West-Pod1_Domain	External Routed Domain	ASV-L3Out-West-Pod1_VLANs	Azure Stack L3 Gateway Routers Outside ACI

To specify the domain type to connect to Azure Stack Hub external gateway routers outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the **admin** account.
2. From the top navigation menu, select **Fabric > Access Policies**.
3. From the left navigation pane, expand and select Physical and External Domains > External Routed Domains.
4. Right-click External Routed Domains and select Create **Layer 3 Domain**.
5. In the Create Layer 3 Domain pop-up window, specify a Name for the domain. For the VLAN Pool, select the previously created VLAN Pool from the drop-down list.



6. Click **Submit** to complete.

Create Attachable Access Entity Profile for Azure Stack Hub External Routed Domain

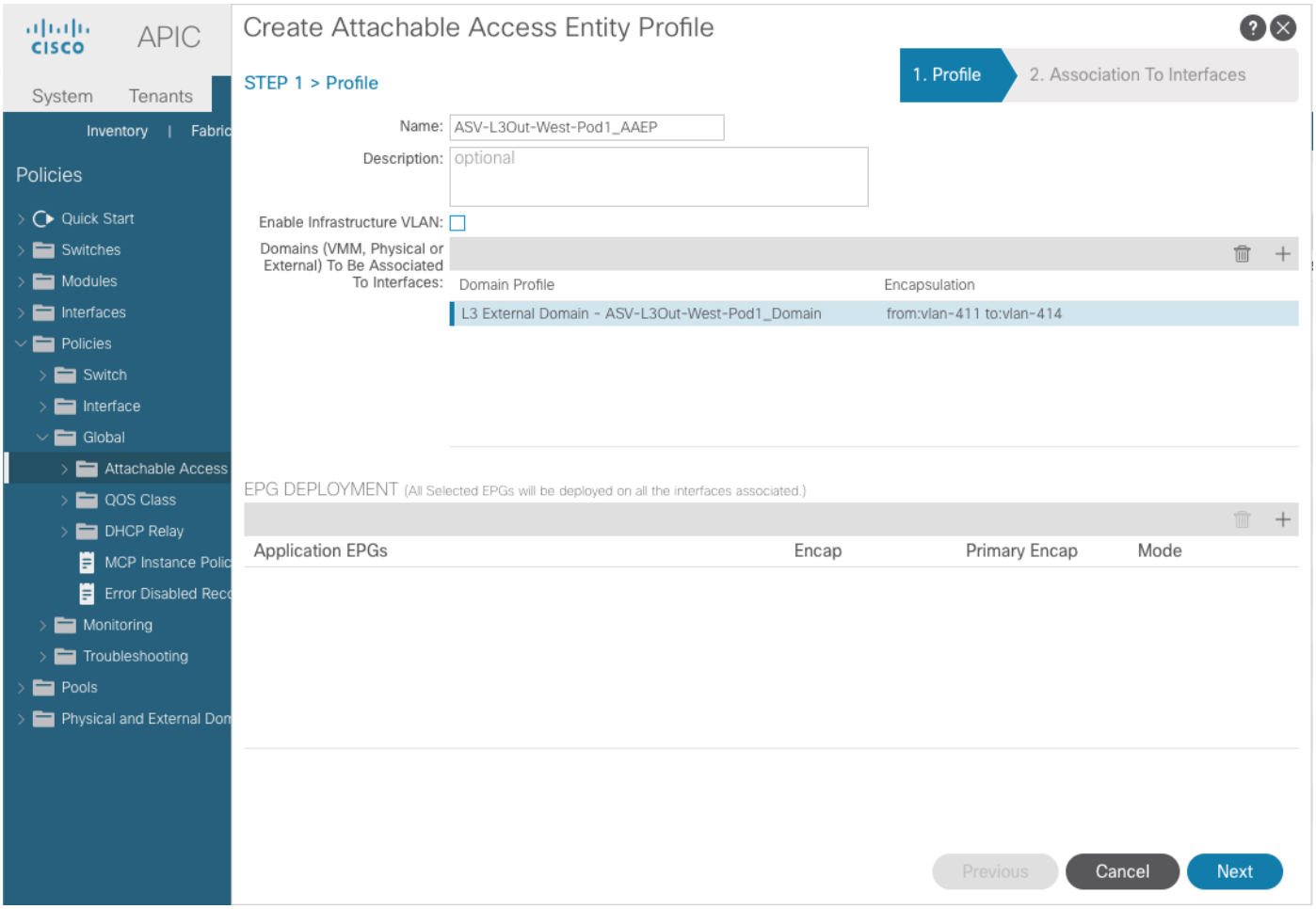
Table 5. Attachable Access Entity Profile (AAEP) for Azure Stack Hub L3Out

	AAEP Name	Domain Name	VLAN Pool Name	Connects To
To Azure Stack Networks Outside ACI	ASV-L3Out-West-Pod1_AAEP	ASV-L3Out-West-Pod1_Domain	ASV-L3Out-West-Pod1_VLANs	L3 Gateway Routers Outside ACI

To create an Attachable Access Entity Profile (AAEP) to connect to external gateway routers outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the **admin** account.
2. From the top navigation menu, select **Fabric** > **Access Policies**.
3. From the left navigation pane, expand and select **Policies** > **Global** > **Attachable Access Entity Profiles.**
4. Right-click and select Create Attachable Access Entity Profile.
5. In the Create Attachable Access Entity Profile pop-up window, specify a Name (for example, **ASV-L3Out-West-Pod1_AAEP**).
6. For the **Domains**, click the **[+]** on the right-side of the window and select the previously created domain from the drop-down list below **Domain Profile**.

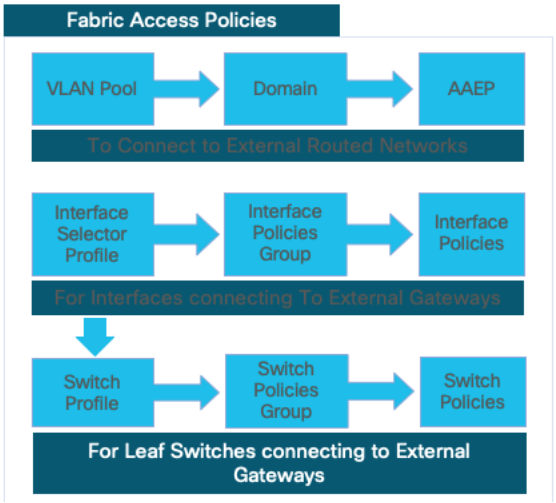
7. Click **Update**.
8. You should now see the selected domain and the associated VLAN Pool as shown below.



9. Click **Next**. This profile is not associated with any interfaces at this time. They can be associated once the interfaces are configured in an upcoming section.
10. Click **Finish** to complete.

Configure Interfaces to External Routed Domain

Border Leaf switches (**Node ID: 105,106**) in Pod-1 connect to Azure Stack Hub TOR Gateways (Nexus 9336C-FX2 series switches) using 40Gbps links, on ports 1/23 and 1/24.



Azure Stack L3Out : Pod-1 Fabric Access Policies

Access Entity Profile	
VLAN Pool	ASV-L3Out-West-Pod1_VLANs
External Routed Domain	ASV-L3Out-West-Pod1_Domain
AAEP	ASV-L3Out-West-Pod1_AAEP

Interface Profile	
Interface Policies	40Gbps-Link, CDP-Enabled, LLDP-Enabled, BPDU-FG-Enabled, VLAN-Scope-Global
Interface Policy Group	ASV-L3Out-West-Pod1_PG
Interface Selector Profile	ASV-L3Out-West-Pod1_IPR
Access Port Selector	SharedL3Out-West-Pod1_p1_23-24

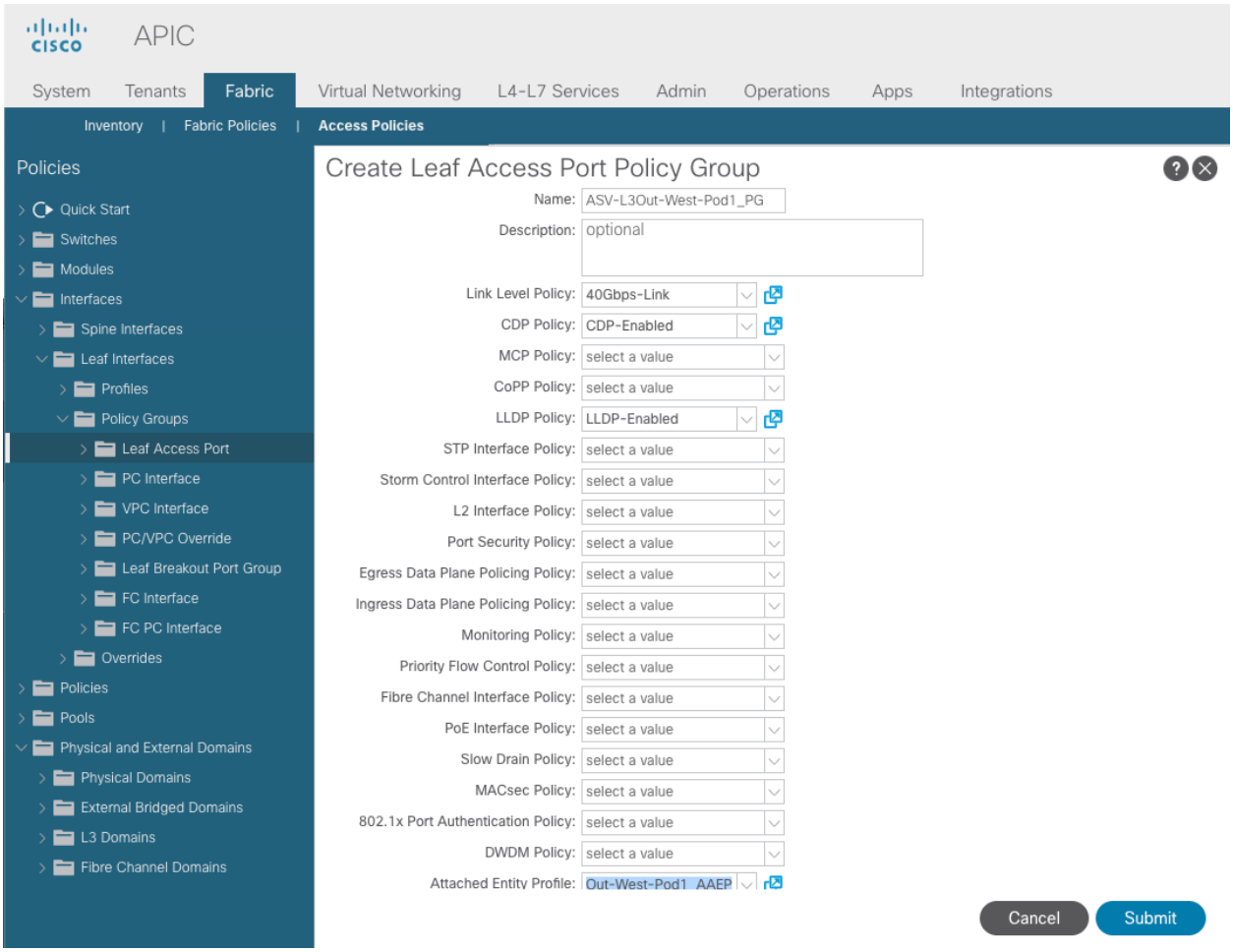
Switch Profile	
Switch Selector	ASV-L3Out-West-Pod1-Leaf_105-106
Switch Selector Profile	ASV-L3Out-West-Pod1-Leaf_PR

Figure 13.
Fabric Access Policies for Azure Stack Hub L3Out

Create Interface Policy Group for Interfaces to Azure Stack Hub Routed Domain

To create an interface policy group to connect to external gateways outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the admin account.
2. From the top navigation menu, select **Fabric > Access Policies**.
3. From the left navigation pane, expand and select Interfaces > Leaf Interfaces > Policy Groups > Leaf Access Port.
4. Right-click and select Create Leaf Access Port Policy Group.
5. In the Create Leaf Access Port Policy Group pop-up window, specify a Name and select the applicable interface policies from the drop-down list for each field.
6. For the Attached Entity Profile, select the previously created AAEP to external routed domain.

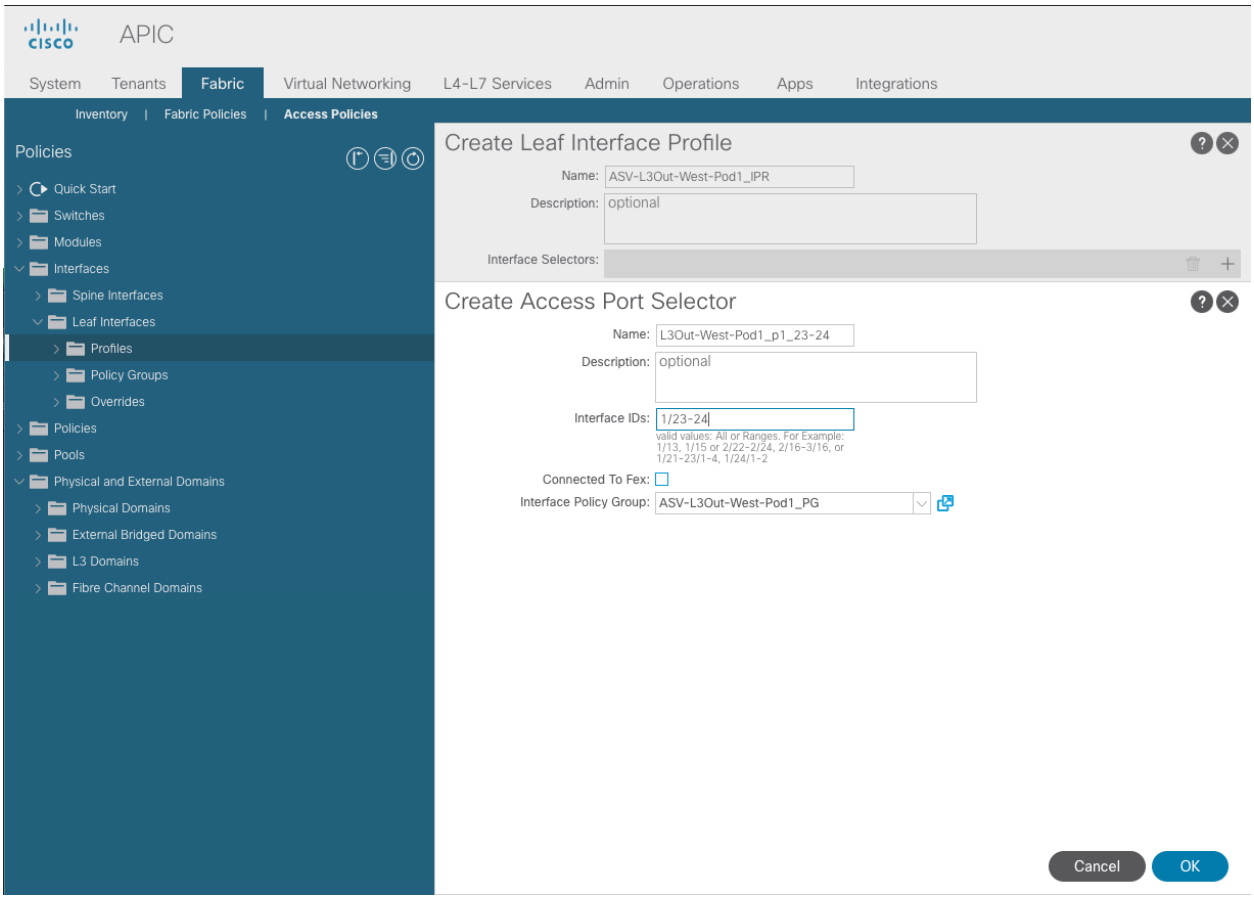


7. Click **Submit** to complete.

Create Interface Profile for Interfaces to Azure Stack Hub Routed Domain

To create an interface profile to connect to Azure Stack Hub external gateways outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the admin account.
2. From the top navigation menu, select **Fabric > Access Policies**.
3. From the left navigation menu, expand and select **Interfaces > Leaf Interfaces > Profiles**.
4. Right-click and select Create Leaf Interface Profile.
5. In the **Create Leaf Interface Profile** pop-up window, specify a **Name**. For **Interface Selectors,** click the **[+]** to select access ports to apply interface policies to. In this case, the interfaces are access ports that connect Border Leaf switches to Azure Stack Hub gateways outside ACI.
6. In the **Create Access Port Selector** pop-up window, specify a selector **Name.** For the **Interface IDs**, specify the access ports connecting to the two external gateways. For the **Interface Policy Group,** select the previously created Policy Group from the drop-down list.

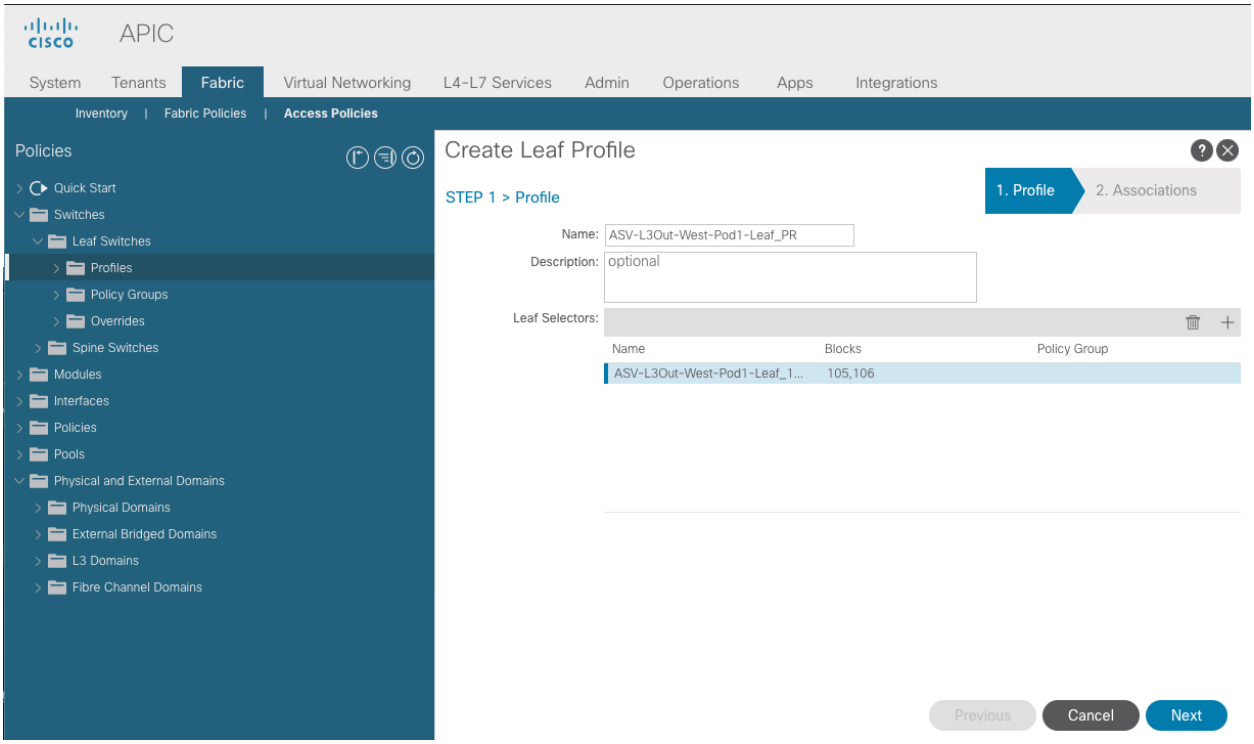


7. Click **OK** to complete and close the **Create Access Port Selector** pop-up window.
8. Click **Submit** to complete and close the **Create Leaf Interface Profile** pop-up window.

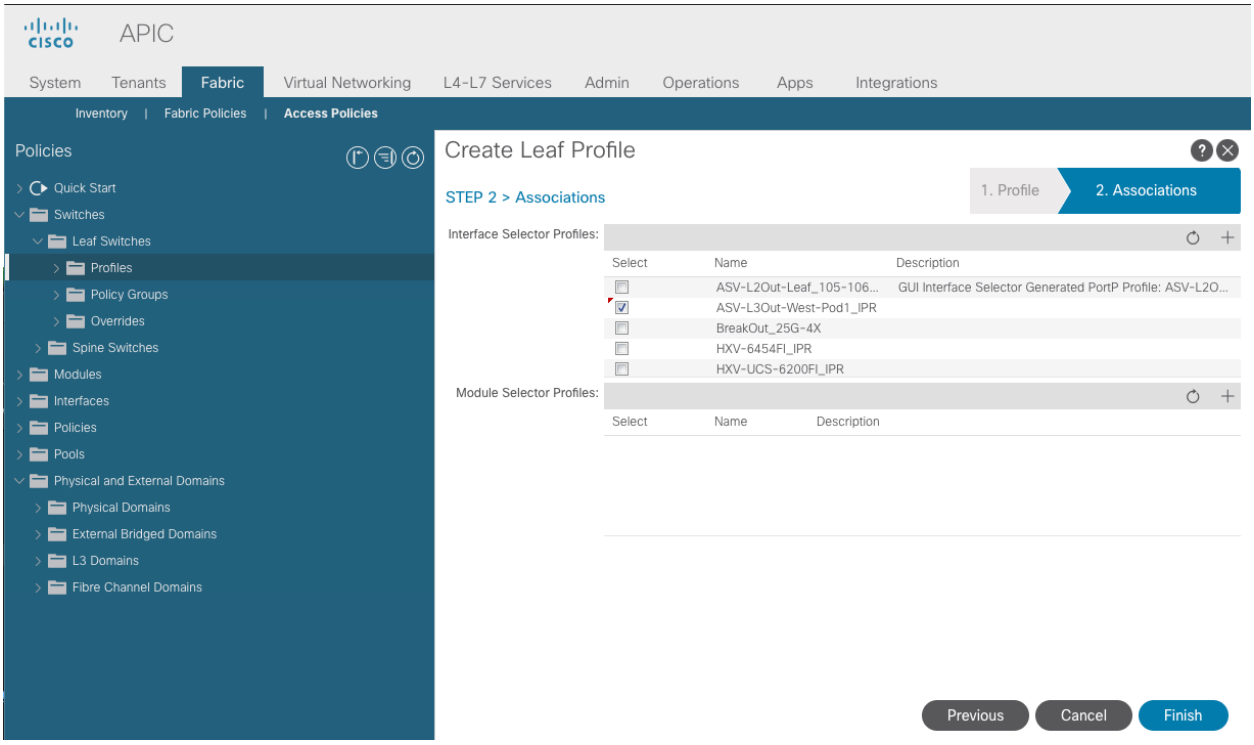
Create Leaf Switch Profile to External Routed Domain

To create a leaf switch profile to configure connectivity to external gateway routers outside the ACI fabric, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the admin account.
2. From the top navigation menu, select **Fabric > Access Policies**.
3. From the left navigation menu, expand and select **Switches > Leaf Switches > Profiles**.
4. Right-click and select **Create Leaf Profile**.
5. In the Create Leaf Profile pop-up window, specify a profile Name. For Leaf Selectors, click the [+] to select the Leaf switches to apply the policies to. In this case, the Leaf switches are the Border Leaf switches that connect to the Azure Stack Hub gateways outside ACI.
6. Specify a Leaf Selector Name. For the Interface IDs, specify the access ports connecting to the two external gateways. For Blocks, select the Node IDs of the Border Leaf switches from the drop-down list. Click **Update**.



7. Click **Next**.
8. In the Associations window, select the previously created Interface Selector Profiles from the list.



9. Click **Finish** to complete.

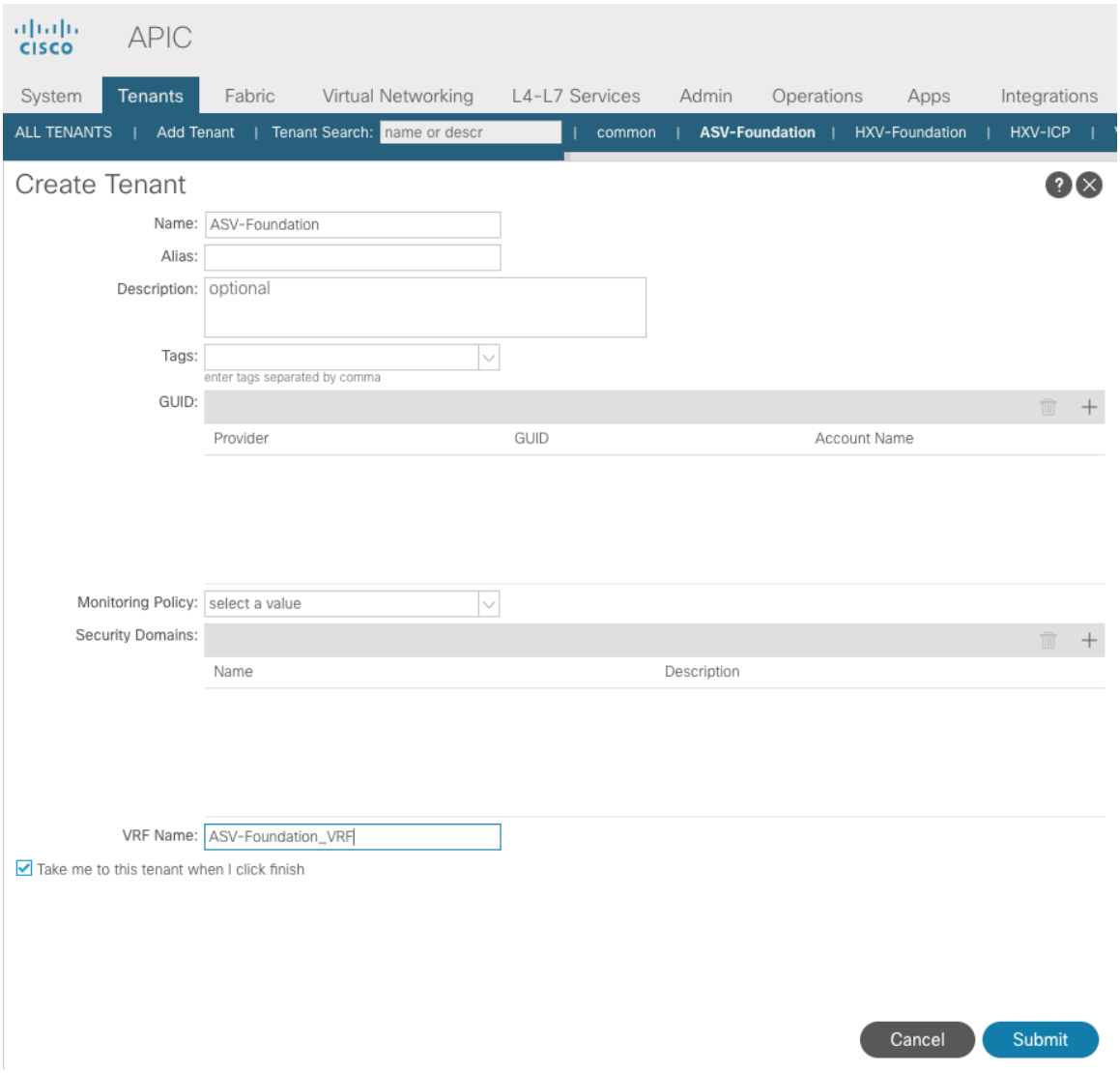
Configure Tenant Networking for Azure Stack Hub L3Out

Table 6. Tenant Networking for Shared L3Out

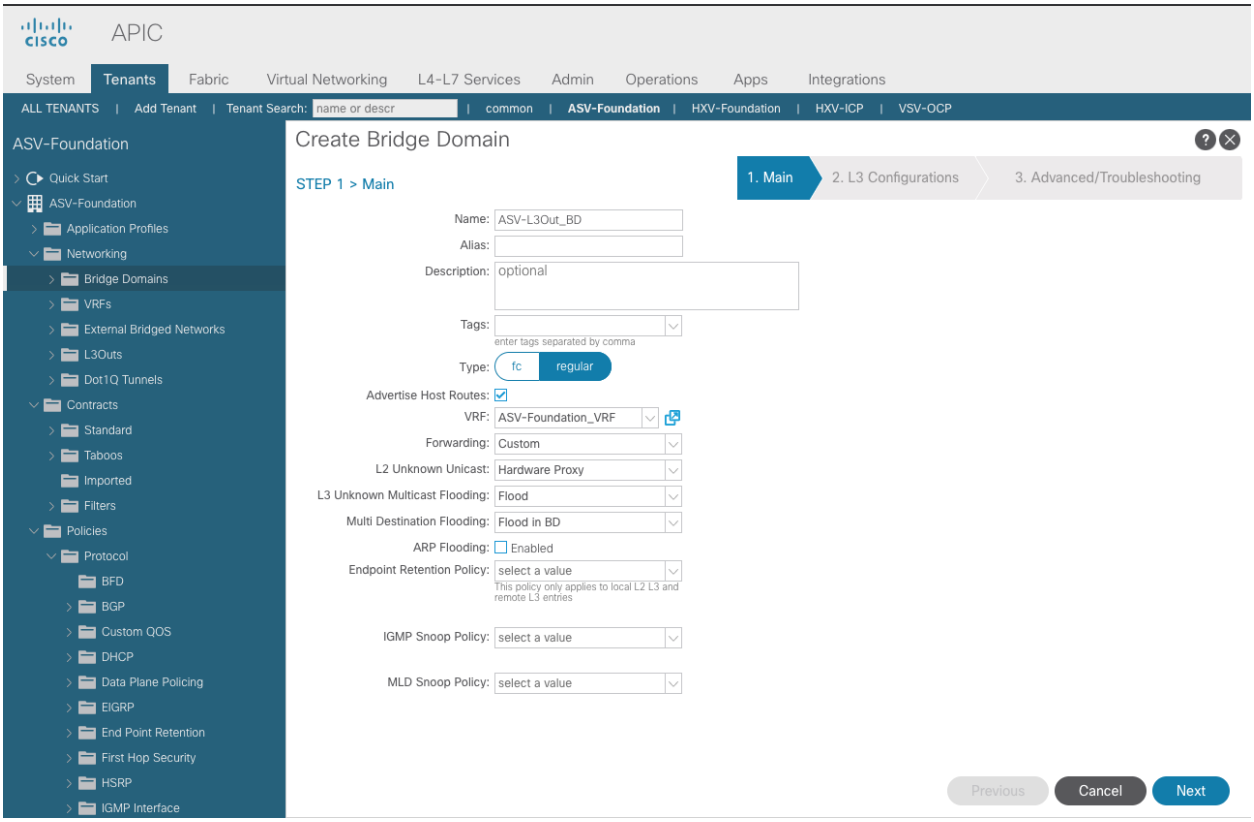
	Tenant Name	VRF	Bridge Domain
Shared L3Out	ASV-Foundation	ASV-Foundation_VRF	ASV-L3Out_BD

To configure Azure Stack Hub tenant networking, follow these steps:

1. Use a browser to navigate to the APIC GUI. Log in using the admin account.
2. From the top navigation menu, select **Tenants > Add Tenant**
3. In the Create Tenant dialog box, specify a Name (for example, **ASV-Foundation**).
4. In the VRF Name field, enter the VRF name (for example, **ASV-Foundation_VRF**).
5. Click **Submit**.



6. To create a bridge domain, in the Navigation pane, expand **Tenant and Networking**
7. Right-click **Bridge Domains** and choose Create Bridge Domain.
8. In the Name field, specify a Name (for example, **ASV-L3Out_BD**).
9. In the VRF field, from the drop-down list, choose the VRF we created (ASV-Foundation_VRF in this example)
10. Uncheck ARP flooding
11. Select Forwarding as **custom**



12. Click **Next** on L3 Configurations page and
13. Click **Finish** to complete on the Advanced/Troubleshooting page.

Configuring BGP External Routed Azure Stack Hub Networks

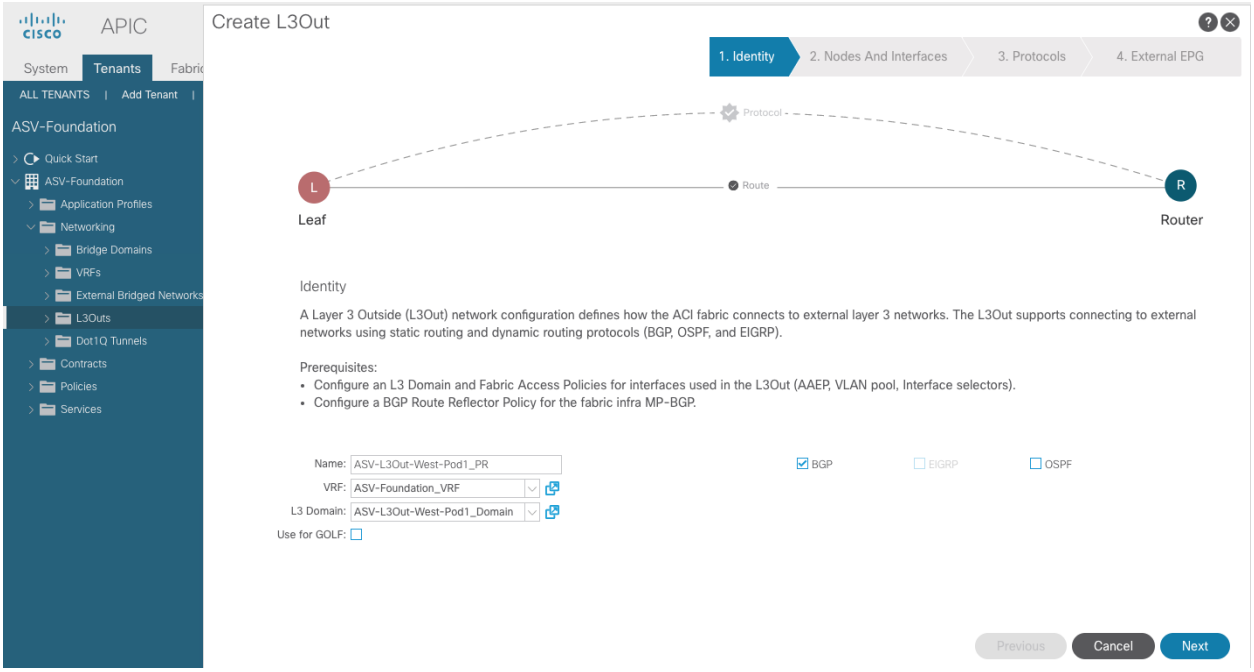
Table 7. Azure Stack Hub L3Out – Pod-1

Azure Stack L3Out – Pod-1

L3Out Name	Routed Node Profile	Router IDs (/32 Mask)	Node IDs	Node Interface Profile
ASV-L3Out-West-Pod1_PR BGP ASN (65534)	ASV-L3Out-West-Pod1-Node_PR	13.13.13.3 13.13.13.4	101 102	ASV-L3Out-West-Pod1-Node_IPR

Routed interfaces	Subnet	External Network	External Network
Node-105, Eth1/23	15.15.15.0/30	Default-Route (0.0.0.0/0)	Azure Stack Public Network (10.121.170.0/24)
Node-105, Eth1/24	15.15.15.4/30	✓ External Route Control Subnet	✓ External Subnets for the External EPG
Node-106, Eth1/23	15.15.15.9/30	✓ External Subnets for the External EPG	✓ Shared Route Control Subnet + Aggregate Shared Routes
Node-106, Eth1/24	15.15.15.12/30	✓ Shared Security Import Subnet	✓ Shared Security Import Subnet

1. In the Navigation pane, expand Tenant_name **(ASV-Foundation) > Networking > L3Outs**.
2. Right-click, and click **Create L3Out**.
3. The Create L3Out wizard appears.

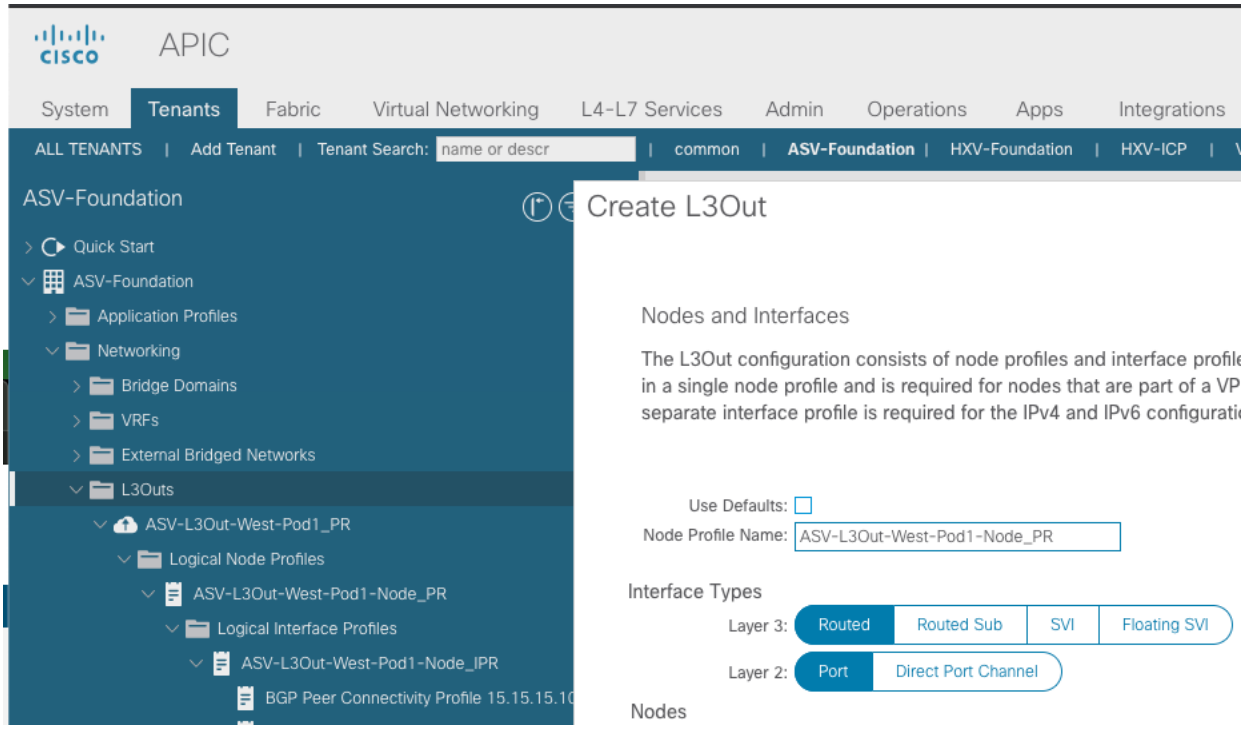


4. Enter the necessary information in the Identity window of the Create L3Out wizard.
5. Enter the necessary information in the Name, VRF and L3 Domain fields.
6. In the area with the routing protocol check boxes, choose **BGP**

Note: BGP peer reachability must be available in one of two ways (OSPF or Static routes). We used static routes in this setup, the same can be configured after the L3Out configuration.

7. Click **Next** to move to the Nodes and Interfaces window.

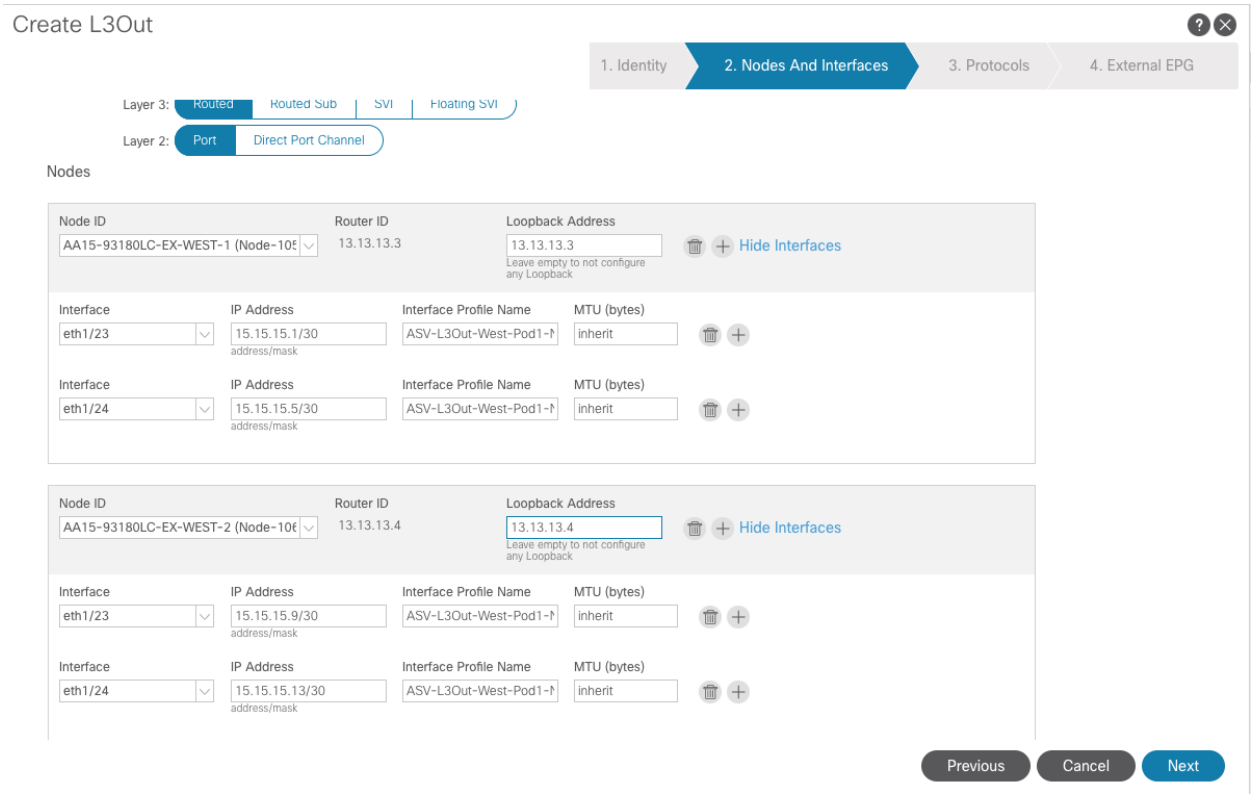
8. Enter the necessary information in the **Nodes and Interfaces** window of the **Create L3Out wizard**.
9. In the **Layer 3** area, select **Routed** and select **Port** in the **Layer 2** area.



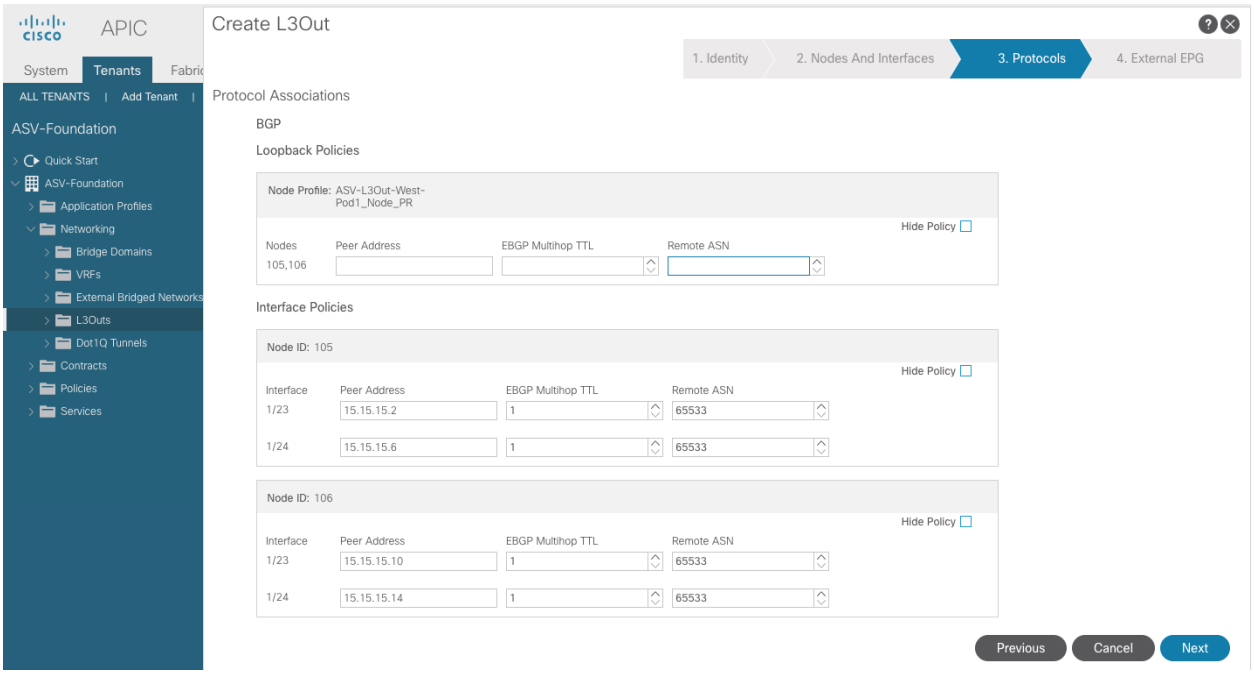
10. Click [+] to add a second node and [+] for the interfaces to have a total of two nodes and two interfaces per node.
11. From the Node ID field drop-down menu, choose the nodes for the L3Out.
12. Use node **105** and **106** in this example.
13. In the Router ID field, enter the router ID.

Note: The Loopback Address field is automatically populated with the same entry that you provide in the Router ID field.

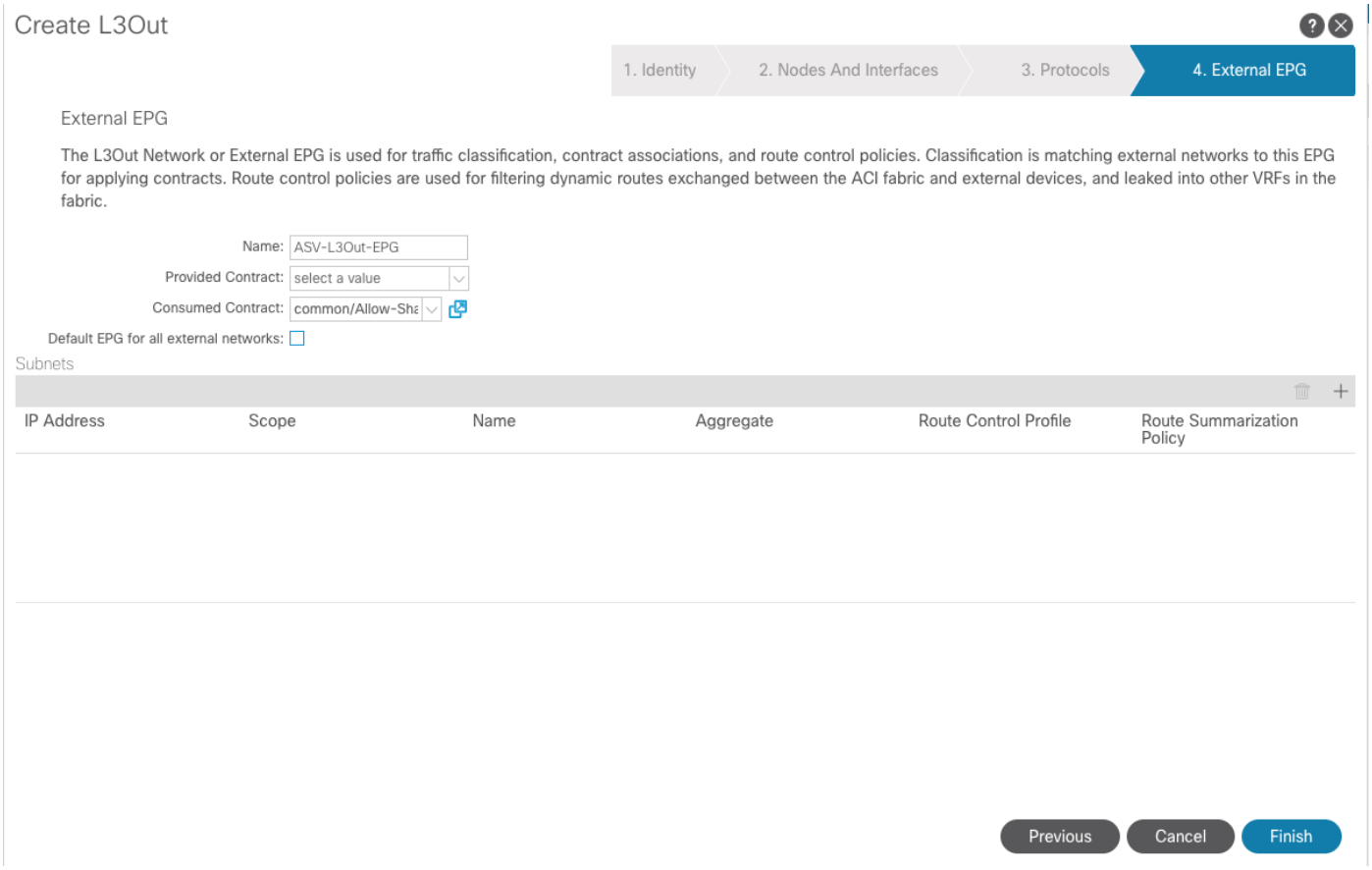
14. Select the interfaces connected to Azure Stack Hub TOR switches and populate their corresponding IP addresses
15. Click **Next** when all the information is populated.



16. The Protocols window appears.
17. Enter the necessary information in the Protocols window of the Create L3Out wizard.
18. In the BGP Loopback Policies and BGP Interface Policies areas, enter the following information from the above table 7:
    - Peer Address: Enter the peer IP address
    - EBGP Multihop TTL: (1) Enter the connection time to live (TTL). The range is from 1 to 255 hops; if zero, no TTL is specified. The default is zero.
    - Remote ASN: (**65533**) Enter a number that uniquely identifies the neighbor autonomous system. The Autonomous System Number can be in 4-byte as plain format from 1 to 4294967295.

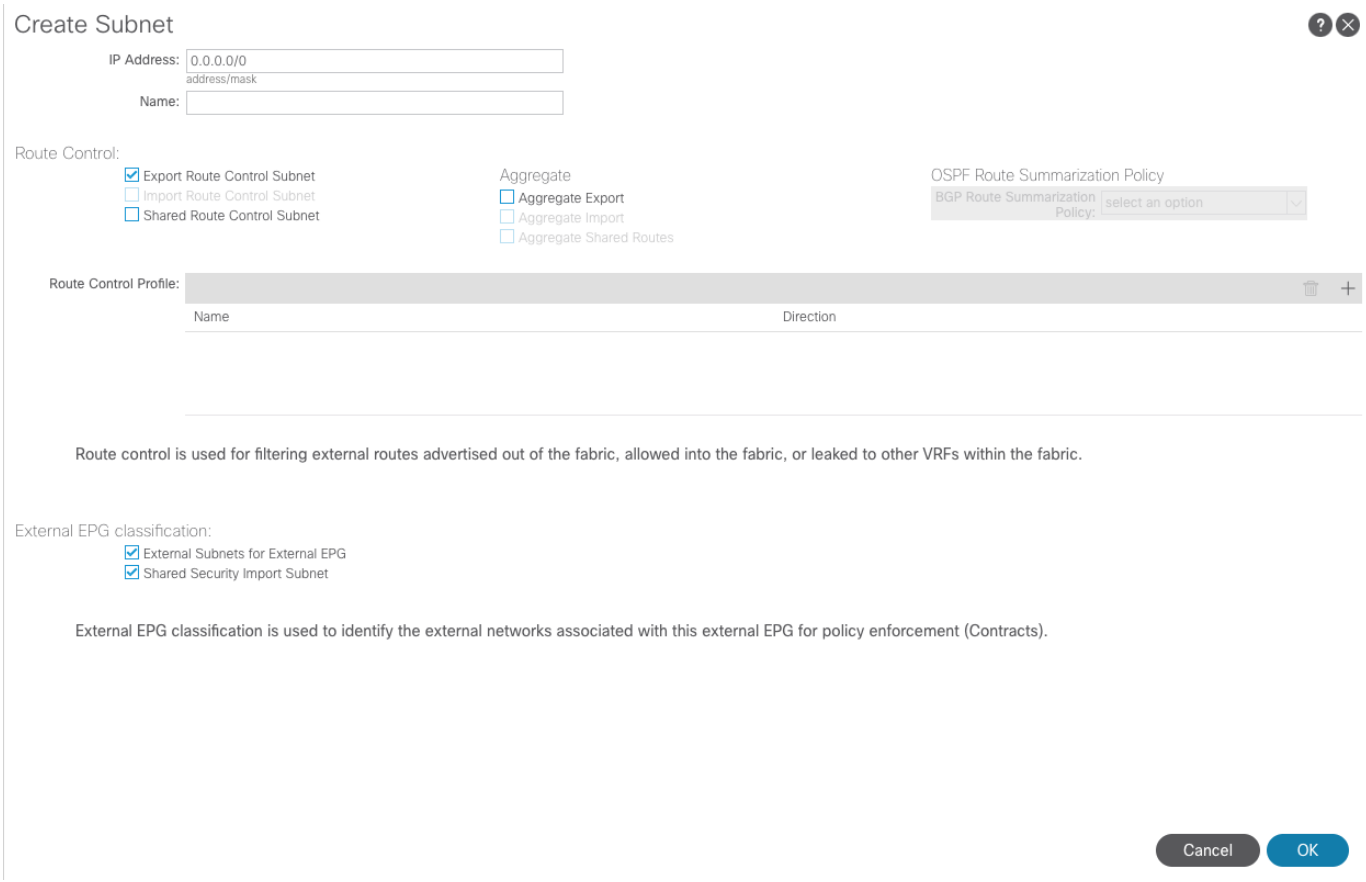


19. Click **Next**.
20. The External EPG window appears.
21. Enter the necessary information in the External EPG window of the Create L3Out wizard.
    - In the **Name** (**ASV-L3Out-EPG**) field, enter a name for the external network.
    - In the **Consumed Contract** field, select (**common/Allow-Shared-L3Out**) from the drop-down menu.
    - Uncheck the **Default EPG for all external networks** field, since we don't want to advertise all the transit routes out of this L3Out connection.

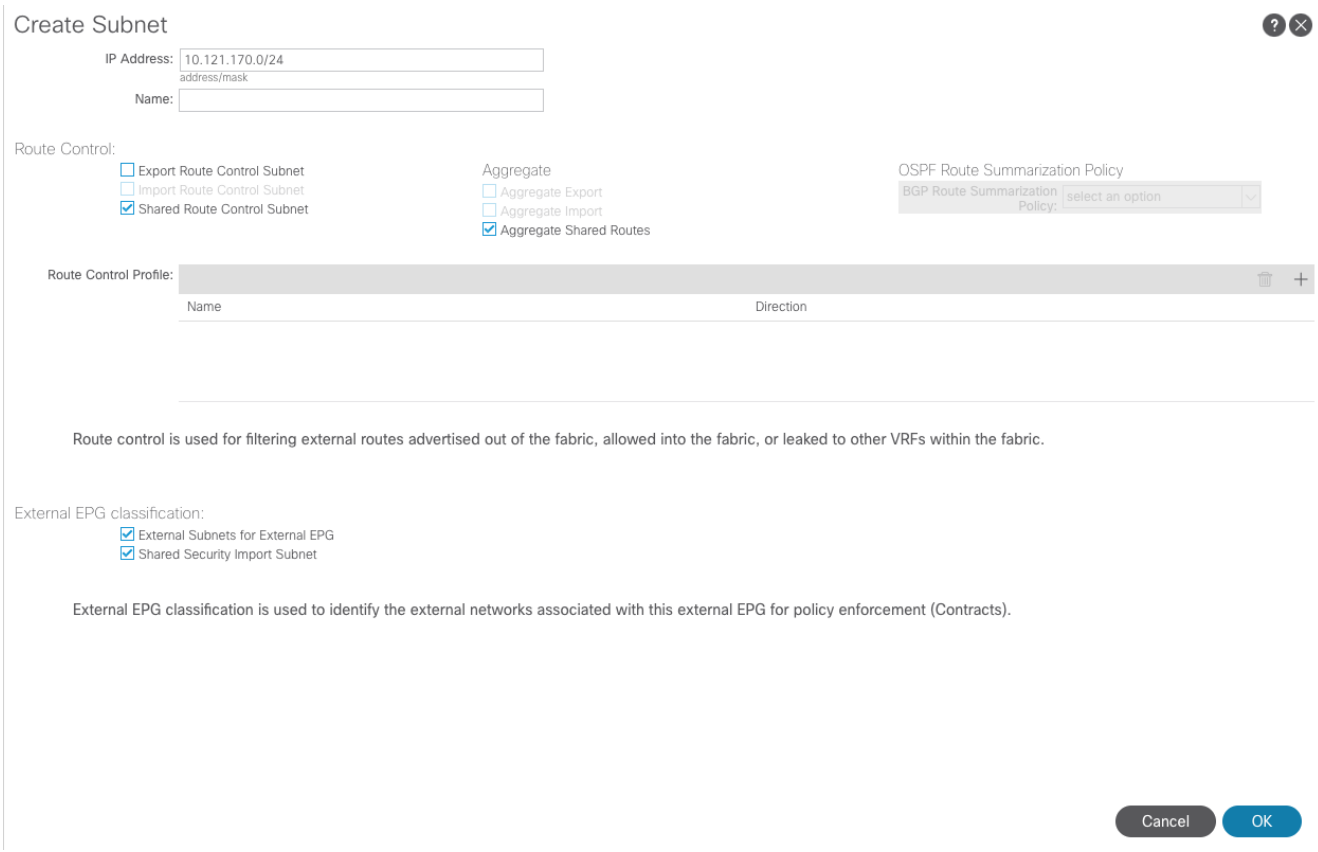


The Subnets area appears if you uncheck this box. Specify the desired subnets and controls as described in the following steps.

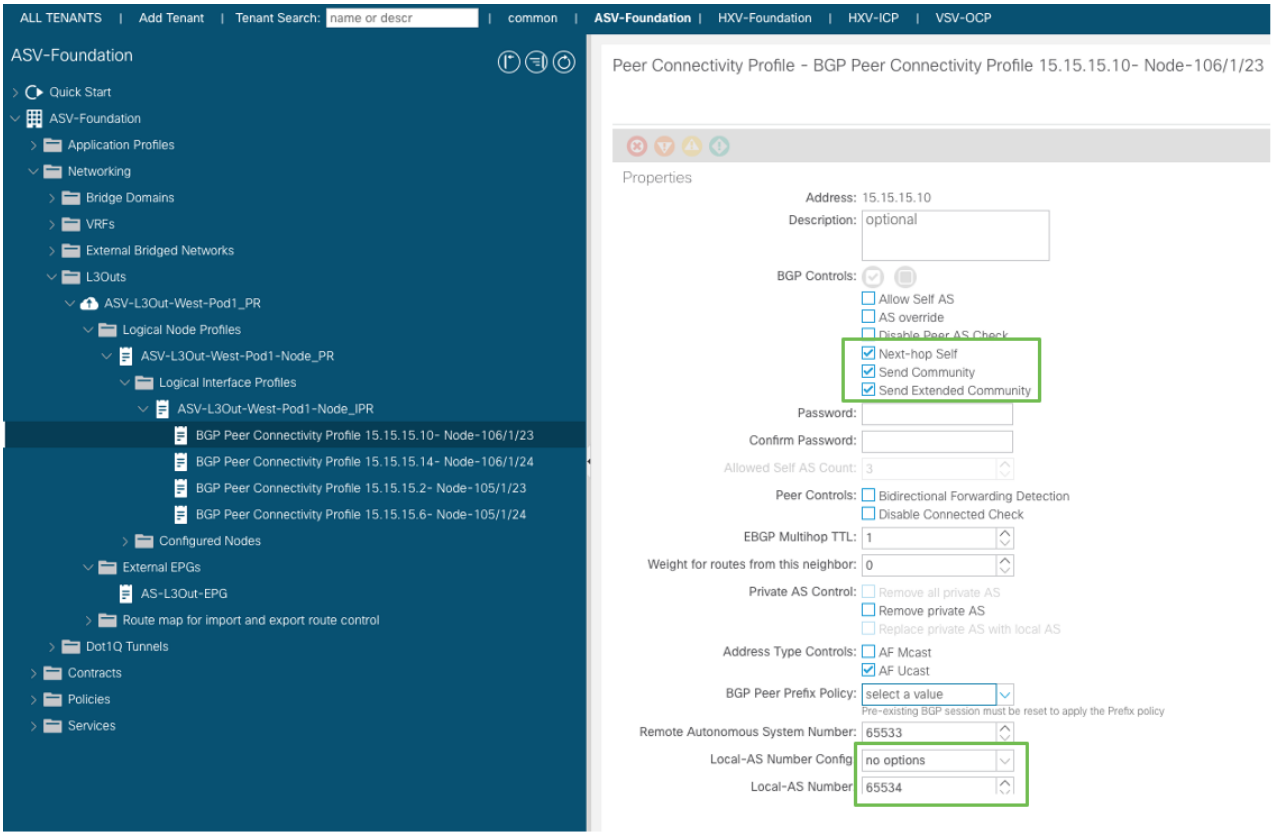
22. Click the [**+**] icon to expand **Subnet**, then perform the following actions in the Create Subnet dialog box.
23. In the IP address field, enter the **(0.0.0.0/0)** IP address and network mask for the external network.
24. In the **Name** field, enter the name of the subnet (optional).
25. In the **Scope** field, check the appropriate check boxes to control the import and export of prefixes for the L3Out.
    - Export Route Control Subnet
    - External Subnet for External EPG
    - Share security import subnet



26. Click the [+] icon again to expand Subnet
27. In the IP address field, enter the **(10.121.170.0/24)** IP address and network mask for the external network.
28. In the **Name** field, enter the name of the subnet (optional).
29. In the **Scope** field, check the appropriate check boxes to control the import and export of prefixes for the L3Out.
    - Shared Route Control Subnet
    - Aggregate Shared Routes
    - External Subnet for External EPG
    - Share security import subnet

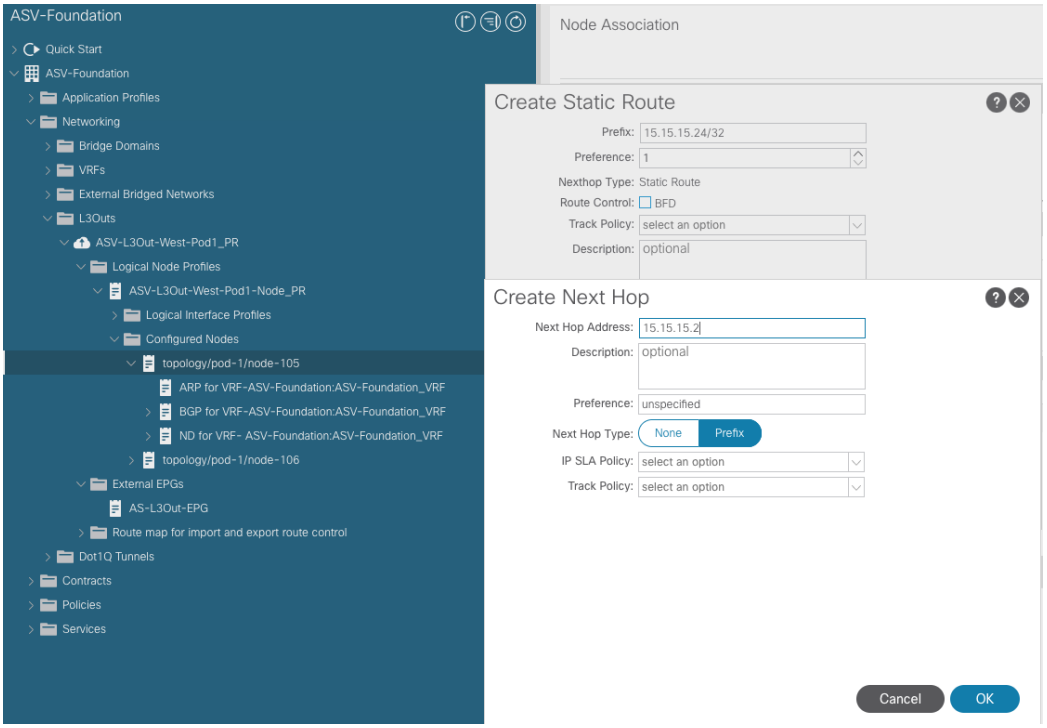


30. Click **OK**.
31. Click **Finish**.
32. In the Navigation pane, under ASV-Foundation > Networking > L3Outs > Logical Node Profiles > Logical Interface Profiles, select each BGP peer connectivity profile and update the following:
    - Next-hop Self
    - Send Community
    - Send Extended Community
    - Local-AS Number Config “no options”
    - Local-AS Number: (**65544)**



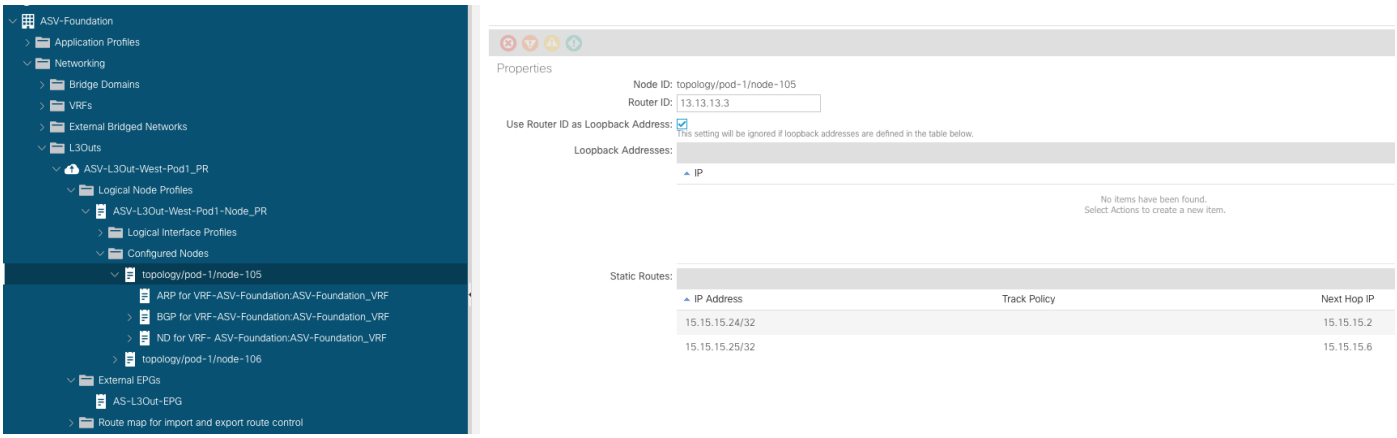
33. Navigate to Tenants > ASV-Foundation > Networking > L3Outs > ASV-L3Out-West-Pod1-Node_PR > Logical Node Profiles > ASV-L3Out-West-Pod1-Node_IPR , then double-click on a node listed in the Nodes (105, 106) area to access the Static Routes area in the Node Association window.

34. Click [+] icon and add the remote loopback interface IP addresses and the gateway IP address.

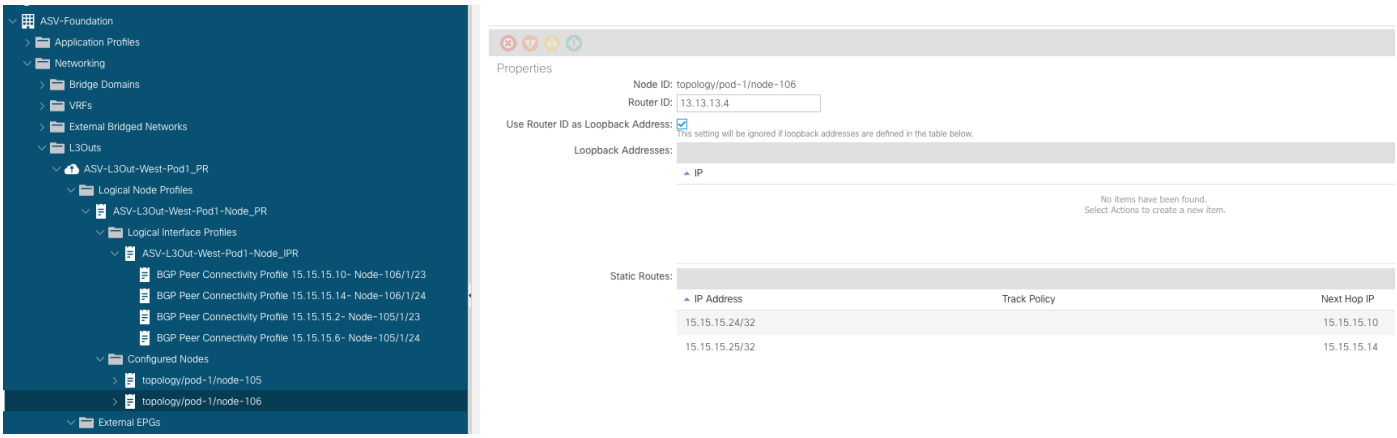


35. Routes configured via both the nodes to both remote loopback IP addresses on the Azure Stack Hub TOR switches are shown below:

Static Routes on Node 105



Static Routes on Node 106



Conclusion

Cisco Integrated System for Microsoft Azure Stack Hub Network integration planning is an important prerequisite for successful Azure Stack Hub integrated systems deployment, operation, and management. This document provides design and implementation information on how to best integrate Azure Stack Hub into your existing Cisco ACI networking environment.

For more information

http://www.cisco.com/go/aci

https://www.cisco.com/c/en/us/solutions/data-center/integrated-system-microsoft-azure-stack/index.html

About the Author

Sreenivasa Edula, Technical Marketing Engineer, UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Sreeni is a Technical Marketing Engineer in the Cisco UCS Data Center Solutions Engineering team focusing on converged and hyper-converged infrastructure solutions, prior to that he worked as a Solutions Architect at EMC Corporation. He has experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage and cloud computing.

Acknowledgments

The author wishes to acknowledge the following individuals, who contributed significant technical knowledge, subject matter expertise, plus review of the laboratory testing and documentation:

Rahul Talekar – Solutions Architect, UCS Data Center Solutions Engineering, Cisco Systems, Inc.

John McAbel – Product Manager, UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Mike Mankovsky – Principal Engineer, UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Revision history

Revision	Coverage
Initial version	• Cisco Integrated System for Microsoft Azure Stack Hub 2002 • Cisco ACI 4.2(4i)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 220233.2 12/20