Overview

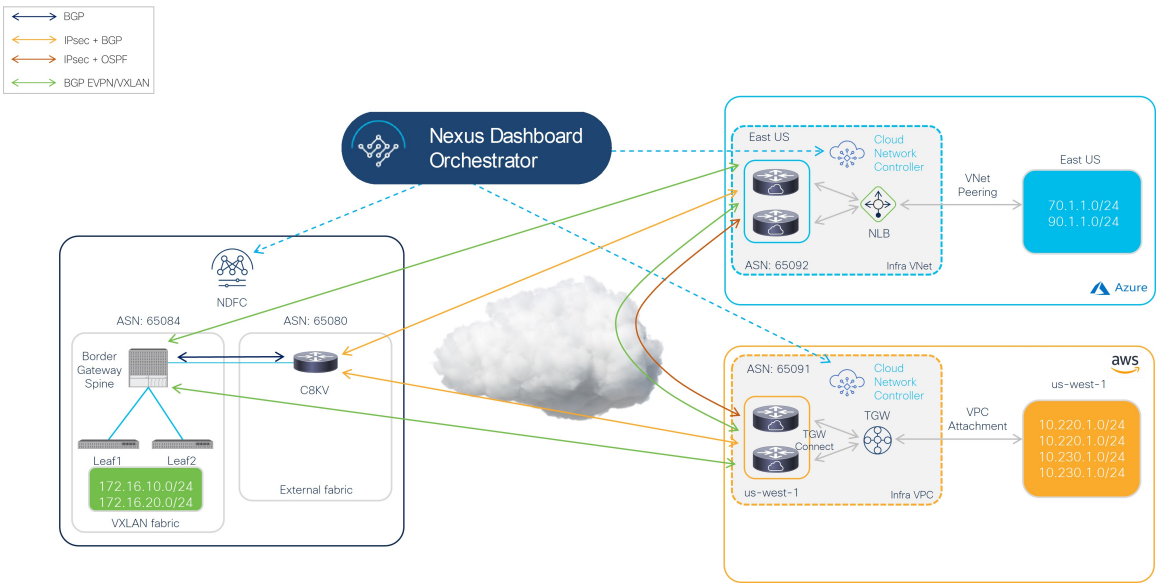
Understanding Components of Hybrid Cloud Connectivity

This document describes deployment steps for the Cisco Hybrid Cloud Networking Solution powered by Cisco Nexus Dashboard Orchestrator (NDO) with a Cisco Nexus 9000 NX-OS based fabric managed by Nexus Dashboard Fabric Controller (NDFC) and public cloud sites managed by Cisco Cloud Network Controller (CNC).

The Cisco Nexus Dashboard Orchestrator (NDO) based Hybrid Cloud solution offers seamless connectivity between on-premises and cloud networks. This solution uses NDFC to manage on-premises VXLAN-based fabric and on-premises Cisco Catalyst 8000Vs, while cloud sites (AWS or Microsoft Azure) are managed by the Cisco Cloud Network Controller (CNC). NDO is used to orchestrate connectivity between on-premises and cloud sites, and between two or more cloud sites. VXLAN is used to build overlay tunnels between the sites.

The following figure shows an example topology for hybrid cloud connectivity using these components. See Supported Topologies for more information.

Figure 1:



In this example topology, the on-premises site managed by NDFC has a secure connection setup to AWS and Azure cloud sites, where Cisco Catalyst 8000Vs sitting on the infra VPC/VNet serve as the cloud gateway for all traffic to and from the on-premises data centers.

On the on-premises site, Border Gateways (BGWs), which support seamless Layer-2/Layer-3 DCI extensions between different on-premises VXLAN EVPN sites, also support Layer-3 extension to the public cloud.

BGP-EVPN is used for the control plane between the BGWs and the Cisco Catalyst 8000Vs in the cloud, and VXLAN is used for the data plane.

As shown in the previous figure, the Cisco Hybrid Cloud Networking Solution consists of the following components:

- **Cisco Nexus Dashboard Orchestrator (NDO)**: NDO acts as a central policy controller, managing policies across multiple on-premises fabrics managed by different NDFC instances, with each cloud site being abstracted by its own Cisco Cloud Network Controller. NDO runs as a service on top of Nexus Dashboard, where Nexus Dashboard can be deployed as a cluster of physical appliances or virtual machines running on VMware ESXi, Linux KVM, Amazon Web Services or Microsoft Azure. Inter-version support was introduced previously, so NDO can manage Cisco Cloud Network Controller running different software versions.
- **Cisco Nexus Dashboard Fabric Controller (NDFC)**: NDFC is a network automation and orchestration tool for building LAN, VXLAN, SAN and Cisco IP Fabric for Media (IPFM) fabrics. NDFC runs as a service on top of Nexus Dashboard cluster that can be either a physical or a virtual cluster. For the Hybrid Cloud Networking Solution, NDFC manages the on-premises VXLAN fabric and on-premises Cisco Cloud Routers (Catalyst 8000V).
- **On-premises VXLAN fabric**: The on-premises VXLAN fabric is built with Nexus 90000/3000 switches managed by NDFC. The fabric should have one or more Border Gateway (BGW) devices that are responsible for originating and terminating VXLAN Multisite Overlay tunnels between on-premises and cloud sites. NDFC has pre-built templates for creating a VXLAN fabric; this document uses the `External_Fabric` template for the VXLAN fabric.

- **On-premises Cisco Cloud Router (CCR)**: The CCR is used to provide reachability between the on-premises VXLAN fabric and the cloud sites. The CCR provides connectivity to the cloud sites using either public internet or private connections (such as AWS Direct Connect or Azure ExpressRoute). The on-premises CCRs are managed by NDFC using a pre-built `External_Fabric` template and need to be assigned the `Core Router` role.

  The Cisco Catalyst 8000V is used as the on-premises CCR for the Cisco Hybrid Cloud Networking Solution.

- **Cisco Cloud Network Controller (CNC)**: Cisco Cloud Network Controller runs as a virtual instance on a supported public cloud to provide automated connectivity, policy translation, and enhanced visibility of workloads in the public cloud. The Cisco Cloud Network Controller translates all the policies received from NDO and programs them into cloud-native constructs, such as VPCs and security groups on AWS, and VNets on Microsoft Azure. Cisco Cloud Network Controller is deployed through the public cloud Marketplace, such as AWS Marketplace and Azure Marketplace.

- **Cisco Catalyst 8000V**: The Cisco Catalyst 8000V is an important component in the public cloud platforms. Cisco Catalyst 8000Vs are used for inter-site communication to on-premises sites and the public cloud platforms. In addition, Cisco Catalyst 8000Vs are used for on-premises cloud connectivity and for connectivity between different cloud providers (for example, Azure to AWS).

Building Hybrid Cloud Connectivity

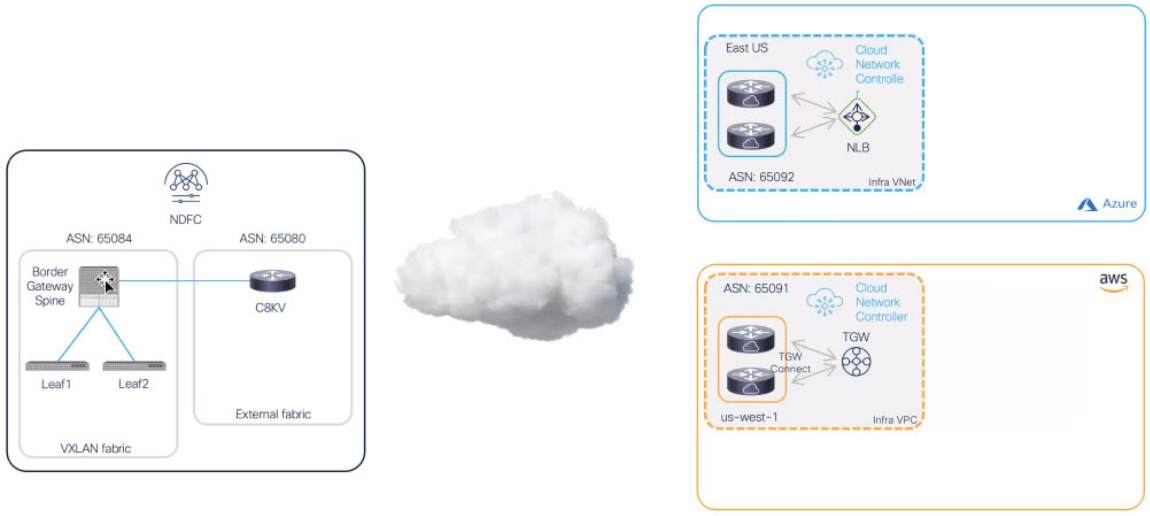
This section describes the process used to build hybrid cloud connectivity.

Starting Point

The following figure shows the starting point for the hybrid cloud connectivity, where we have the various pieces described in Understanding Components of Hybrid Cloud Connectivity, on page 1:

- Nexus Dashboard Fabric Controller (NDFC) fabrics:
  - On-premises VXLAN fabric
  - External fabric
- Cloud sites (AWS and Azure) managed by Cloud Network Controller

Figure 2:

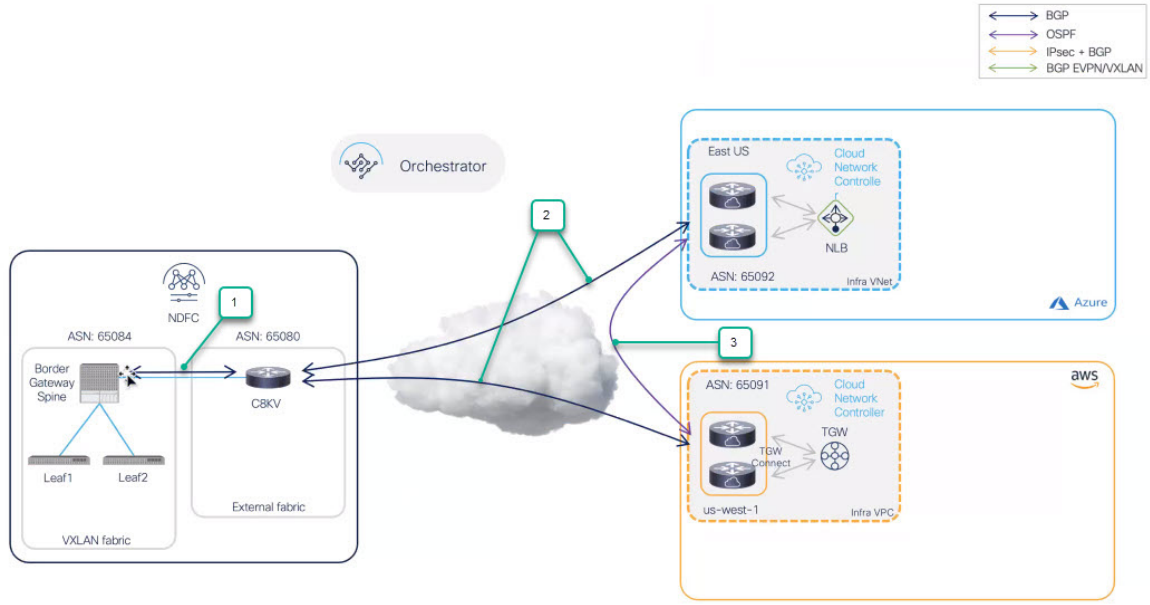


Building the Underlay Layer

Next, we will show how the underlay later is built:

1. First, a BGP connection is established between the border gateway spine switch in the VXLAN fabric and the Cisco Catalyst 8000V in the external fabric.
2. Then, BGP peering is used to establish the underlay connectivity between the on-premises Cisco Catalyst 8000V in the external fabric to each of the cloud routers in the cloud sites.
3. Finally, OSPF is used between the cloud sites for cloud-to-cloud underlay connectivity.

Figure 3:

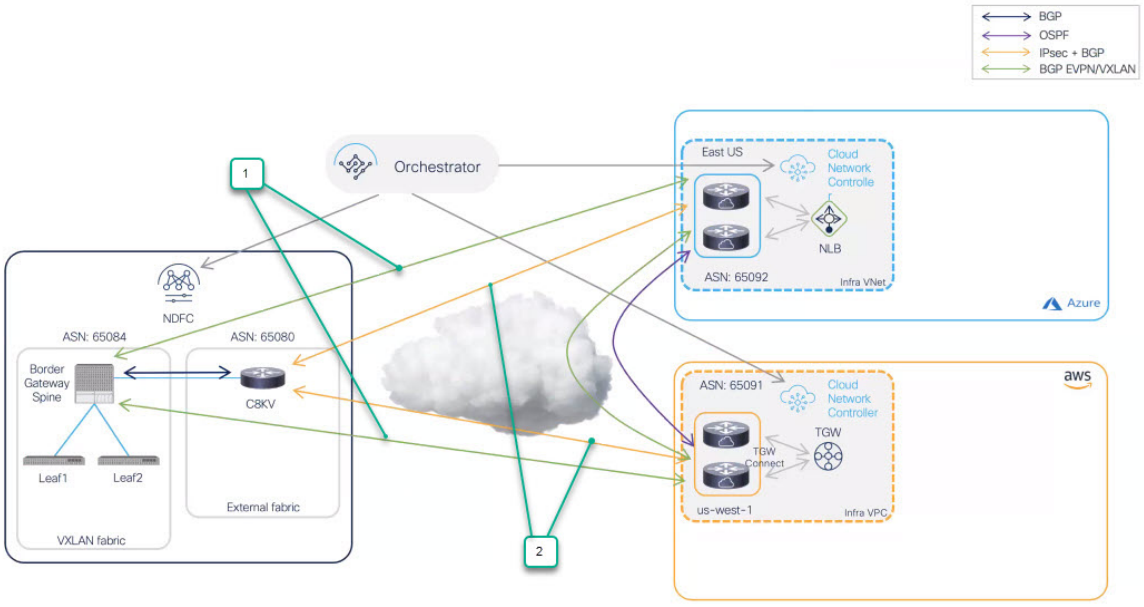


Building Overlay

Finally, we show how to establish the VXLAN Multisite Overlay on top of underlay connectivity established in previous step:

1. A VXLAN multi-site is established, which originates from the border gateway spine switch in the VXLAN fabric and terminates at the Cisco Catalyst 8000Vs in the cloud sites.
2. If you select Public Internet as the connection type, then IPsec and BGP are used to connect between the NDFC VXLAN fabric site and the cloud sites.

Figure 4:



Terminology

The following terms are used throughout this document.

Term	Acronym	Definition
Border Gateway	BGW	One of the supported switch roles in an NDFC Easy Fabric (for example, a VXLAN EVPN fabric). The BGW is used to extend Layer 2/Layer 3 DCI connectivity between on-premises fabrics and Layer 3 connectivity toward public cloud sites (for example, hybrid cloud connectivity).

Term	Acronym	Definition
Core Router		One of the supported roles in an NDFC external fabric. The core router is used to establish Layer 3 connectivity (Underlay) on one side with the VXLAN EVPN fabric, and on the other with the Catalyst 8000Vs in cloud sites.
Direct Connect		Used in the AWS cloud. AWS Direct Connect is a cloud service that links your network directly to AWS to deliver consistent, low-latency performance.
ExpressRoute		Used in the Azure cloud. You can use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on premises or in a co-location environment.
Inter-Site Network	ISN	The Layer 3 infrastructure used to interconnect on-premises VXLAN fabrics, between the on-premises VXLAN fabrics and with the public cloud (also referred to as the "underlay"). As such, the ISN could also include the Internet or the Direct Connect and ExpressRoute dedicated circuits.
IP Security Router	IPsec router	A router capable of Internet Protocol Security (IPsec) is required to establish IPsec connections between the on-premises site and the cloud sites Cisco Cloud Network Controller.

Term	Acronym	Definition
Route Server	RS	The control plane node used to facilitate the establishment of EVPN adjacencies between on-premises BGW devices, alleviating the need of creating full-mesh peering between all of them. The Route Server runs BGP protocol and is used to pass routes between two or more BGP peers. The Route Server function is the eBGP equivalent of the "Route Reflector" function traditionally used for iBGP sessions; it helps in reducing the number of BGP peering required.
Virtual Network	VNet	Used in the Azure cloud. Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VMs), to securely communicate with each other, the internet, and on-premises networks. As related to the Cloud Network Controller, the VRF in the Cloud Network Controller maps to a VNet in Azure.
Virtual Private Cloud	VPC	Used in the AWS cloud. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. As related to the Cloud Network Controller, the VRF in the Cloud Network Controller maps to a VPC in AWS.

Prerequisites

The following software versions are required:

- Cisco Nexus Dashboard (ND) version 2.3.1c or later (physical or virtual cluster)
- Cisco Nexus Dashboard Fabric Controller (NDFC) version 12.1.2e or later
- Cisco Nexus Dashboard Orchestrator (NDO) version 4.1(1) or later
- Cisco Cloud Network Controller (CNC) version 25.1(1e) or later for AWS site and Microsoft Azure site

Guidelines and Limitations

Following are certain guidelines and limitations that you should understand when deploying the hybrid cloud connectivity solution:

- Currently, each Cisco Cloud Network Controller can manage up to sixteen regions in AWS and Azure clouds. If you want to manage more than sixteen regions, you will have to deploy additional Cisco Cloud Network Controllers. For more information, see the "Understanding Limitations for Number of Sites, Regions and CCRs" section in the *Cisco Cloud Network Controller for AWS Installation Guide* or *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(x) or later.

Related Documentation

You can find documentation for the components that make up the Cisco Hybrid Cloud Networking Solution in the following locations:

- Cisco Nexus Dashboard Orchestrator (NDO) documentation
- Cisco Nexus Dashboard Fabric Controller (NDFC) documentation
- Cisco Cloud Network Controller (CNC) documentation
- Cisco Catalyst 8000V documentation
- Amazon Web Services (AWS) documentation
- Microsoft Azure documentation